



January Public Forum 2021



*Debate***US!**

Formerly Millennial
Speech and Debate

Table of Contents

Table of Contents

<i>Table of Contents</i>	2
Definitions	11
“Privacy” Defined.....	12
Affirmative Arguments	15
Overload	16
Information Overload	17
Yes Overload.....	29
Overload = nuke war	41
Iran !	42
Turns aff – drones.....	43
Turns aff – generic	45
Turns aff - NCTC.....	47
Turns aff – NSA	48
Turns aff – NSA – grid collapse	53
Turns aff – UPSTREAM.....	55
Turns cyberterror	56
Turns terror	59
Turns military readiness	71
Internet Freedom	76
Surveillance kills soft power.....	91
Economy	93
NSA killing tech competitiveness	104
Perception key.....	106
AT: Doesn’t hurt cloud computing	108
Cyber Security - Encryption	110
What is Encryption?.....	111
Encryption is Surveillance	113
Inherency – Encryption Cracking Now	125
International Modeling.....	131
Cyber Security Advantage Links.....	132
Economy Advantage.....	137
Privacy Advantage	142
Frontlines to Cybersecurity Contention	145
FT: No Real Threat	146
Impact Extension	147
FT: Deterrence	148
FT: No Capability	149
FT: No Blackout.....	152
EXT- Grid Impact.....	154

FT: Backups.....	156
FT: Not Likely	157
FT: Resilient.....	159
FT: Cant solve cyberterrorism.....	162
FT: No US Leadership	164
EXT-Solves Cybersecurity	166
FT: Trust Now	167
EXT: Econ Imp.....	168
Cooperation	170
Global Cooperation.....	171
European Cooperation.....	175
Emerging Powers Cooperation.....	184
India Cooperation	185
China Cooperation.....	187
Tech Companies Cooperation	190
Cooperation Key to Stopping ISIS	195
Arab-American Cooperation.....	196
Surveillance Violates Privacy	200
Inherency/Uniqueness.....	201
Privacy First.....	211
Privacy = Gateway Right	215
Privacy = Moral Obligation.....	216
Privacy - Deontology.....	220
Privacy good – Post Liberal	221
Alt Fails – Aff key.....	223
Perm – Semantic Discontinuity.....	226
Greatest Hits of Rights Cards	228
Surveillance Bad – Totalitarianism.....	232
Surveillance Bad – Democracy -Chilling Effect.....	234
Surveillance Bad – Democracy	236
Democracy good – Growth	238
Global Totalitarianism	239
Surveillance is Totalitarian.....	240
Tyranny Creep	258
Surveillance Bad – Social Control	259
Surveillance Bad – Dehumanization	263
Surveillance Bad – Constitutionality.....	265
Surveillance Internal.....	269
Rights based Advantage Impact/Framing.....	271
FISA Probable Cause Requirements Fail	274
Ext – Justify Any Surveillance Action	279
Ext – Vagueness Means Can't Define	280
Privacy Key To Dignity.....	282
Privacy Key To Identity Formation.....	285
Mass Surveillance Not Needed to Fight Terrorism.....	288
Surveillance doesn't solve	302
NSLs Specific	306
Drones.....	307
Drones – Link Turn.....	308
Airport Security.....	309

PRISM	312
CVE fails	314
Hacking encryption turn	317
Privacy Key To Free Speech	318
Privacy Key To Other Rights	319
Surveillance Bad - Liberty	320
Privacy good - Autonomy	323
Privacy good - Individuality	324
Privacy good – Self Determination	327
Privacy Good – Democracy	328
Privacy good – Serial Policy Failure	333
Privacy good – Check State Power	335
Intellectual Privacy key 1 st Amend	336
Fear Magnifies Privacy Loss	337
Privacy Outweighs w/Util	338
Privacy Impacts	353
Moral Imperative	362
Surveillance Kills Privacy	363
The Constitutional Right to Privacy	367
Privacy Key to Democracy	371
Privacy Key to Freedom	374
Privacy Critical to Self-Actualization	375
Privacy Key to Personal Security	379
Privacy Key to Freedom of Association	380
International Law Protects Privacy	382
Targeted Surveillance Good/Mass Surveillance Bad	384
Protecting Privacy key to Innovation	387
Loss of Privacy Threatens Cyber Security	394
Privacy Internal Link Turns Case – Markets/Economic Growth	395
Privacy Generally Good	397
Societal Benefits	400
Autonomy	401
Dignity	405
Identity Development	409
Intellectual Freedom	412
Relationships	420
Corporate Surveillance Undermines Democracy	421
Totalitarianism/Loss of Democracy	422
Social Structure	437
Employment	439
Human Rights	440
Privacy Key To Other Rights	442
Rights based Advantage Impact/Framing	444
Privacy First	447
Privacy = Moral Obligation	451
Privacy - Deontology	453
702 Surveillance Program	454
702 Supports Surveillance/Rights Deprivation	455
Privacy key to competitiveness	460
Should End NSA Surveillance	462

XO 12333 Doesn't Target US Citizens.....	466
702 not US Citizens	467
XO 12333 not domestic.....	470
Surveillance must be non-public information.....	472
Excludes zero day vulnerabilities.....	473
Privacy/Tyranny Advantage Answers	476
Fourth Amendment Answers	482
Surveillance State Frontline	485
Extension – Alt Causes to Panopticism.....	488
A2: Authoritarianism.....	490
A2: Tyranny.....	492
A2: State Abuses are morally objectionable.....	493
EXT: No Abuse of Surveillance	495
Ext - -No Significant NSA Information Gathering	496
Ext -- No Greater than What Private Companies Do.....	498
Ext – Not US Citizens.....	500
Ext – Oversight Solves.....	501
Ext – It's Voluntary.....	504
A2: No Legislative Authority for Metadata Collection	505
A2: Scope of Collection is Too Broad.....	507
Government Power Answers	509
Phone Records Program Could Have Prevented 9/11	510
Answer to Negative Arguments	511
AT Circumvention.....	512
AT: Executive Circumvention	512
AT circumvention – generic.....	513
AT circumvention – intel-sharing	514
Tcircumvention – privates	515
AT Circumvention (PDD 28)	516
AT FBI Circumvention.....	518
AT: FISA surveillance only foreign.....	519
AT: 702 only foreign.....	524
AT Terrorism	528
AT Terrorism if no Surveillance.....	529
AT NSA Surveillance Key to stopping terrorism.....	535
AT Surveillance Stopped 54 Attacks	537
IT Benjamin Wittes — General	540
IT Benjamin Wittes — “Glenn Greenwald Bad”.....	547
IT Benjamin Wittes — “Nothing To Hide”	556
I2 Benjamin Wittes — “Surveillance Debates Bad”	559
AT Section 215 Specific -- Frontline	563
AT 44 Examples of Section 215’s Effectiveness	566
AT Stopped Somali Funding	572
AT Section 215 Stopped NY Stock Exchange Attacks	575
AT Section 215 Was Critical to Catch the Capitol Bomber.....	576
AT Section 215 Key to David Coleman Headley Investigation	577
Ext – Examples Stopped Through Other Means	578
AT Section 215 Increases the Speed of Terror Investigations.....	579
AT Section 215 Would Have Stopped 9-11 if it Existed Then	581

AT Section 215 Will Stop Future Attacks.....	583
AT Section 215 Stopped the Zanzi/NY City Attack.....	584
AT Now Terrorists Know We are Trying to Monitor Their Communication.....	585
AT Congressional Support Proves Democratic Support for Section 215.....	586
Extension Mass Surveillance Undermines the War on Terror (Information Overload)	590
AT Moalin/Saudi Capture.....	592
AT More Data Needed to Fight Terrorism.....	593
AT Provides sense of security	594
AT Not enough information.....	595
AT tech solves Overload.....	597
AT more data solves	600
AT Congress Checks Overload.....	604
AT CIA.....	605
AT Privacy	614
AT Privacy General	615
Private Seector Makes Violations Non-Unique.....	621
AT Deontological Right to Privacy	632
AT Mass Surveillance	638
AT NSA Spying Violates Privacy.....	640
AT NSA Surveillance Violates Privacy	641
AT Nazi's Violated Privacy	645
AT Constitutional Violation.....	646
AT Warrant Requirements Meant to Protect Privacy	647
AT Rights General.....	649
AT "Petro – Freedom is Absolute".....	654
Aff Misc	655
Serial Policy Failure.....	656
Infoglut.....	659
Authenticity	665
Deliberation/indentity.....	666
Truth testing.....	668
AT Abusive Probable Cause Determinations Reviewed by the Courts.....	670
AT But We Use Reasonable Suspicion.....	673
AT "Nothing to Hide"	678
AT "Posner – Balancing Good"	679
AT Corporate privacy violations are worse	680
AT Privacy Invasions Inevitable	683
AT Liberalist Conception of Privacy is Bad.....	685
AT Government Won't Abuse Collected Data.....	687
AT Conception of Privacy is Sexist	694
AT Security First.....	695
AT Don't Do Things You Shouldn't Do	697
AT People Don't Care About Privacy	698
AT Metadata Disclosure Doesn't Violate Privacy	699
AT Private Sector Conducts Surveillance	702
AT Kritiks of Privacy	703
AT Surveillance Solves Discrimination.....	705
AT "Nothing To Hide"	707
AT "No Chilling Effect"	709
AT "No Threshold for Privacy"	711

AT “Privacy Not Key To New Ideas”	713
AT “No Risk of Tyranny”	715
AT Small Harm from a Privacy Violation	716
AT Nothing To Hide.....	717
AT No Risk of Tyranny.....	719
AT Government Not Collecting the Data.....	720
AT De-Identification Solves	721
AT Regulations Solve	722
AT “Privacy Laws Solve”.....	725
AT “People Can Opt Out”	726
AT “You Don’t Have to Share Your Data”.....	732
AT First Amendment Right to Exchange Information.....	733
AT Privacy Undermines the Collective.....	735
AT Good to Trade Privacy for Convenience.....	736
AT Privacy Violations Undermine Usage of the IoT	737
AT Privacy is a Commodity, People Voluntarily Give it Up	738
AT Data is Speech.....	739
Negative Arguments.....	742
Terrorism	743
Terrorism DA.....	744
Terrorism Links.....	747
Link – transparency.....	756
Link - PRISM.....	758
Terrorism Links.....	761
Deterrence	784
Every Piece Matters	785
National Security Letters.....	787
General Surveillance Restriction Links.....	789
Mass Surveillance Links.....	801
General NSA Surveillance.....	811
Bulk Collection.....	813
Storage, Super minimization.....	814
Data must be *Aggregated*	815
Link Wall – Detection.....	817
Video Surveillance Links.....	818
Warrant Requirement Links.....	823
Stricter Court Review	825
Internet Surveillance.....	826
XKEYSCORE	835
Court Action, stricter legal standards.....	836
FISA Courts Too Slow to solve counter-terror.....	841
Encryption.....	842
--AT metadata solves.....	865
--AT cloud solves	866
--AT hacking solves.....	867
--AT court order solves.....	869
--AT voluntary solves.....	871
Business Records/Section 2015>Email and Phone Surveillance Restriction Links.....	872
Section 702 Programs/PRISM Necessary to Defeat Terrorism	879
PRISM key to CT – 2NC	882

PRISM Key to Cyber.....	884
PRISM key to Domestic Terrorism	886
PRISM Speed Key.....	887
Materiality requirement.....	910
Third Party Doctrine: FISA.....	911
Third Party Doctrine: Undercover Informant.....	913
Third Party Doctrine: Bank Records	915
Third Party Doctrine: Telephone Calls.....	916
Third Party Doctrine: Metadata	917
Administrative Search Doctrine: FISA.....	918
Administrative Search Doctrine: TSA.....	921
Airport Security Links.....	923
Airport -- Airline attacks coming	936
Airport -- 9/11 style attacks lead to war.....	940
Domestic Surveillance	942
Spies/DITU	946
Increasing Transparency Links	949
Domestic Anti-Terrorism Key.....	950
Counterterrorism Generally Effective.....	951
OCOs	953
Internet key to ISIS	956
OCOs solve.....	961
Intelligence Critical to National Security	962
Intelligence Necessary to Prevent Genocide	965
RFID Links	966
Borders Links.....	969
Prisons	978
FISA links	979
Financial Surveillance Links	981
Links specific to Phone Meta-Data.....	983
Restrictions on FBI/CIA Cooperation	988
Link Boosters: vs Critical Terrorism Affs.....	991
Digital Surveillance.....	996
Internet Surveillance.....	997
Surveillance-Proof Channels	998
Frontlines for Terror DA.....	999
FT Cyber Link Turn.....	1000
FT Doesn't Solve	1001
FT metadata solves.....	1003
FT cloud solves.....	1004
FT hacking solves.....	1005
FT court order solves.....	1007
FT voluntary solves.....	1009
FT Sunset Thumper.....	1010
FT "Name an attack that the program stopped"	1011
FT Arab-American Relations, Intel Coop turn	1013
FT Only Suspected Terrorists.....	1015
FT Useless Data	1016
FT Link Turn- Data Overload	1017
FT HUMINT turn	1023

FT Allied cooperation turn	1028
FT Going dark / encryption	1032
FT false positives (hay stack/puzzle)	1036
FT “New Technology for searches will solve the Terror Disad”	1037
FT Zero sum	1038
FT Recruitment	1039
FT Targeted Surveillance Turn	1041
FT Perception Turn	1045
FT Link Turn – Public/Law Enforcement Cooperation	1050
FT Bruce Schneier	1052
FT New America Foundation Report	1053
FT White House Panel Report	1055
FT Glenn Greenwald	1056
Crime.....	1059
Links.....	1060
Circumvention.....	1065
Circumvention – bulk collection	1066
2nc – redundant capabilities	1068
NSA circumvention	1070
2nc – domestic only limit	1073
Circumvention – allied intel sharing	1076
2nc – circumvention turns the case	1078
Circumvention – FBI specific	1079
Circumvention – section 702	1080
Security	1083
Security First	1084
Security Trumps Constitution	1086
Security Balance Good	1087
National Security Protection Generally Good	1090
Utilitarianism Best	1092
When philosophers become.....	1092
Civil Liberties/Rights Infringements Justified in The War on Terror	1094
Rights not Absolute	1099
Rights Threaten Community	1107
Procedural Rights Threaten Community	1111
Rawls Answers	1112
Privacy Bad/Privacy Not Good	1113
Privacy Generally Bad	1114
Innovation Turn	1116
Extensions – Targeted Advertising Good	1120
General Answers	1127
Extensions – No Harm to Private Use of Data	1141
Extensions – People Voluntarily Share Info	1143
Extensions – Isn’t/Can’t Define	1144
Extensions – No Impact	1146
Extensions—Benefits of the Services Outweigh	1148
Privacy Bad – Social Cohesion	1150
Privacy Bad – Gender	1151

Discrimination Answers	1153
Free Speech Turn	1154
Answer to Affirmative Arguments.....	1156
AT Surveillance State.....	1157
AT Overload.....	1160
Alt Causes	1161
Inev	1162
More data good.....	1163
Squo solves – Big Data.....	1169
Squo solves - CC.....	1171
Squo Solves – gov checks.....	1172
Squo solves - investment.....	1173
Squo Solves - research	1174
Squo solves - tech	1175
AT Chinese Cyberwar.....	1177
AT Border Overload.....	1179
AT NSA good – cyberterror.....	1180
AT legal solutions solve	1181
AT Panopticism.....	1182
AT Authoritarianism.....	1184
AT Tyranny	1186
AT State Abuses are morally objectionable.....	1187
AT Abuse of Surveillance.....	1189
AT Right to Privacy	1190
AT “Petro – Freedom is Absolute”.....	1195
AT Government Surveillance with IoT Bad.....	1196
AT Privacy Key to Dignity.....	1198
AT Need a Thinking Space	1200
AT Privacy an Absolute Right/Moral Obligation.....	1202
AT Privacy is an Inalienable Right”.....	1204
AT “Privacy is a Right”.....	1206
AT Privacy Key to Democracy	1208

Definitions

“Privacy” Defined

Privacy is the ability of people to control information about themselves that they don't want released

Jim Harper is the editor of Privacilla.org and director of information policy studies at the Cato Institute, 2004, Understanding Privacy – and the Real Threats to It,
<http://object.cato.org/sites/cato.org/files/pubs/pdf/pa520.pdf>

An essential starting point, long missing in discussions of privacy, is a definition of the concept itself. The word “privacy” is used casually to describe many concerns in the modern world, and few concepts have been discussed so much without ever being solidly defined. If privacy is going to be a serious topic in information policy—something more than a catch-word in interest-group politics—it needs definition. The attempt below is a serious run at it, but more work from other perspectives will be worthwhile: Privacy is a state of affairs or condition having to do with the amount of personal information about individuals that is known to others. People maintain privacy by controlling who receives information about them and on what terms. Privacy is the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values.

Privacy is a personal, subjective condition

Jim Harper is the editor of Privacilla.org and director of information policy studies at the Cato Institute, 2004, Understanding Privacy – and the Real Threats to It,
<http://object.cato.org/sites/cato.org/files/pubs/pdf/pa520.pdf>

A Personal, Subjective Condition Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be. To illustrate this, one has only to make a few comparisons: Some Americans are very reluctant to share their political beliefs, refusing to divulge any of their leanings or the votes they have cast. They keep their politics private. Their neighbors may post yard signs, wear brightly colored pins, and go door-to-door to show affiliation with a political party or candidate. The latter have a sense of privacy that does not require withholding information about their politics.

Privacy and information privacy

Jan Henrik Ziegeldorf, Communication and Distributed Systems, RWTH Aachen University, Oscar Garcia Morchon, Philips Research and Klaus Wehrle, Communication and Distributed Systems, RWTH Aachen University, Privacy in the Internet of Things: Threats and Challenges,” SECURITY AND COMMUNICATION NETWORKS 2013,
<https://pdfs.semanticscholar.org/8356/9ba92d199a7a5cb172f4b9e28a145e621f41.pdf>

Privacy is a very broad and diverse notion for which literature offers many definitions and perspectives [11]. From a historic view, the notion of privacy shifted between media, territorial, communication, and bodily privacy. With the increasing use and efficiency of electronic data processing information privacy has become the predominant issue today. Information privacy was defined by Westin in 1968 as “the right to select what personal information about me is known to what people” [12]. While Westin’s definition, although it referred to non-electronic environments, is still valid, it is also too general to enable focussed discussion about privacy in the IoT. We thus adapt and concretize definition:

Privacy defined by the ICCPR (International Covenant on Civil and Political Rights)

G. Alex Sinha, Aryeh Neier Fellow, Human Rights Watch and the American Civil Liberties Union, NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW Winter 2013, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2327806

What interests fall within the right to privacy? Volio argues that the right “includes much besides the private matters explicitly listed”—namely, family, home, correspondence, honor, and reputation.²⁹⁶ He claims that the term “privacy” carries its own substantial content that extends beyond the itemized list in Article 17 (pointing to lists of subcomponents of the right to privacy identified by the 1967 Nordic Conference and Dean Prosser’s list of factors for defining privacy under American tort law).²⁹⁷ Nowak claims that privacy, as protected in the ICCPR, comprises “[that sphere of individual autonomy whose existence and field of action does not touch upon the sphere of liberty of others . . .]”²⁹⁸ He notes that “[i]n the 20th century, [protection for the home, family and correspondence] . . . were joined by secrecy of telecommunications, by the general protection of personal data and the genetic code of human beings.”²⁹⁹ Like Volio, Nowak also lists several components of a right to privacy that reach beyond the enumerated categories in Article 17 but that are protected under the broader term “privacy.”³⁰⁰ He identifies relevant interests that fall under headings such as identity, integrity, intimacy, autonomy, communication, and sexuality.³⁰¹ Of particular relevance for present purposes is the category of intimacy, which Nowak claims includes the “protection of personal data.”³⁰² Nowak claims that such protection is especially important because of “technological developments in electronic data processing.”³⁰³ Under Article 17(2), state parties must “regulate the recording, processing, use and conveyance of automated personal data and . . . protect those affected against misuse by State organs as well as private parties.”³⁰⁴ Moreover, “[i]n addition to prohibiting data processing for purposes that are incompatible with the Covenant, data protection laws must establish rights to information, correction and, if need be, deletion of data and to provide effective supervisory measures.”³⁰⁵ Academic commentators are not alone in holding these views. The Human Rights Committee has also spoken directly about the collection and storage of personal data: In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.³⁰⁶ Awareness of privacy risks imposed by smart things and services surrounding the data subject individual control over the collection and processing of personal information by the surrounding smart things awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject’s personal control sphere Our definition of privacy captures in essence the idea of informational self-determination by enabling the subject (i) to assess his personal privacy risks, (ii) to take appropriate action to protect his privacy, and (iii) to be assured that it is enforced beyond his immediate control sphere. Our definition of privacy captures in essence the idea of informational self-determination by enabling the subject (i) to assess his personal privacy risks, (ii) to take appropriate action to protect his privacy, and (iii) to be assured that it is enforced beyond his immediate control sphere. The operating systems analogy described by Radomirovic in [13] is a similar concept to characterize what we refer to as the personal sphere of the data subject. In smart home scenarios it can be pictured as that person’s household or immediate vicinity, as Radomirovic fittingly observes. However, the exact scope of the subject’s personal sphere can differ from situation to situation and it is still unclear what constitutes the individual’s personal sphere, or operating system boundaries in the analogous terms, in e.g. a workplace environment or public space. Similarly, the notion of personal information is necessarily fuzzy, since privacy is a deeply social concept and subject to greatly varying individual perception and requirements [14, 15]. Hence, care must be taken when designing new systems and services to carefully assess the sensitivity of the involved information and relating user requirements, e.g. as businesses are starting to implement in privacy impact analysis’s (PIAs). Ultimately, our definition must be understood such that the user may define what he considers personal information.

Affirmative Arguments

Overload

Information Overload

Mass surveillance decimates effective counter-terrorism — data mining is the wrong tool.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, 2015 (“Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist,” *Digg* — excerpt from *Data and Goliath*, March 24th, Available Online at <https://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist>, Accessed 07-12-2015)

The NSA repeatedly uses a connect-the-dots metaphor to justify its surveillance activities. Again and again — after 9/11, after the Underwear Bomber, after the Boston Marathon bombings — government is criticized for not connecting the dots.

However, this is a terribly misleading metaphor. Connecting the dots in a coloring book is easy, because they're all numbered and visible. In real life, the dots can only be recognized after the fact.

That doesn't stop us from demanding to know why the authorities couldn't connect the dots. The warning signs left by the Fort Hood shooter, the Boston Marathon bombers, and the Isla Vista shooter look obvious in hindsight. Nassim Taleb, an expert on risk engineering, calls this tendency the “narrative fallacy.” Humans are natural storytellers, and the world of stories is much more tidy, predictable, and coherent than reality. Millions of people behave strangely enough to attract the FBI's notice, and almost all of them are harmless. The TSA's no-fly list has over 20,000 people on it. The Terrorist Identities Datamart Environment, also known as the watch list, has 680,000, 40% of whom have “no recognized terrorist group affiliation.”

Data mining is offered as the technique that will enable us to connect those dots. But while corporations are successfully mining our personal data in order to target advertising, detect financial fraud, and perform other tasks, three critical issues make data mining an inappropriate tool for finding terrorists.

The first, and most important, issue is error rates. For advertising, data mining can be successful even with a large error rate, but finding terrorists requires a much higher degree of accuracy than data-mining systems can possibly provide.

Data mining works best when you're searching for a well-defined profile, when there are a reasonable number of events per year, and when the cost of false alarms is low. Detecting credit card fraud is one of data mining's security success stories: all credit card companies mine their transaction databases for spending patterns that indicate a stolen card. There are over a billion active credit cards in circulation in the United States, and nearly 8% of those are fraudulently used each year. Many credit card thefts share a pattern — purchases in locations not normally frequented by the cardholder, and purchases of travel, luxury goods, and easily fenced items — and in many cases data-mining systems can minimize the losses by preventing fraudulent transactions. The only cost of a false alarm is a phone call to the cardholder asking her to verify a couple of her purchases.

Similarly, the IRS uses data mining to identify tax evaders, the police use it to predict crime hot spots, and banks use it to predict loan defaults. These applications have had mixed success, based on the data and the application, but they're all within the scope of what data mining can accomplish.

Terrorist plots are different, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless.

The reason lies in the mathematics of detection. All detection systems have errors, and system designers can tune them to minimize either false positives or false negatives. In a terrorist-detection system, a false positive occurs when the system mistakenly identifies something harmless as a threat. A false negative occurs when the system misses an actual attack. Depending on how you “tune” your detection system, you can increase the number of false positives to assure you are less likely to miss an attack, or you can reduce the number of false positives at the expense of missing attacks.

Because terrorist attacks are so rare, false positives completely overwhelm the system, no matter how well you tune. And I mean completely: millions of people will be falsely accused for every real terrorist plot the system finds, if it ever finds any.

We might be able to deal with all of the innocents being flagged by the system if the cost of false positives were minor. Think about the full-body scanners at airports. Those alert all the time when scanning people. But a TSA officer can easily check for a false alarm with a simple pat-down. This doesn't work for a more general data-based terrorism-detection system. Each alert requires a lengthy investigation to determine whether it's real or not. That takes time and money, and prevents intelligence officers from doing other productive work. Or, more pithily, when you're watching everything, you're not seeing anything.

The US intelligence community also likens finding a terrorist plot to looking for a needle in a haystack. And, as former NSA director General Keith Alexander said, “you need the haystack to find the needle.” That statement perfectly illustrates the problem with mass surveillance and bulk collection. When you're looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you're also adding much more noise. And despite the NSA's “collect it all” mentality, its own documents bear this out. The military intelligence community even talks about the problem of “drinking from a fire hose”: having so much irrelevant data that it's impossible to find the important bits.

We saw this problem with the NSA's eavesdropping program: the false positives overwhelmed the system. In the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Suspicious Activity Reports —or SAR — database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent \$8,500 to a Somali group that posed no direct threat to the US — and that was probably trumped up so the NSA would have better talking points in front of Congress.

The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon finish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportionate impact on the criteria used to decide who's a likely terrorist, leading to ineffective detection strategies.

The third problem is that the people the NSA is trying to find are wily, and they're trying to avoid detection. In the world of personalized marketing, the typical surveillance subject isn't trying to hide his activities. That is not true in a police or national security context. An adversarial relationship makes the problem much harder, and means that most commercial big data analysis tools just don't work. A commercial tool can simply ignore people trying to hide and assume benign behavior on the part of everyone else. Government data-mining techniques can't do that, because those are the very people they're looking for.

Adversaries vary in the sophistication of their ability to avoid surveillance. Most criminals and terrorists — and political dissidents, sad to say — are pretty unsavvy and make lots of mistakes. But that's no justification for data mining; targeted surveillance could potentially identify them just as well. The question is whether mass surveillance performs sufficiently better than targeted surveillance to justify its extremely high costs. Several analyses of all the NSA's efforts indicate that it does not.

The three problems listed above cannot be fixed. Data mining is simply the wrong tool for this job, which means that all the mass surveillance required to feed it cannot be justified. When he was NSA director, General Keith Alexander argued that ubiquitous surveillance would have enabled the NSA to prevent 9/11. That seems unlikely. He wasn't able to prevent the Boston Marathon bombings in 2013, even though one of the bombers was on the terrorist watch list and both had sloppy social media trails — and this was after a dozen post-9/11 years of honing techniques. The NSA collected data on the Tsarnaevs before the bombing, but hadn't realized that it was more important than the data they collected on millions of other people.

This point was made in the 9/11 Commission Report. That report described a failure to "connect the dots," which proponents of mass surveillance claim requires collection of more data. But what the report actually said was that the intelligence community had all the information about the plot without mass surveillance, and that the failures were the result of inadequate analysis.

Mass surveillance didn't catch underwear bomber Umar Farouk Abdulmutallab in 2006, even though his father had repeatedly warned the U.S. government that he was dangerous. And the liquid bombers (they're the reason governments prohibit passengers from bringing large bottles of liquids, creams, and gels on airplanes in their carry-on luggage) were captured in 2006 in their London apartment not due to mass surveillance but through traditional investigative police work. Whenever we learn about an NSA success, it invariably comes from targeted surveillance rather than from mass surveillance. One analysis showed that the FBI identifies potential terrorist plots from reports of suspicious activity, reports of plots, and investigations of other, unrelated, crimes.

This is a critical point. Ubiquitous surveillance and data mining are not suitable tools for finding dedicated criminals or terrorists. We taxpayers are wasting billions on mass-surveillance programs, and not getting the security we've been promised. More importantly, the money we're wasting on these ineffective surveillance programs is not being spent on investigation.

intelligence, and emergency response: tactics that have been proven to work. The NSA's surveillance efforts have actually made us less secure.

Surveillance causes data overload- hurts operations more

Kalhan '14 [Anil, J.D. from Yale Law School, Associate Professor of Law, Drexel University. A.B., Brown University, "Immigration Surveillance," Maryland Law Review, Volume 74, Issue 1, <http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3646&context=mlr>]

Vindicating these interests in the context of immigration surveillance therefore requires context-appropriate constraints on the collection, use, storage, and dissemination of personal information for immigration enforcement purposes—including robust limits on retention periods and secondary uses of information that were not originally contemplated. To date, however, exuberance over the potential benefits of interoperable databases and other new technologies has clouded attention to the continued importance of these limits when implementing these systems for migration and mobility control purposes. In an era in which more data is almost always assumed to be better, more information sharing and interconnectivity between database systems is also often assumed to be better as well.³⁰⁹ But as John Palfrey and Urs Gasser have emphasized, “complete interoperability at all times and in all places . . . can introduce new vulnerabilities” and “exacerbate existing problems.” Accordingly, they argue, placing constraints upon information sharing and interoperability and retaining “friction in [the] system” may often be more optimal.³¹⁰

Information overload makes it harder to identify terrorists

Matthias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

By flooding the system with false positives, big-data approaches to counterterrorism might actually make it harder to identify real terrorists before they act. Two years before the Boston Marathon bombing, Tamerlan Tsarnaev, the older of the two brothers alleged to have committed the attack, was assessed by the city's Joint Terrorism Task Force. They determined that he was not a threat. This was one of about a thousand assessments that the Boston J.T.T.F. conducted that year, a number that had nearly doubled in the previous two years, according to the Boston F.B.I. As of 2013, the Justice Department has trained nearly three hundred thousand law-enforcement officers in how to file “suspicious-activity reports.” In 2010, a central database held about three thousand of these reports; by 2012 it had grown to almost twenty-eight thousand. “The bigger haystack makes it harder to find the needle,” Sensenbrenner told me. Thomas Drake, a former N.S.A. executive and whistle-blower who has become one of the agency’s most vocal critics, told me, “If you target everything, there’s no target.” Drake favors what he calls “a traditional law-enforcement” approach to terrorism, gathering more intelligence on a smaller set of targets. Decisions about which targets matter, he said, should be driven by human expertise, not by a database.

Paris proves information overload makes it more difficult to catch terrorists

Dustin Volz, January 21, 2015, National Journal, "Snowden: France's 'Intrusive' Surveillance Failed to Stop Paris Attacks," <http://www.nationaljournal.com/tech/snowden-france-s-intrusive-surveillance-laws-failed-to-stop-paris-attacks-20150121> DOA: 1-25-15

Edward Snowden is pointing to the recent terrorist attacks in France as evidence that government mass-surveillance programs don't work because they are "burying people under too much data." "When we look at the Paris attacks specifically, we see that **France passed one of the most intrusive, expansive surveillance laws in all of Europe last year, and it didn't stop the attack,**" the fugitive leaker said in an interview with NOS, a Dutch news organization, released Wednesday. "**And this is consistent with what we've seen in every country.**"

Mass surveillance collects too much data, creating “noise” that makes it difficult to detect actual threats

RT.com, May 2, 2014, <http://rt.com/usa/156536-hayden-greenwald-state-surveillance-debate/>

Greenwald went on to spar with Hayden and Dershowitz over whether the current method of metadata collection would have prevented the terrorist attacks on September 11, 2001.

Hayden argued that intelligence analysts would have noticed the number of calls from San Diego to the Middle East and caught the terrorists who were living inside the US illegally. The problem, he said, was that when the NSA prevented the attack, they would still have to defend the surveillance program because as far as the public would be concerned, nothing went wrong.

But Greenwald stated that a number of experts have come forward to say that such a claim is not only false, but also offensive to the public. Lawrence Wright, the winner of a 2003 Pulitzer Prize for his Al-Qaeda coverage, wrote in the New Yorker earlier this year that one of the primary reasons US authorities failed to stop 9/11 is because they were taking in too much information to accurately sort through. The sheer data volume that such a method of surveillance has created is now threatening to ruin the very internet that so many people now rely upon. "*The gift and the curse of all that data, aside from the civil liberty violations, is that yeah there may be some signal but there's a lot of noise,*" Ohanian said. "**It's a very hard software problem to solve...through the efforts of this mass surveillance we've also undermined so much of the technology that makes the internet work, that keeps us safe. It threatens the technology of how the internet works, and works well.**" "Be it resolved state surveillance is a legitimate defence of our freedoms."

NSA ineffective – info-overload

Puiu 15 – Tibi, ZME Science "**The NSA is gathering so much data, it's become swamped and ironically ineffective at preventing terrorism**" <http://www.zmescience.com/research/technology/nsa-overwhelmed-data-53354/>

One of the most famous NSA whistleblowers (or the 'original NSA whistleblower'), William Binney, said **the agency is collecting stupendous amounts of data** – so much that **it's actually hampering intelligence operations**. Binney worked for three decades for the intelligence agency, but left shortly after the 9/11 attacks. **A program** he had developed **was scrapped and replaced with a system he said was more expensive and more intrusive**, which made him feel he worked for an incompetent employer. Plans to enact the now controversial Patriot Act was the last straw, so he quit. Since then, Binney has frequently criticized

the agency and revealed some of its operations hazards and weaknesses. Among these, he alleges: The NSA buried key intelligence that could have prevented 9/11; The agency's bulk data collection from internet and telephone communications is unconstitutional and illegal in the US; Electronic intelligence gathering is being used for covert law enforcement, political control and industrial espionage, both in and beyond the US; Edward Snowden's leaks could have been prevented. Ironically, Snowden cites Binney as an inspiration. His greatest insights however is that the NSA is ineffective at preventing terrorism because analysts are too swamped with information under its bulk collection programme. Considering Binney's impeccable track record – he was co-founder and director of the World Geopolitical & Military Analysis at the Signals Intelligence Automation Research Center (SARC), a branch with 6,000 employees – I can only presume he knows what he's talking about. The Patriot Act is a U.S. law passed in the wake of the September 11, 2001 terrorist attacks. Its goals are to strengthen domestic security and broaden the powers of law-enforcement agencies with regards to identifying and stopping terrorists. In effect, the law laxes the restrictions authorities have to search telephone, e-mail communications, medical, financial, and other records. Because a lot of people use web services whose servers are located in the US, this means that the records of people not located or doing business in the US are also spied upon by the NSA. All this information, however, comes at a price: overload. According to the Guardian, the NSA buffers a whooping 21 petabytes a day! In this flood of information, an NSA analyst will quickly find himself overwhelmed. Queering keywords like "bomb" or "drugs" might prove a nightmare for the analyst in question. It's impossible not to, considering four billion people — around two-thirds of the world's population — are under the NSA and partner agencies' watchful eyes, according to Binney. "That's why they couldn't stop the Boston bombing, or the Paris shootings, because the data was all there," said Binney for ZDnet.

Info isn't used or shared properly

Eddington 15 -- Patrick Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute. He was formerly a senior policy advisor to Rep. Rush Holt (D-N.J.) and a military imagery analyst at the CIA's National Photographic Interpretation Center. "No, Mass Surveillance Won't Stop Terrorist Attacks" <http://reason.com/archives/2015/01/27/mass-surveillance-and-terrorism#.0wxmih:U8Io>

The recent terrorist attack on the office of French satirical magazine Charlie Hebdo generated a now-familiar meme: Another terrorist attack means we need more surveillance. Sen. Bob Corker (R-Tenn.) said that while "Congress having oversight certainly is important ... what is more important relative to these types of events is ensuring we don't overly hamstring the NSA's ability to collect this kind of information in advance and keep these kinds of activities from occurring." Similarly, Sen. Lindsey Graham (R-S.C.) spoke of his "fear" that "our intelligence capabilities, those designed to prevent such an attack from taking place on our shores, are quickly eroding," adding that the government surveillance "designed to prevent these types of attacks from occurring is under siege." A recent poll demonstrates that their sentiments are widely shared in the wake of the attack. But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the answer: 2009: Umar Farouk Abdulmutallab—i.e., the "underwear bomber"—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community (IC) failed "to connect, integrate, and fully understand the intelligence" it had collected. 2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation. 2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency (NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS. 2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine. No, mass surveillance does not prevent terrorist attacks. It's worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally-dubious ones—were premised on the belief that bin Laden's hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data. Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government's hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination. That malady perfectly describes every intelligence failure from Pearl Harbor to the present day. The Office of the Director of National Intelligence (created by Congress in 2004) was supposed to be the answer to the "failure-to-connect-the-dots" problem. Ten years on, the problem remains, the IC bureaucracy is bigger than ever, and our government is continuing to rely on mass surveillance programs that have failed time and again to stop terrorists while simultaneously undermining the civil liberties and personal privacy of every American. The quest to "collect it all," to borrow a phrase from NSA Director Keith Alexander, only leads to the accumulation of masses of useless information, making it harder to find real threats and costing billions to store. A recent Guardian editorial noted that such mass-surveillance myopia is spreading among European political leaders as well, despite the fact that "terrorists, from 9/11 to the Woolwich jihadists and the neo-Nazi Anders Breivik, have almost always come to the authorities' attention before murdering." Mass surveillance is not only destructive

of our liberties, its continued use is a virtual guarantee of more lethal intelligence failures. And our continued will to disbelieve those facts is a mental dodge we engage in at our peril.

NSA insiders recognize information overload as a serious problem- it undermines counterterror efforts

Maass 5/28 (Peter, national security author, fellow at the Shorenstein Center at Harvard and the American Academy in Berlin, “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE,” <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/>, May 28, 2015, The Intercept, silbs)

<< AS MEMBERS OF CONGRESS struggle to agree on which surveillance programs to re-authorize before the Patriot Act expires, they might consider the unusual advice of an intelligence analyst at the National Security Agency who warned about the danger of collecting too much data. Imagine, the analyst wrote in a leaked document, that you are standing in a shopping aisle trying to decide between jam, jelly or fruit spread, which size, sugar-free or not, generic or Smucker’s. It can be paralyzing.

“We in the agency are at risk of a similar, collective paralysis in the face of a dizzying array of choices every single day,” the analyst wrote in 2011. “‘Analysis paralysis’ isn’t only a cute rhyme. It’s the term for what happens when you spend so much time analyzing a situation that you ultimately stymie any outcome It’s what happens in SIGINT [signals intelligence] when we have access to endless possibilities, but we struggle to prioritize, narrow, and exploit the best ones.”

The document is one of about a dozen in which NSA intelligence experts express concerns usually heard from the agency’s critics: that the U.S. government’s “collect it all” strategy can undermine the effort to fight terrorism. The documents, provided to The Intercept by NSA whistleblower Edward Snowden, appear to contradict years of statements from senior officials who have claimed that pervasive surveillance of global communications helps the government identify terrorists before they strike or quickly find them after an attack.

The Patriot Act, portions of which expire on Sunday, has been used since 2001 to conduct a number of dragnet surveillance programs, including the bulk collection of phone metadata from American companies. But the documents suggest that analysts at the NSA have drowned in data since 9/11, making it more difficult for them to find the real threats. The titles of the documents capture their overall message: “Data Is Not Intelligence,” “The Fallacies Behind the Scenes,” “Cognitive Overflow?” “Summit Fever” and “In Praise of Not Knowing.” Other titles include “Dealing With a ‘Tsunami’ of Intercept” and “Overcome by Overload?”

The documents are not uniform in their positions. Some acknowledge the overload problem but say the agency is adjusting well. They do not specifically mention the Patriot Act, just the larger dilemma of cutting through a flood of incoming data. But in an apparent sign of the scale of the problem, the documents confirm that the NSA even has a special category of programs that is called “Coping With Information Overload.”

The jam vs. jelly document, titled “Too Many Choices,” started off in a colorful way but ended with a fairly stark warning: “The SIGINT mission is far too vital to unnecessarily expand the haystacks while we search for the needles. Prioritization is key.” [>>](#)

NSA insiders cite academic literature about the human attention economy and decision making- bulk data harms both

Maass 5/28 (Peter, national security author, fellow at the Shorenstein Center at Harvard and the American Academy in Berlin, “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE,” <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/>, May 28, 2015, The Intercept, silbs)

“We are drowning in information. And yet we know nothing. For sure.”

—NSA Intelligence Analyst

Many of these documents were written by intelligence analysts who had regular columns distributed on NSANet, the agency’s intranet. One of the columns was called “Signal v. Noise,” another was called “The SIGINT Philosopher.” Two of the documents cite the academic work of Herbert Simon, who won a Nobel Prize for his pioneering research on what’s become known as the attention economy. Simon wrote that consumers and managers have trouble making smart choices because their exposure to more information decreases their ability to understand the information. Both documents mention the same passage from Simon’s essay, Designing Organizations for an Information-Rich World:

In an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it.”

In addition to consulting Nobel-prize winning work, NSA analysts have turned to easier literature, such as Malcolm Gladwell’s best-selling Blink: The Power of Thinking Without Thinking. The author of a 2011 document referenced Blink and stated, “The key to good decision making is not knowledge. It is understanding. We are swimming in the former. We are desperately lacking in the latter.” The author added, “Gladwell has captured one of the biggest challenges facing SID today. Our costs associated with this information overload are not only financial, such as the need to build data warehouses large enough to store the mountain of data that arrives at our doorstep each day, but also include the more intangible costs of too much data to review, process, translate and report.”

Alexander, the NSA director from 2005 to 2014 and chief proponent of the agency’s “collect it all” strategy, vigorously defended the bulk collection programs. “What we have, from my perspective, is a reasonable approach on how we can defend our nation and protect our civil liberties and privacy,” he said at a security conference in Aspen in 2013. He added, “You need the haystack to find the needle.” The same point has been made by other officials, including

James Cole, the former deputy attorney general who told a congressional committee in 2013, “If you’re looking for the needle in the haystack, you have to have the entire haystack to look through.”

The opposing viewpoint was voiced earlier this month by Snowden, who noted in an interview with the Guardian that the men who committed recent terrorist attacks in France, Canada and Australia were under surveillance—their data was in the haystack yet they weren’t singled out. “It wasn’t the fact that we weren’t watching people or not,” Snowden said. “It was the fact that we were watching people so much that we did not understand what we had. The problem is that when you collect it all, when you monitor everyone, you understand nothing.”

In a 2011 interview with SIDtoday, a deputy director in the Signals Intelligence Directorate was asked about “analytic modernization” at the agency. His response, while positive on the NSA’s ability to surmount obstacles, noted that it faced difficulties, including the fact that some targets use encryption and switch phone numbers to avoid detection. He pointed to volume as a particular problem. >>

We’re already past the limits on human intelligence- data doesn’t do anything if it can’t be analyzed or used effectively

Maass 5/28 (Peter, national security author, fellow at the Shorenstein Center at Harvard and the American Academy in Berlin, “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE,” <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/>, May 28, 2015, The Intercept, silbs)

<< “We live in an Information Age when we have massive reserves of information and don’t have the capability to exploit it,” he stated. “I was told that there are 2 petabytes of data in the SIGINT System at any given time. How much is that? That’s equal to 20 million 4-drawer filing cabinets. How many cabinets per analyst is that? By the end of this year, we’ll have 1 terabyte of data per second coming in. You can’t crank that through the existing processes and be effective.”

The documents noted the difficulty of sifting through the ever-growing haystack of data. For instance, a 2011 document titled “ELINT Analysts – Overcome by Overload? Help is Here with IM&S” outlined a half dozen computer tools that “are designed to invert the paradigm where an analyst spends more time searching for data than analyzing it.” Another document, written by an intelligence analyst in 2010, bluntly stated that “we are drowning in information. And yet we know nothing. For sure.” The analyst went on to ask, “Anyone know just how many tools are available at the Agency, alone? Would you know where to go to find out? Anyone ever start a new target...without the first clue where to begin? Did you ever start a project wondering if you were the sole person in the Intelligence Community to work this project? How would you find out?” The analyst, trying to encourage more sharing of tips about the best ways to find data in the haystack, concluded by writing, in boldface, “Don’t let those coming behind you suffer the way you have.”

The agency appears to be spending significant sums of money to solve the haystack problem. The document headlined “Dealing With a ‘Tsunami’ of Intercept,” written in 2006 by three NSA officials and previously published by The Intercept, outlined a series of programs to prepare for a

near future in which the speed and volume of signals intelligence would explode “almost beyond imagination.” The document referred to a mysterious NSA entity—the “Coping With Information Overload Office.” This appears to be related to an item in the Intelligence Community’s 2013 Budget Justification to Congress, known as the “black budget”—\$48.6 million for projects related to “Coping with Information Overload.”

The data glut is felt in the NSA’s partner agency in Britain, too. A slideshow entitled “A Short Introduction to SIGINT,” from GCHQ, the British intelligence agency, posed the following question: “How are people supposed to keep on top of all their targets and the new ones when they have far more than [they] could do in a day? How are they supposed to find the needle in the haystack and prioritise what is most important to look at?” The slideshow continued, “Give an analyst three leads, one of which is interesting: they may have time to follow that up. Give them three hundred leads, ten of which are interesting: that’s probably not much use.”

These documents tend to shy away from confrontation—they express concern with the status quo but do not blame senior officials or demand an abrupt change of course. They were written by agency staffers who appear to believe in the general mission of the NSA. For instance, the author of a “SIGINT Philosopher” column wrote that if the NSA was a corporation, it could have the following mission statement: “building informed decision makers — so that targets do not suffer our nation’s wrath unless they really deserve it — by exercising deity-like monitoring of the target.”

On occasion, however, the veil of bureaucratic deference is lowered. In another “SIGINT Philosopher” column, “Cognitive Overflow?,” the author offered a forthright assessment of the haystack problem and the weakness of proposed solutions:

“If an individual brain has finite ‘channel capacity,’ does the vast collective of SID, comprised of thousands of brilliant, yet limited, brains also have a definite ‘channel capacity’? If so, what is it? How do we know when we’ve reached it? What if we’ve already exceeded it? In essence, could SID’s reach exceed its grasp? Can the combined cognitive power of SID connect all the necessary dots to avoid, predict, or advise when the improbable, complex, or unthinkable happens?”

The column did not offer an optimistic view.

“Take for example the number of tools, clearances, systems, compliances, and administrative requirements we encounter before we even begin to engage in the work of the mission itself.” the column continued. “The mission then involves an ever-expanding set of complex issues, targets, accesses, and capabilities. The ‘cognitive burden,’ so to speak, must at times feel overwhelming to some of us.”

The analyst who wrote the column dismissed, politely but firmly, the typical response of senior officials when they are asked in public about their ability to find needles in their expanding haystack.

“Surely someone will point out that the burgeoning amalgam of technological advances will aid us in shouldering the burden.” he noted. “However, historically, this scenario doesn’t seem to completely bear out. The onslaught of more computer power—often intended to automate some processes—has in many respects demanded an expansion of our combined ‘channel capacity’ rather than curbing the flow of the information.” >>

Information overload allowed for the Boston terror attacks- increasing efficiency is key to stop future attacks

Spies 14 (Mike, journalist, “Did NSA-Style Snooping Blind the FBI to Boston’s Bombers? The FBI knew about Tamerlan Tsarnaev in 2011, but information overload meant he was never singled out for attention,” <http://www.vocativ.com/usa/nat-sec/fbi-finally-admits-lost-track-boston-marathon-bomber/>, vocativ, April 13, 2014, silbs)

When the bureau received the tip from the Russians in 2011, it opened an investigation—or an “assessment” in FBI parlance—that included at least one in-person interview with Tamerlan, as well as additional interviews with members of his family. Three weeks later, the Boston bureau’s Joint Terrorism Task Force, which brings representatives from the city’s police department and U.S. Customs and Border Patrol into the fold, placed Tamerlan’s name into a database of people suspected of extremism or ties to terrorists. Along with his name, there was also an alert, specifying that the Boston JTTF must be notified should Tamerlan make international travel plans, which would trigger pings upon his departure and return.

Later, when Tamerlan traveled to Russia and eventually returned to the United States, the JTTF was notified on both occasions. But what remains so disquieting, a year after the bombings, is the FBI’s decision to ignore the warnings. Recently, FBI spokesman Paul Bresson provided Vocativ with a rare inside look at the agency’s investigation of Tamerlan Tsarnaev, and what went wrong.

On June 24, 2011, the bureau, after determining there was nothing suspicious, officially ended its inquiry into Tamerlan. But according to the inspector general for U.S. intelligence agencies, which briefed Congress last week on its latest report concerning the bombings, the FBI didn’t stop there—it continued to pump the Russians for additional information but were apparently ignored. The Russians dispute this claim, but if it is true, it means the FBI was still concerned about Tamerlan, even after the case was officially closed.

So then why, only seven months later, on January 22, 2012, when the JTTF received word that Tamerlan was leaving the country for Russia—where he would spend nearly six months in the volatile state of Dagestan, now considered the heart of the Chechen insurgency—did the agency decide he was not worth questioning? “You have to determine irregularities in travel,” says Bresson. “If he’s making constant trips overseas, going to places like Afghanistan and Pakistan—that’s something we’d need to look into. But this was just one time, and it wasn’t out of the ordinary. I mean, just in Boston alone, our JTTF gets tips like this every day. Nothing about Tamerlan’s trip threw up any warning signs.”

Kade Crockford, the director of the Technology for Liberty Program at ACLU Massachusetts, believes it should have. Crockford, perhaps the foremost authority on the lingering questions raised by the Boston bombings, sees the FBI’s failure to look into Tamerlan’s journey as part of a larger institutional problem. “Millions of people are listed in government databases as potential terrorist threats,” says Crockford. “The FBI has the legal authority to approach anyone for an interview, at any time. Tamerlan’s case confirms what we have long suspected: The databases are so large that they are practically useless. When everyone is a suspect, no one is a suspect.”

“The FBI, originally, was an investigative agency,” says Mike German, a fellow at the Brennan Center for Justice’s Liberty and National Security Program. But since 9/11, the bureau, like many

federal agencies, has increasingly refocused its efforts on intelligence gathering as part of the overall counterterrorism agenda. This, German believes, is where the central failing lies.

“Just like false alarms dull the response of firefighters, these ‘see something, say something’ leads [result in] only cursory investigations, then they move to the next one,” says German. “The Boston FBI JTF conducted 1,000 assessments like this one in 2011 alone, which should be evidence of the problem—if you’re doing 1,000 in a year, those are not going to be as thorough as you need them to be. And you’re not going to be treating them as criminal investigations.” One of the allegations against Tamerlan was that he was going to Russia to meet with underground groups. “This violates the laws of the U.S.,” says German. “So it’s difficult to understand why that didn’t raise more alarms.”

The FBI’s failings went beyond the years before the bombings; they also extended into the days immediately following the attack. On April 17, 2013, two days after pressure-cooker bombs exploded near the marathon’s finish line, the FBI received an image of both Tamerlan and Dzhokhar Tsarneav. But the FBI was unable to identify the two suspects, despite the fact that the agency had photographs of Tamerlan, who’d been arrested for domestic violence, in its database, and that the U.S. government had spent billions of dollars on facial-recognition software meant for just such purposes.

“We attempted to use the facial-recognition technology, but it didn’t work,” admits Bresson. “I’m not sure why.”

And what about the agents and police in the area—did they receive the images, too?

“It stands to reason that the images were shared with all agencies in the Boston community,” Bresson says. “But we literally had no idea who these guys were.”

Yes Overload

Experts agree – squo surveillance is counterproductive and wastes money

Ward 15 – staff writer (Stan, “NSA swamped with data overload also trashes the Constitution,” Best VPN, 5/18/2015, <https://www.bestvpn.com/blog/19187/nsa-swamped-with-data-overload-also-trashes-the-constitution/>) //RGP

Almost on the second anniversary of the Edward Snowden revelations, another (in)famous NSA whistleblower has again spoken up. This comes at a pivotal juncture in the legislative calendar as contentious debate about surveillance rages over the impending sunset of some of the Patriot Act. It has long been an argument of the civil liberties crowd that bulk data gathering was counter-productive, if not counter-intuitive. The argument was couched in language suggesting that to “collect it all”, as the then NSA director James Clapper famously decried, was to, in effect, gather nothing, as the choking amounts of information collected would be so great as to be unable to be analyzed effectively. This assertion is supported by William Binney, a founder of Contrast Security and a former NSA official, logging more than three decades at the agency. In alluding to what he termed “bulk data failure”, Binney said that an analyst today can run one simple query across the NSA’s various databases, only to become immediately overloaded with information. With about four billion people (around two-thirds of the world’s population) under the NSA and partner agencies’ watchful eyes, according to his estimates, there is far too much data being collected. “That’s why they couldn’t stop the Boston bombing, or the Paris shootings, because the data was all there... The data was all there... the NSA is great at going back over it forensically for years to see what they were doing before that. But that doesn’t stop it.” Binney is in a position to know, earning his stripes during the terrorism build up that culminated with the 9/11 World Trade Center bombing in 2001. He left just days after the draconian legislation known as the USA Patriot Act was enacted by Congress on the heels of that attack. One of the reasons which prompted his leaving was the scrapping of a surveillance system on which he long worked, only to be replaced by more intrusive systems. It is interesting to note here that Edward Snowden, in alluding to Binney, said he was inspired by Binney’s plight, and that this, in part, prodded him to leak thousands of classified documents to journalists. Little did Binney know that his work was to be but the tip of the iceberg in a program that eventually grew to indiscriminately “collect it all.” What is worrisome is the complicity with the bulk data collection by dozens of private companies – maybe as many as 72. Yet this type of collection pales in comparison to that of the “Upstream” program in which the NSA tapped into undersea fiber optic cables. With the cooperation of Britain’s GCHQ, the NSA is able to sift more than 21 petabytes a day. Gathering such enormous amounts of information is expensive and ineffective, according to Binney. But it gets lawmakers attention in a way that results in massive increases in NSA budgets. Binney warns that, “They’re taking away half of the Constitution in secret.” President Obama has presided over this agency’s land grab, and has endorsed it, often referring to Upstream as a “critical national security tool.” His feckless approach to the spying build up is the reason for its proliferation, and is why Congress meanders rudderless in attempts to curtail it. The President’s anti-privacy stance is being “rewarded” by repudiation among members of his own party, and is reflected in their rejecting his latest legacy-building, pet piece of legislation – the Trans Pacific Partnership (TPP). But their constituents would be better served by producing legislation that would restore Constitutional rights trampled on by the NSA.

Bulk data collection fails – it saps critical resources and diverts attention

Maass 15 – Journalist for The Intercept (Peter, “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE,” The Intercept, 5/28/2015, <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/>) //RGP

AS MEMBERS OF CONGRESS struggle to agree on which surveillance programs to re-authorize before the Patriot Act expires, they might consider the unusual advice of an intelligence analyst at the National Security Agency who warned about the danger of collecting too much data. Imagine, the analyst wrote in a leaked document, that you are standing in a shopping aisle trying to decide between jam, jelly or fruit spread, which size, sugar-free or not, generic or Smucker’s. It can be paralyzing. “We in the agency are at risk of a similar, collective paralysis in the face of a dizzying array of choices every single day,” the analyst wrote in 2011. “Analysis paralysis’ isn’t only a cute rhyme. It’s the term for what happens

when you spend so much time analyzing a situation that you ultimately stymie any outcome It's what happens in SIGINT [signals intelligence] when we have access to endless possibilities, but we struggle to prioritize, narrow, and exploit the best ones." The document is one of about a dozen in which NSA intelligence experts express concerns usually heard from the agency's critics: that the U.S. government's "collect it all" strategy can undermine the effort to fight terrorism. The documents, provided to The Intercept by NSA whistleblower Edward Snowden, appear to contradict years of statements from senior officials who have claimed that pervasive surveillance of global communications helps the government identify terrorists before they strike or quickly find them after an attack. The Patriot Act, portions of which expire on Sunday, has been used since 2001 to conduct a number of dragnet surveillance programs, including the bulk collection of phone metadata from American companies. But the documents suggest that analysts at the NSA have drowned in data since 9/11, making it more difficult for them to find the real threats. The titles of the documents capture their overall message: "Data Is Not Intelligence," "The Fallacies Behind the Scenes," "Cognitive Overflow?" "Summit Fever" and "In Praise of Not Knowing." Other titles include "Dealing With a 'Tsunami' of Intercept" and "Overcome by Overload?" The documents are not uniform in their positions. Some acknowledge the overload problem but say the agency is adjusting well. They do not specifically mention the Patriot Act, just the larger dilemma of cutting through a flood of incoming data. But in an apparent sign of the scale of the problem, the documents confirm that the NSA even has a special category of programs that is called "Coping With Information Overload." The jam vs. jelly document, titled "Too Many Choices," started off in a colorful way but ended with a fairly stark warning: "The SIGINT mission is far too vital to unnecessarily expand the haystacks while we search for the needles. Prioritization is key." These doubts are infrequently heard from officials inside the NSA. These documents are a window into the private thinking of mid-level officials who are almost never permitted to discuss their concerns in public. AN AMUSING PARABLE circulated at the NSA a few years ago. Two people go to a farm and purchase a truckload of melons for a dollar each. They then sell the melons along a busy road for the same price, a dollar. As they drive back to the farm for another load, they realize they aren't making a profit, so one of them suggests, "Do you think we need a bigger truck?" The parable was written by an intelligence analyst in a document dated Jan. 23, 2012 that was titled, "Do We Need a Bigger SIGINT Truck?" It expresses, in a lively fashion, a critique of the agency's effort to collect what former NSA Director Keith Alexander referred to as "the whole haystack." The critique goes to the heart of the agency's drive to gather as much of the world's communications as possible: because it may not find what it needs in a partial haystack of data, the haystack is expanded as much as possible, on the assumption that more data will eventually yield useful information. "THE PROBLEM IS THAT WHEN YOU COLLECT IT ALL, WHEN YOU MONITOR EVERYONE, YOU UNDERSTAND NOTHING." —EDWARD SNOWDEN The Snowden files show that in practice, it doesn't turn out that way: more is not necessarily better, and in fact, extreme volume creates its own challenges. "Recently I tried to answer what seemed like a relatively straightforward question about which telephony metadata collection capabilities are the most important in case we need to shut something off when the metadata coffers get full," wrote the intelligence analyst. "By the end of the day, I felt like capitulating with the white flag of, 'We need COLOSSAL data storage so we don't have to worry about it,' (aka we need a bigger SIGINT truck)." The analyst added, "Without metrics, how do we know that we have improved something or made it worse? There's a running joke ... that we'll only know if collection is important by shutting it off and seeing if someone screams." Another document, while not mentioning the dangers of collecting too much data, expressed concerns about pursuing entrenched but unproductive programs. "How many times have you been watching a terrible movie, only to convince yourself to stick it out to the end and find out what happens, since you've already invested too much time or money to simply walk away?" the document asked. "This 'gone too far to stop now' mentality is our built-in mechanism to help us allocate and ration resources. However, it can work to our detriment in prioritizing and deciding which projects or efforts are worth further expenditure of resources, regardless of how much has already been 'sunk.' As has been said before, insanity is doing the same thing over and over and expecting different results." "WE ARE DROWNING IN INFORMATION. AND YET WE KNOW NOTHING. FOR SURE." —NSA INTELLIGENCE ANALYST Many of these documents were written by intelligence analysts who had regular columns distributed on NSANet, the agency's intranet. One of the columns was called "Signal v. Noise," another was called "The SIGINT Philosopher." Two of the documents cite the academic work of Herbert Simon, who won a Nobel Prize for his pioneering research on what's become known as the attention economy. Simon wrote that consumers and managers have trouble making smart choices because their exposure to more information decreases their ability to understand the information. Both documents mention the same passage from Simon's essay, Designing Organizations for an Information-Rich World: "In an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it." In addition to consulting Nobel-prize winning work, NSA analysts have turned to easier literature, such as Malcolm Gladwell's best-

selling Blink: The Power of Thinking Without Thinking. The author of a 2011 document referenced Blink and stated, “The key to good decision making is not knowledge. It is understanding. We are swimming in the former. We are desperately lacking in the latter.” The author added, “Gladwell has captured one of the biggest challenges facing SID today. Our costs associated with this information overload are not only financial, such as the need to build data warehouses large enough to store the mountain of data that arrives at our doorstep each day, but also include the more intangible costs of too much data to review, process, translate and report.” Alexander, the NSA director from 2005 to 2014 and chief proponent of the agency’s “collect it all” strategy, vigorously defended the bulk collection programs. “What we have, from my perspective, is a reasonable approach on how we can defend our nation and protect our civil liberties and privacy,” he said at a security conference in Aspen in 2013. He added, “You need the haystack to find the needle.” The same point has been made by other officials, including James Cole, the former deputy attorney general who told a congressional committee in 2013, “If you’re looking for the needle in the haystack, you have to have the entire haystack to look through.” NSA Slide, May 2011 The opposing viewpoint was voiced earlier this month by Snowden, who noted in an interview with the Guardian that the men who committed recent terrorist attacks in France, Canada and Australia were under surveillance—their data was in the haystack yet they weren’t singled out. “It wasn’t the fact that we weren’t watching people or not,” Snowden said. “It was the fact that we were watching people so much that we did not understand what we had. The problem is that when you collect it all, when you monitor everyone, you understand nothing.” In a 2011 interview with SIDtoday, a deputy director in the Signals Intelligence Directorate was asked about “analytic modernization” at the agency. His response, while positive on the NSA’s ability to surmount obstacles, noted that it faced difficulties, including the fact that some targets use encryption and switch phone numbers to avoid detection. He pointed to volume as a particular problem. “We live in an Information Age when we have massive reserves of information and don’t have the capability to exploit it,” he stated. “I was told that there are 2 petabytes of data in the SIGINT System at any given time. How much is that? That’s equal to 20 million 4-drawer filing cabinets. How many cabinets per analyst is that? By the end of this year, we’ll have 1 terabyte of data per second coming in. You can’t crank that through the existing processes and be effective.” The documents noted the difficulty of sifting through the ever-growing haystack of data. For instance, a 2011 document titled “ELINT Analysts – Overcome by Overload? Help is Here with IM&S” outlined a half dozen computer tools that “are designed to invert the paradigm where an analyst spends more time searching for data than analyzing it.” Another document, written by an intelligence analyst in 2010, bluntly stated that “we are drowning in information. And yet we know nothing. For sure.” The analyst went on to ask, “Anyone know just how many tools are available at the Agency, alone? Would you know where to go to find out? Anyone ever start a new target...without the first clue where to begin? Did you ever start a project wondering if you were the sole person in the Intelligence Community to work this project? How would you find out?” The analyst, trying to encourage more sharing of tips about the best ways to find data in the haystack, concluded by writing, in boldface, “Don’t let those coming behind you suffer the way you have.” The agency appears to be spending significant sums of money to solve the haystack problem. The document headlined “Dealing With a ‘Tsunami’ of Intercept,” written in 2006 by three NSA officials and previously published by The Intercept, outlined a series of programs to prepare for a near future in which the speed and volume of signals intelligence would explode “almost beyond imagination.” The document referred to a mysterious NSA entity—the “Coping With Information Overload Office.” This appears to be related to an item in the Intelligence Community’s 2013 Budget Justification to Congress, known as the “black budget”—\$48.6 million for projects related to “Coping with Information Overload.”

Mass surveillance is counter-productive for fighting terrorism – it causes information overload

Gross 13 – covers technology and telecom policy in the U.S. government for the IDG News Service, and is based in Washington, D.C. (Grant, “Critics question whether NSA data collection is effective,” PC World, 6/25/2013, <http://www.pcworld.com/article/2042976/critics-question-whether-nsa-data-collection-is-effective.html>) //RGP

The recently revealed mass collection of phone records and other communications by the U.S. National Security Agency may not be effective in preventing terrorism, according to some critics. The data collection programs, as revealed by former NSA contractor Edward Snowden, is giving government agencies information overload, critics said during the Computers, Freedom and Privacy Conference in Washington, D.C. “In knowing a lot about a lot of different people [the data collection] is great for that,” said Mike German, a former Federal Bureau of Investigation special agent whose policy counsel for national security at the American Civil Liberties Union.

"In actually finding the very few bad actors that are out there, not so good." The mass collection of data from innocent people "won't tell you how guilty people act," German added. The problem with catching terrorism suspects has never been the inability to collect information, but to analyze the "oceans" of information collected, he said. Mass data collection is "like trying to look for needles by building bigger haystacks," added Wendy Grossman, a freelance technology writer who helped organize the conference. But Timothy Edgar, a former civil liberties watchdog in the Obama White House and at the Office of Director of National Intelligence, partly defended the NSA collection programs, noting that U.S. intelligence officials attribute the surveillance programs with preventing more than 50 terrorist actions. Some critics have disputed those assertions. Edgar criticized President Barack Obama's administration for keeping the NSA programs secret. He also said it was "ridiculous" for Obama to suggest that U.S. residents shouldn't be concerned about privacy because the NSA is collecting phone metadata and not the content of phone calls. Information about who people call and when they call is sensitive, he said. But Edgar, now a visiting fellow at the Watson Institute for International Studies at Brown University, also said that Congress, the Foreign Intelligence Surveillance Court and internal auditors provide some oversight of the data collection programs, with more checks on data collection in place in the U.S. than in many other countries. Analysts can query the phone records database only if they see a connection to terrorism, he said. The U.S. has some safeguards that are "meaningful and substantive, although I'm sure many in this room ... and maybe even me, if I think about it long enough, might think they're not good enough," Edgar said. While German noted that the NSA has reported multiple instances of unauthorized access by employees to the antiterrorism databases, Edgar defended the self-reporting. "It's an indication of a compliance system that's actually meaningful and working," he said. "If you had a compliance system that said there was no violation, there were never any mistakes, there was never any improper targeting that took place ... that would be an indication of a compliance regime that was completely meaningless." The mass data collection combined with better data analysis tools translates into an "arms race" where intelligence officials try to find new connections with the data they collect, said Ashkan Soltani, a technology and privacy consultant. New data analysis tools lead intelligence officials to believe they can find more links to terrorism if they just have "enough data," but that belief is "too much sci fi," he said. "This is the difficult part, if you're saying that if we have enough data we'll be able to predict the future," the ACLU's German said.

NSA is overloaded – disproportion between analysts and data risks surprises SIDtoday, 11

The Signals Intelligence Directorate Today Editor, "Is There a Sustainable Ops Tempo in S2? How Can Analysts Deal With the Flood of Collection? – An interview with [redacted] (conclusion)," 4/16/11,
<https://s3.amazonaws.com/s3.documentcloud.org/documents/2089125/analytic-modernization.pdf> // IS

Q: 7. (U//FOUO) Various pushes for analytic modernization have been going on for decades at NSA, but now the issue really seems to be taking center stage. In fact, the number one "SIGINT Goal for 2011-2015" is to "revolutionize analysis." What's different now?

A: (S//SI//REL) We live in an Information Age when we have massive reserves of information and don't have the capability to exploit it. I was told that there are 2 petabytes of data in the SIGINT System at any given time. How much is that? That's equal to 20 million 4-drawer filing cabinets. How many cabinets per analyst is that?? By the end of this year, we'll have 1 terabyte of data per second coming in. You can't crank that through the existing processes and be effective.

Q: (U) ...So it's a matter of volume?

A: (S//SI//REL) Not volume alone, but also complexity. We need to piece together the data. It's impossible to do that using traditional methods. Strong selectors - like phone numbers - will become a thing of the past. It used to be that if you had a target's number, you could follow it for most of your career. Not anymore. My daughter doesn't even make phone calls, and many targets

do the same. Also, the commercial market demands privacy, and this will drive our targets to go encrypted, maybe into unexploitable realms. Our nation needs us to look for patterns surrounding a particular spot on Earth and make the connections - who can do that if not us? And we can't do it using traditional methods.

Q: (U) Looking into the future, is there anything that especially worries you? ...An eventuality (internal or external) that would make it hard for A&P to continue to put out quality intelligence?

A: (U//FOUO) I'm worried that we have so much good stuff that we could lock down analysts and have them just producing product, and something would jump out and surprise us. So we need the discipline to invest in the wild and the unknowns.

Analyst improvement is key to check overload SID Reporting Board, 7

Signals Intelligence Directorate Reporting Board, part of the largest functional directorate in the NSA, "Data Is Not Intelligence," 09/18/07,
<https://s3.amazonaws.com/s3.documentcloud.org/documents/2088973/data-is-not-intelligence.pdf>
// IS

(U) **Data Is Not Intelligence'**

FROM: [Redacted]

SID Reporting Board (S12R) Run Date: 09/18/2007

(U//FOUO) These words came from Dr. Thomas Fingar (pictured) in his keynote address at the Analytic Transformation Symposium in Chicago on 5 September. Such a strong reminder at the opening of his address was intended to remind those at the symposium of the importance he and the Director of National Intelligence, the Honorable J. Michael McConnell, place on improving analysis throughout the Intelligence Community.

(U//FOUO) Dr. Fingar, the Deputy Director of National Intelligence for Analysis, made this statement at the opening of the symposium sponsored by the Intelligence and National Security Alliance, a non-profit, non-partisan public policy forum focusing on intelligence and national security issues. The symposium was held in Chicago, Illinois, from 4 to 6 September 2007.

(U//FOUO) Dr. Fingar continued by saying that "intelligence comes from the brains of analysts."

He clearly wanted those attending the symposium to understand his view of the importance of the analytic process in producing intelligence. The emphasis throughout his remarks was that the Intelligence Community must transform its analytic mission. The transformation is being effected in three areas: enhancing the quality of analytic products; managing the mission more effectively at a Community level; and building more integrated analytic operations across the Intelligence Community.

(U//FOUO) To enhance the quality of analytic products, analysts themselves must improve. They can do this by receiving more and better formal training, and by continuing to learn through experience and mentoring from more experienced analysts. In addition, they must alter mindsets

that keep them from sharing information, especially that which would improve an intelligence product. An adjunct to changing mindsets about sharing information is establishing trust between and among analysts as a way to improve the quality of analytic products.

(U//FOUO) In an explanation of how to manage the analytic mission more effectively at the Community level, Dr. Fingar reviewed the A-Space and Library of National Intelligence (LNI) programs. While some leaders might consider these two programs more as tools, Dr. Fingar stressed that they were programs to help analysts enhance products. A-Space will provide a virtual environment in which analysts can work on data and collaborate. The LNI will give analysts a research facility that will help them gather already-disseminated intelligence on a topic.

(U//FOUO) The effort to build more integrated analytic operations involves, in part, greatly improving collaboration. Setting common standards is a key to collaboration, and collaboration will enhance the quality of analytic products, according to Dr. Fingar. He emphasized that the IC analytic standards recently approved were a step, but only a step. He called for "transparency" in intelligence analysis; that is, that all analysis has to be reproducible. Following established common standards will help ensure transparency. More importantly, collaboration will help establish an analytic community.

(U//FOUO) Dr. Fingar's address set the tone for the rest of the symposium. The point was that the quality of intelligence products must improve--must "transform." The most important part in the transformation is the analyst. In training analysts better, by encouraging them to learn continually through experience and mentoring, product will improve. More effective management, through programs such as A-Space and the LNI, will help give analysts data and intelligence they need, and a better environment in which to work. Collaboration is encouraged and made easier by these programs, and collaboration is part of building integrated operations. All of these together will help ensure that the quality of analytic products improves--that customers receive intelligence, not data.

Data risks errors which have immediate and larger impacts – our timeframe is nanoseconds

Zoldan, 13

Ari Zoldan is an entrepreneur in the technology industry and business analyst based primarily in New York City and Washington, D.C. "More Data, More Problems: is Big Data Always Right?" Wired, May 2013, <http://www.wired.com/2013/05/more-data-more-problems-is-big-data-always-right/> // IS

Which leads us to our second problem: the sheer amount of data! No wonder we are more prone to "signal error" and "confirmation bias." Signal error is when large gaps of data have been overlooked by analysts. If places like Coney Island and Rockaway were overlooked in Hurricane Sandy, like they were in the Twitter study, we could be looking at a higher death toll today. Confirmation bias is the phenomenon that people will search within the data to confirm their own preexisting viewpoint, and disregard the data that goes against their previously held position. In other words, you will find what you seek out. What if FEMA looked at the Twitter data with a preexisting belief that the worst hit part of the Tri-state area was Manhattan? They may have allocated their resources in places that didn't need it the most. The third problem is best described by Marcia Richards Suelzer, senior analyst at Wolters Kluwer. She says, "We can now make catastrophic miscalculations in nanoseconds and broadcast them universally. We have lost the

balance in ‘lag time.’’ Simply put, when we botch the facts, our ability to create damage is greatly magnified because of our enhanced technology, global interconnectivity, and huge data sizes.

Upstream controls the bulk of data – whistleblowers confirm Whittaker, 15

Zack Whittaker is a writer-editor for ZDNet, and sister sites CNET and CBS News, citing an NSA whistleblower, “NSA is so overwhelmed with data, it’s no longer effective, says whistleblower,” ZDNet, 4/30/15, http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/?tag=nl.e539&s_cid=e539&ttag=e539&ftag=TRE17cf61 // IS

"The Upstream program is where the vast bulk of the information was being collected," said Binney, talking about how the NSA tapped undersea fiber optic cables. With help from its British counterparts at GCHQ, the NSA is able to "buffer" more than 21 petabytes a day.

Binney said the "collect it all" mantra now may be the norm, but it's expensive and ineffective.

NSA's spot-a-terrorist data-mining algorithms fail

Musgrave 13 (Shawn, Projects Editor at the public records intelligence site MuckRock.com, 6/8, “Does Mining Our Big Data for Terrorists Actually Make Us Any Safer?” <http://motherboard.vice.com/blog/does-mining-our-big-data-for-terrorists-actually-make-us-any-safer//Tang>)

Whether it's at the NSA, FBI, CIA or some more classified body we mere citizens aren't mature enough to know about, data-mining is the belle of the intelligence ball. The power of statistical prediction to connect the dots, preemptively identify the bad guys and thwart the next terrorist attack has been trumpeted loudly in defense of surveillance programs, including the NSA's latest misadventure. But many counterterrorism and statistical experts doubt that even the most advanced spot-a-terrorist algorithms can produce anything beyond false positives and mangled civil liberties. In his address Friday afternoon, President Obama downplayed the recent revelations about NSA surveillance, dismissing much of the ensuing scrutiny as “hype.” He said that the NSA's extensive collection of phone call metadata from Verizon, Sprint and AT&T, as well as its PRISM program to vacuum up server data from Google, Facebook, Microsoft and other Internet service providers (Dropbox coming soon!) were both legal and appropriately supervised. These programs “help us prevent terrorist attacks,” he said, and “on net it was worth us doing.” Senator Diane Feinstein, standing next to Saxby Chambliss, her Republican counterpart on the Senate Intelligence Committee, explained to the citizenry, “It's called protecting America.” As construction workers put the finishing touches on the NSA's new data facility in Utah—it is said that it will be the largest data center in the world—details continue to emerge that flesh out the exact shape and scope of NSA's various dragnets. As groups like the Electronic Frontier Foundation have been warning for years, it's clear that the agency is pouring considerable resources into collecting and parsing through vast datasets in hopes of neutralizing terrorist threats. But, as has been asked of the TSA and DHS more widely, where's the actual proof these programs offer more benefits than downsides? Where are the thwarted plots to balance against the chill of privacy loss and the threats to, say, activists and the government's political opponents? Among national security experts and data scientists, there's considerable skepticism that NSA-style data-mining is an appropriate tool for ferreting out security threats. As Ben Smith reported yesterday, finding the Boston bombers relied on old fashioned police work, not troves of data. In a 2008 study, the National Research Council concluded that combing data streams for terrorists is “neither feasible as an objective nor desirable as a goal.” In particular, the report's authors underscore dubious data quality and high risk of false positives as practical obstacles to mining data for signatures of terrorist behavior. “There's been considerable interest in the intelligence community around using data to identify terrorists,”

says Stephen Fienberg, a professor of statistics and social sciences at Carnegie Mellon University, who contributed to the NRC report. "But the specifics have always been elusive, and the claims are rarely backed up by serious empirical study." IN A 2006 INTERVIEW WITH THE NEW YORK TIMES, AN FBI OFFICIAL JOKED THAT THE ENDLESS STREAM OF LEADS MEANT MORE "CALLS TO PIZZA HUT" OR CONTACTING A "SCHOOL TEACHER WITH NO INDICATION THEY'VE EVER BEEN INVOLVED IN INTERNATIONAL TERRORISM - CASE CLOSED." Fienberg insists that the rarity of terrorist events (and terrorists themselves) makes predicting their occurrence a fraught crapshoot. He says that intelligence analysts lack training data – indicative patterns of behavior drawn from observing multiple iterations of a complex event – to verify whether their models have predictive validity. "These are very, very rare events – terrorist events and terrorists themselves – that you're trying to predict. Clearly there are places where this kind of predictive activity has been very successful – fraud detection in telecommunications, for example – but there we're talking not-so-rare events." Jeff Jonas, a data scientist at IBM and senior associate at the Center for Strategic and International Studies, agrees, dismissing such terrorism prediction models as "civil liberty infringement engines." In a 2006 paper co-written by Jim Harper of the Cato Institute, Jonas asserts that sheer probability and a lack of historical data dooms counterterrorism data-mining to a quagmire of false positives. "Unless investigators can winnow their investigations down to data sets already known to reflect a high incidence of actual terrorist information," Jonas and Harper write, "the high number of false positives will render any results essentially useless." Ethical (not to mention constitutional) issues of wrongly painting people as terrorists aside, Jonas and Harper suggest that chasing down so many bogus leads only detracts from pursuing genuine ones, and thus actually hampers effective counterterrorism. In a 2006 interview with the New York Times, an FBI official confirmed the considerable waste and frustration of running down bogus tip-offs from the NSA's wiretap dragnet, joking that the endless stream of leads meant more "calls to Pizza Hut" or contacting a "school teacher with no indication they've ever been involved in international terrorism - case closed." Given enough data and fine-tuning of algorithms, of course, other experts emphasize that false positives can be reduced significantly, and insist that data-mining will play a key role in counterterrorism. Kim Taipale of the Center for Advanced Studies in Science and Technology Policy testified to this effect before the Senate Judiciary Committee in 2007, criticizing Jonas and Harper specifically for making "pseudo-technical" arguments that fail to reflect the way actual data-mining algorithms work. NSA's Utah data center. Photo courtesy NSA. And even critics admit that, with enough data to develop these training sets, analysts might be able to sift out terrorist markers. "If you can get your arms around a big enough set of data, you'll always find something in there," says Fred Cate, director of the Center for Applied Cybersecurity Research at Indiana University Law School, another contributor to the NRC report. "It's not unreasonable to think that the more data you can get access to that you might discover something of predictive value." The ease of mining personal data may make these systems ripe for abuse, but that ease also lends itself to a "better safe than sorry" mindset. "There's a certain 'because it's there' nature to this," says Cate. "If you know all these records are there, you worry about explaining why you didn't try to get access to them" to stop a terror plot. As more and more revealing information finds its way online and into commercial databases, the temptation increases for intelligence agencies to gobble up this data just in case. But the wider the net we cast—and the broader incursion on the privacy of Americans and others—the heavier the burden becomes to produce a terrorist or two. And to Cate's knowledge, despite extensive mining, the NSA has struck no such motherlode. While the government has acknowledged that these latest data surveillance programs are several years old, they have yet to trot out any concrete evidence of their efficacy. Between the NSA's dismal record, drowsy oversight from the top-secret FISA courts and vague promises from Obama, Feinstein and others that this will all be worth it someday, Washington should buckle up for plenty more "hype" from the civil libertarian set. Absent public exposure, independent oversight, and robust evaluation, it's impossible to determine whether such efforts truly have anything to throw on the scale against citizen privacy.

NSA mass surveillance results in overload

Angwin 13 (Julia, writer for WSJ, 12/25, "NSA Struggles to Make Sense of Flood of Surveillance Data,"

<http://www.wsj.com/articles/SB10001424052702304202204579252022823658850//Tang>)

William Binney, creator of some of the computer code used by the National Security Agency to snoop on Internet traffic around the world, delivered an unusual message here in September to an audience worried that the spy agency knows too much. It knows so much, he said, that it can't understand what it has. "What they are doing is making themselves dysfunctional by taking all this data," Mr. Binney said at a privacy conference here. The agency is drowning in useless data, which harms its ability to conduct legitimate surveillance, claims Mr. Binney, who rose to the civilian equivalent of a general during more than 30 years at the NSA before

retiring in 2001. Analysts are swamped with so much information that they can't do their jobs effectively, and the enormous stockpile is an irresistible temptation for misuse. Mr. Binney's warning has gotten far less attention than legal questions raised by leaks from former NSA contractor Edward Snowden about the agency's mass collection of information around the world. Those revelations unleashed a re-examination of the spy agency's aggressive tactics. MORE Snowden Warns of Dangers of Citizen Surveillance But the NSA needs more room to store all the data it collects—and new phone records, data on money transfers and other information keep pouring in. A new storage center being built in Utah will eventually be able to hold more than 100,000 times as much as the contents of printed materials in the Library of Congress, according to outside experts. Some of the documents released by Mr. Snowden detail concerns inside the NSA about drowning in information. An internal briefing document in 2012 about foreign cellphone-location tracking by the agency said the efforts were "outpacing our ability to ingest, process and store" data. In March 2013, some NSA analysts asked for permission to collect less data through a program called Muscular because the "relatively small intelligence value it contains does not justify the sheer volume of collection," another document shows. In response to questions about Mr. Binney's claims, an NSA spokeswoman says the agency is "not collecting everything, but we do need the tools to collect intelligence on foreign adversaries who wish to do harm to the nation and its allies." Existing surveillance programs were approved by "all three branches of government," and each branch "has a role in oversight," she adds. In a statement through his lawyer, Mr. Snowden says: "When your working process every morning starts with poking around a haystack of seven billion innocent lives, you're going to miss things." He adds: "We're blinding people with data we don't need." A presidential panel recommended earlier this month that the agency shut down its bulk collection of telephone-call records of all Americans. The federal government could accomplish the same goal by querying phone companies, the panel concluded. The panel also recommended the creation of "smart software" that could sort data as the information is collected, rather than the current system where "vast amounts of data are swept up and the sorting is done after it has been copied" on to data-storage systems. Administration officials are reviewing the report. A separate task force is expected to issue its own findings next year, and lawmakers have proposed several bills that would change how the NSA collects and uses data. The 70-year-old Mr. Binney says he is generally underwhelmed by the panel's "bureaucratic" report, though "it would be something meaningful if the controversy leads to adoption of the "smart software" strategy and creation of a technology oversight group with full access to "be in the knickers of the NSA" and Federal Bureau of Investigation. Mr. Binney lives off his government pension and makes occasional appearances to talk about his work at the NSA. The spy agency has defended its sweeping surveillance programs as essential in the fight against terrorism. But having too much data can hurt those efforts, according to Mr. Binney and a handful of colleagues who have raised concerns since losing an internal battle to build privacy-protecting Internet surveillance tools in the late 1990s. At the time, the agency was struggling to transform itself from a monitor of mostly analog signals, such as radio and satellite transmissions, to an effective sleuth in the emerging digital world. Diane Roark, a House Intelligence Committee staff member assigned to oversee the NSA, says she was "very disturbed" to learn in meetings at the agency's headquarters in Fort Meade, Md., in 1997 "what bad shape they were in." She saw a glimmer of hope in a corner of the NSA called the Sigin Automation Research Center. Mr. Binney, who joined the agency in 1965 with a cadre of young mathematicians hired to tackle the increasingly mathematical world of ciphers and codes, was working with the research center's chief to create an innovative approach to monitoring Internet traffic. "Our approach was to focus on the known terrorist community, which predominately existed overseas," recalls Ed Loomis, who ran the research center. "However, we were also interested in any communications they had with anyone in America." The push was legally tricky. Only the FBI is allowed to collect such information within the U.S.—and usually must prove to a judge that there is a good reason to launch surveillance. Mr. Loomis worried that the rules were too restrictive and could hinder the NSA's terrorist-catching abilities. So Messrs. Binney and Loomis built a system to scrape data from the Internet, throw away the content about U.S. citizens and zoom in on the leftover metadata—or the "to" and "from" information in Internet traffic. They called it ThinThread. To keep the data-gathering effort manageable, the two men designed ThinThread to collect data within "two hops" of a suspected bad guy. That meant the system would be built to automatically flag people who communicated with "dirty numbers" or possible terrorists—and records of people who contacted them. Messrs. Binney and Loomis also believed that ThinThread's powers should be constrained to protect the privacy of Americans. Mr. Binney designed a way to encrypt all the U.S. metadata, and their plans allowed the spy agency's analysts to unscramble the information only with permission from a warrant approved by the Foreign Intelligence Surveillance Court. The court oversees NSA activities that affect U.S. residents. ThinThread was never deployed. Agency lawyers refused to relax a ban on recording any U.S. communications. Dickie George, a senior NSA official who retired in 2011, says the consensus was that Mr. Binney's "heart was in the right place," but the technology wasn't ready. Messrs. Binney and Loomis say ThinThread could have done the job for which it was built. But Mr. Loomis was told to shut down the project. Instead, he was told, the NSA would fund a surveillance program called Trailblazer, built by outside contractors. Distraught about the decision, Messrs. Binney and Loomis and another NSA employee, Kirk Wiebe, announced plans to retire on Oct.

31, 2001. Mr. Binney reconsidered after the Sept. 11, 2001, terrorist attacks, but left as intended after hearing about new plans to use his metadata-analysis technology to hunt for terrorists. There was one big difference. The privacy protections designed to shield Americans from illegal intrusions weren't on the drawing board anymore, he says. In 2002, the three retired NSA employees and Ms. Roark asked the Defense Department's inspector general to investigate whether the decision to halt ThinThread and fund Trailblazer was made appropriately. Trailblazer's data-filtering system was never built, either. Instead, NSA officials secretly sought and won support for an array of programs to conduct warrantless wiretapping of phone and Internet content. They got similar approval to collect and analyze metadata from nearly every U.S. phone call and vast swaths of Internet traffic. Mr. Binney settled into retirement. But the spy agency's surveillance efforts began to draw more attention. In 2006, AT&T Inc. technician Mark Klein leaked documents showing that the company was working with the NSA to scour the Internet with technology that was similar to the system built by Messrs. Binney and Loomis. Outside criticism of the agency grew after articles in the New York Times and Baltimore Sun about the agency's surveillance efforts, including ThinThread. President George W. Bush briefly shut down the warrantless wiretapping program, but then parts of it were legalized by a new law passed in Congress. Meanwhile, the metadata analysis program continued in secret. Federal officials suspected the three retired NSA employees and Ms. Roark, the former House staff member, of involvement in the leaks, according to government documents. FBI agents swooped in on all four, and Mr. Binney says agents drew their guns on him while he was in the shower. A Justice Department official couldn't be reached for comment on the case. Messrs. Binney, Loomis and Wiebe and Ms. Roark weren't charged with wrongdoing, but the FBI soon pursued NSA official Thomas Drake, a ThinThread supporter. In 2010, prosecutors charged him with violating the Espionage Act, citing "willful retention" of classified documents. Mr. Drake pleaded guilty to one count of exceeding authorized use of a government computer. Mr. Drake says government officials "wanted to make an object lesson of me, drive the stake of national security right through me, and then prop me out on the public commons as punishment for holding up the mirror of their own malfeasance and usurpations of power." The raids and prosecution of Mr. Drake angered Mr. Binney. He decided to go public with his concerns. In April 2012, he spoke at an event called a "Surveillance Teach-in" at the Whitney Museum of American Art in New York. Wearing a short-sleeve, collared shirt and jeans, Mr. Binney looked like a grandfatherly professor amid the crowd of activists, some wearing Anonymous masks. "I was focused on foreign threats," he said. "Unfortunately, after 9/11, they took my solutions and directed them at this country and everybody in it." Mr. Binney's claims were hard to prove. Even Mr. Loomis, the co-creator of ThinThread, didn't think it was possible that the same NSA lawyers who refused to budge on the ban against recording any U.S. communications had approved more invasive surveillance procedures after he left the agency. "After all my struggles with those folks, I just couldn't believe that they went 180 degrees against the law," he said. In August 2012, filmmaker Laura Poitras released an eight-minute, online documentary about Mr. Binney. She called him a whistleblower. Mr. Snowden saw the video and reached out to Ms. Poitras with an avalanche of undisclosed documents, she says. Some of the documents leaked by the NSA contractor back up Mr. Binney. For example, documents detailed the agency's two clandestine metadata-surveillance programs: the bulk collection of phone-calling records and Internet traffic-analysis program. The NSA hasn't disputed the documents. The Obama administration says the Internet program was shut down in 2011, while the bulk collection of phone records still is going on. John C. Inglis, the NSA's deputy director, told lawmakers in July that the agency had court approval to do warrantless "third-hop" queries of bulk telephone records. A "third-hop" analysis of one suspected terrorist could allow the NSA to sift through the records of at least a million people. Mr. Binney says he advised NSA officials to "never go beyond two hops." He has urged lawmakers and an oversight board to limit data collection to "two hops" and establish a technical auditing team to verify the spy agency's claims about its data collection and usage. The presidential panel suggested ending the bulk collection of phone metadata entirely. Instead, phone companies should store the records and turn them over only with a court order, the panel added. President Barack Obama will decide in coming weeks which of the panel's recommendations he will implement. The recommendations aren't binding. In recent months, the retired computer-code creator has been greeted like a hero almost everywhere he goes. Mr. Snowden, living in Russia under temporary asylum, says through his lawyer that he has "tremendous respect" for Mr. Binney, "who did everything he could according to the rules."

Most recent ev

Puiu 15 – staff writer (Tibi, “The NSA is gathering so much data, it’s become swamped and ironically ineffective at preventing terrorism,” ZME Science, 5/6/2015,
<http://www.zmescience.com/research/technology/nsa-overwhelmed-data-53354/>) //RGP

One of the most famous NSA whistleblowers (or the ‘original NSA whistleblower’), William Binney, said the agency is collecting stupendous amounts of data – so much that it’s actually hampering intelligence operations. Binney worked for three decades for the intelligence agency, but left shortly after the 9/11 attacks. A program he had developed was scrapped and replaced with a system he said was more expensive and more intrusive, which made him feel he worked for an incompetent employer. Plans to enact the now controversial Patriot Act was the last straw, so he quit. Since then, Binney has frequently criticized the agency and revealed some of its operations hazards and weaknesses. Among these, he alleges: The NSA buried key intelligence that could have prevented 9/11; The agency’s bulk data collection from internet and telephone communications is unconstitutional and illegal in the US; Electronic intelligence gathering is being used for covert law

enforcement, political control and industrial espionage, both in and beyond the US; Edward Snowden's leaks could have been prevented. Ironically, Snowden cites Binney as an inspiration. His greatest insights however is that the NSA is ineffective at preventing terrorism because analysts are too swamped with information under its bulk collection programme. Considering Binney's impeccable track record – he was co-founder and director of the World Geopolitical & Military Analysis at the Signals Intelligence Automation Research Center (SARC), a branch with 6,000 employees – I can only presume he knows what he's talking about. The Patriot Act is a U.S. law passed in the wake of the September 11, 2001 terrorist attacks. Its goals are to strengthen domestic security and broaden the powers of law-enforcement agencies with regards to identifying and stopping terrorists. In effect, the law laxes the restrictions authorities have to search telephone, e-mail communications, medical, financial, and other records. Because a lot of people use web services whose servers are located in the US, this means that the records of people not located or doing business in the US are also spied upon by the NSA. All this information, however, comes at a price: overload. According to the Guardian, the NSA buffers a whooping 21 petabytes a day! In this flood of information, an NSA analyst will quickly find himself overwhelmed. Queering keywords like “bomb” or “drugs” might prove a nightmare for the analyst in question. It's impossible not to, considering four billion people — around two-thirds of the world's population — are under the NSA and partner agencies' watchful eyes, according to Binney. That's why they couldn't stop the Boston bombing, or the Paris shootings, because the data was all there,” said Binney for ZDnet. “The data was all there... the NSA is great at going back over it forensically for years to see what they were doing before that,” he said. “But that doesn't stop it.” So, according to Binney, analysts still use rudimentary tools to filter the vast amounts of information the NSA is collecting. With everybody speaking about “big data” and other such buzz phrases, it's a bit hilarious to think the NSA is actually safe guarding for terrorism by looking for needles in haystacks. “The Upstream program is where the vast bulk of the information was being collected,” said Binney, talking about how the NSA tapped undersea fiber optic cables. Basically, the NSA is collecting as much data as it can get its hands on at this point (legally or otherwise...), but it all seems too greedy for their own good, not to mention public safety. According to Binney, the fact the NSA is collecting this much data isn't to their advantage, but actually a vulnerability.

Information overload destroys system effectiveness

Mathiesen, professor of sociology of law, '13 (Thomas Mathiesen Professor of Sociology of Law at the University of Oslo, “Towards a Surveillant Society: The Rise of Surveillance Systems in Europe” Pgs 195-196, 2013, https://books.google.com/books?id=X1ZutlZgfD8C&dq=too+much+surveillance+AND+overload&source=gbs_navlinks_s) //GY

Many of the large surveillance system described earlier are not easy to use, or close to unusable, when it comes to finding terrorists in advance, whether lone wolves or groups. This goes for Eurodac, the Data Retention Directive, the various PNRs, the API, the Prum Treaty, and perhaps also for the Schengen Information System. These five or more systems face a common threat, namely what we may call information overload. There is far too much information – in all of the systems, which makes the picking out of terrorists on an individual or group basis in advance extremely difficult. The Data Retention Directive, the various PNRs and the Prum Treaty are perhaps particularly vulnerable to this. Take the Data Retention Directive. It collects all information concerning communication (except content) on all citizens in a given State. The information has to be retained for a long period of time – up to two years. Simple arithmetic tells us that the information which has to be, and is, retained, becomes colossal. Let us say that a particular State is small, and has roughly five million inhabitants (Norway is a small country, and had 4,920,300 inhabitants on 1 January 2011; we will soon have 5 million). Most inhabitants have telephones, often several mobile telephones, as well as access to the Internet and other communication technologies. Say that communication technology equals the number of inhabitants, five million for one year. This is clearly an underestimation, but roughly the average

retention period – Norway has in fact a retention period of one year. If the given State has decided on mandatory retention for two years – which is the limit – the database contains not five, but ten million technologies. However, the technology contains a large number of data entries. If the given State has decided on mandatory retention on all communication – who owns the communication technology which is used, who uses the communication technology in question, at what time does the communication begin, at what time does it end, from where is the call is taken and from where is it received, whether the caller or the called or both are moving around during the communication, to where they have moved, all of this and a number of other data entries for one year brings the database to an enormous number of millions of data entries per year. After one year the data which is stored has to be deleted. But it never ends, because a similar number of data entries are stored for each individual and for all of the five million inhabitants for another year, and another year and another year... Add to this that not only the inhabitants of this particular State are in the system, but so are all of the inhabitants of all the States of Europe (and outside States, like Norway). You end up with a fabulous number of data entries which turns the famous finding of the needle in the haystack into a reality – to say the least. For States deciding on two years of mandatory retention – the limit – the number of data entries will be doubled – even more fabulous. Many of the EU States are much larger than Norway – Great Britain had 61 million inhabitants in 2009. There are 27 large and small States in the EU. You stop counting.

Overload = nuke war

Information overload leads to a cyber crash – outweighs nuclear war

Goor, physicist and political scientist, MA Law, '13 (Dan Goor, political scientist, MA in Law and Diplomacy, “PRISM, a symptom of “information explosion,” beware!” 2013, <https://dangoor.wordpress.com/2013/07/02/prism-a-symptom-of-information-explosion-beware/> //GY

PRISM, a symptom of “information explosion,” beware!¶ While the political and security implications of leaks by Edward Snowden are monopolizing the news, the main danger is from information overload, misinterpretations and perhaps dangerous (or even rogue) action could be the main issue.¶ Too much information leads to chaos, In the mid fifteen hundreds, Miguel de Cervantes Saavedra predicted that too much information will drive people insane by demonstrating how his hero, Don Quixote, went mad because he read too much. Albert Einstein said the: “I fear the day when the [information] technology overlaps with our humanity; the world will only have a generation of idiots.”¶ In George Orwell’s 1984 he wrote of government that has total visibility to what every person does, and soon we shall be able to read people’s minds, to know what thoughts each person may have.¶ Communication is a complex process, which land itself to high level of misinterpretations. With Government monitoring everything its citizenry does, and take action based on interpretation by both man and machine, one can expect an eventual state of chaos in the world.¶ This year NSA’s one and one half million square foot facility in Utah would become operational, it would accommodate the trillions of bits of information that NSA is gathering from the United States and from around the world. Following is Wikipedia overview of the NSA facility:¶ “The Utah Data Center, also known as the Intelligence Community Comprehensive National Cybersecurity Initiative Data Center,[1] is a data storage facility for the United States Intelligence Community that is designed to store extremely large amounts of data.[2][3][4] Its purpose is to support the Comprehensive National Cybersecurity Initiative (CNCI), though its precise mission is classified.[5] The National Security Agency (NSA), which will lead operations at the facility, is the executive agent for the Director of National Intelligence.[6] It is located at Camp Williams, near Bluffdale, Utah, between Utah Lake and Great Salt Lake.”¶ The Google information about judicial requests from various countries supports the notion that the world is moving towards an information overload, the world is leading towards a “cyber crash,” that could well dwarf any nuclear confrontation that may confront the human race.¶ Should, or could, safeguards be put in place to prevent information from going wild?¶ Several years ago when Gordon Moore of Intel predicted that every few years computation power would double, an alarm should have sounded. Moore was close to correct, except that information technology is growing even faster and could become an avalanche out of control.¶ It is likely that the human race will survive the “cyber explosion,” just as it survived Malthus prediction of resource shortage, of atomic annihilation. That notwithstanding, the prudent thing for both scientists and politicians to exercise some rational control on information growth.

Iran !

Overload causes Iran war Trobock, 14

Randall Trubbock, Master of Science in Cybersecurity from Utica College, May 2014, “The Application Of Splunk In The Intelligence Gathering Process,” Proquest // is amp

Faulty intelligence methods, such as those that would be the result of **information overload**, pose a **significant threat** to peace throughout the world. For example, having inaccurate or incomplete intelligence on Iran’s nuclear capabilities and the locations or nature of its nuclear plants, a risk-averse Israel might overestimate its need to take both drastic and pre-emptive measures against Iran (Young, 2013). This could result in involvement from several countries, including the United States, potentially costing billions of dollars and thousands of soldiers’ lives.

Turns off – drones

Despite a plethora of surveillance technology border surveillance fails due to data overload

Abrams and Cyphers No date (David, Chief Technology Officer, True Systems, Dennis, VP Sales Operations, “TrueSentry Border Surveillance”, http://www.daveab.com/files/TrueSentry_Border_Surveillance.pdf//Tang)

BORDER SECURITY remains a key homeland security challenge. Border guards, surveillance operators, and command staff do not have an integrated command and control system to protect national borders. There is a lack of sufficient coverage from sensors and cameras. Important threats are lost in an overload of information from false alarms. The collaboration and communications needed for tactical intercept missions is lacking. Wide and diverse terrain coupled with large-scale population centers, sea ports, and national boundaries make a difficult environment to effectively scale-up border surveillance. Far-field cameras, thermal vision, and pan/tilt/zoom cameras are used to remotely monitor border zones. Unmanned aerial vehicles (UAVs) fly continuous GPS-guided missions to give operators a bird's eye view. Surveillance towers typically use radar as a cost-effective way to get broad sensor coverage of diverse border zone terrain. Intrusion detection systems like underground buried cables are used to monitor electromagnetic field changes to distinguish between people, vehicles and animals at a perimeter. Outdoor motion detection is also done with microwave and infrared sensors. Intelligent pressure fence sensors detect when intruders climb or cut a fence-line. Yet for all these advances in surveillance equipment we are still left with border guards struggling with high false alarm rates and low probability of detection and intercept. There are just too many cameras and not enough border forces to monitor them all. Threats are lost because of too many false alarms. The cost of verifying targets, escalating them into threats, and dispatching response teams is too high. Intercept mission teams do not have effective collaboration tools. Intelligence and threat pattern analysis is just too time consuming to thwart the next intrusion.

Border drones are ineffective and costly

Bennet 1/7 (Brian, reporter for the LA Times, 1/7/15, “Border drones are ineffective, badly managed, too expensive, official says”, <http://www.latimes.com/nation/immigration/la-na-border-drones-20150107-story.html>//Tang)

Drones patrolling the U.S. border are poorly managed and ineffective at stopping illegal immigration, and the government should abandon a \$400-million plan to expand their use, according to an internal watchdog report released Tuesday. The 8-year-old drone program has cost more than expected, according to a report by the Department of Homeland Security's inspector general, John Roth. Rather than spend more on drones, the department should "put those funds to better use." Roth recommended. He described the Predator B drones flown along the border by U.S. Customs and Border Protection as "dubious achievers." "Notwithstanding the significant investment, we see no evidence that the drones contribute to a more secure border, and there is no reason to invest additional taxpayer funds at this time." Roth said in a statement. The audit concluded that Customs and Border Protection could better use the funds on manned aircraft and ground surveillance technology. The drones were designed to fly over the border to spot smugglers and illegal border crossers. But auditors found that 78% of the time that agents had planned to use the craft, they were grounded because of bad weather, budget constraints or maintenance problems. Even when aloft, auditors found, the drones contributed little. Three drones flying around the Tucson area helped apprehend about 2,200 people illegally crossing the border in 2013, fewer than 2% of the 120,939 apprehended that year in the area. Border Patrol supervisors had planned on using drones to inspect ground-sensor alerts. But a drone was used in that scenario only six times in 2013. Auditors found that officials

underestimated the cost of the drones by leaving out operating costs such as pilot salaries, equipment and overhead. Adding such items increased the flying cost nearly fivefold, to \$12,255 per hour. People think these kinds of surveillance technologies will be a silver bullet. Time after time, we see the practical realities of these systems don't live up to the hype. - Jay Stanley, ACLU privacy expert "It really doesn't feel like [Customs and Border Protection] has a good handle on how it is using its drones, how much it costs to operate the drones, where that money is coming from or whether it is meeting any of its performance metrics," said Jennifer Lynch, a lawyer for the Electronic Frontier Foundation, a San Francisco-based privacy and digital rights group. The report's conclusions will make it harder for officials to justify further investment in the border surveillance drones, especially at a time when Homeland Security's budget is at the center of the battle over President Obama's program to give work permits to millions of immigrants in the country illegally. Each Predator B system costs about \$20 million. "People think these kinds of surveillance technologies will be a silver bullet," said Jay Stanley, a privacy expert at the American Civil Liberties Union. "Time after time, we see the practical realities of these systems don't live up to the hype." Customs and Border Protection, which is part of Homeland Security, operates the fleet of nine long-range Predator B drones from bases in Arizona, Texas and North Dakota. The agency purchased 11 drones, but one crashed in Arizona in 2006 and another fell into the Pacific Ocean off San Diego after a mechanical failure last year. Agency officials said in response to the audit that they had no plans to expand the fleet aside from replacing the Predator that crashed last year. The agency is authorized to spend an additional \$433 million to buy up to 14 more drones. The drones — unarmed versions of the MQ-9 Reaper drone flown by the Air Force to hunt targets in Pakistan, Somalia and elsewhere — fly the vast majority of their missions in narrowly defined sections of the Southwest border, the audit found. They spent most of their time along 100 miles of border in Arizona near Tucson and 70 miles of border in Texas. Rep. Henry Cuellar (D-Texas) has promoted the use of drones along the border but believes the agency should improve how it measures their effectiveness. Homeland Security "can't prove the program is effective because they don't have the right measures," Cuellar said in an interview. "The technology is good, but how you implement and use it — that is another question." The audit also said that drones had been flown to help the FBI, the Texas Department of Public Safety and the Minnesota Department of Natural Resources. Such missions have long frustrated Border Patrol agents, who complain that drones and other aircraft aren't available when they need them, said Shawn Moran, vice president of the Border Patrol agents' union. "We saw the drones were being lent out to many entities for nonborder-related operations and we said, 'These drones, if they belong to [Customs and Border Protection], should be used to support [its] operations primarily,'" Moran said.

Turns off – generic

Additional surveillance directly trades off with security concerns – the more information we have the less effective counter terror measures are

Greenwald 10 (Glenn, constitutional lawyer, 8/9, “The Digital Surveillance State: Vast, Secret, and Dangerous”, <http://www.cato-unbound.org/2010/08/09/glenn-greenwald/digital-surveillance-state-vast-secret-dangerous//Tang>)

What makes this leviathan particularly odious is that it does not even supply the security which is endlessly invoked to justify it. It actually does the opposite. As many surveillance experts have repeatedly argued, including House Intelligence Committee member Rush Holt, the more secret surveillance powers we vest in the government, the more unsafe we become. Cato’s Julian Sanchez put it this way: “We’ve gotten so used to the ‘privacy/security tradeoff’ that it’s worth reminding ourselves, every now and again, that surrendering privacy does not automatically make us more secure—that systems of surveillance can themselves be a major source of insecurity.” That’s because the Surveillance State already collects so much information about us, our activities and our communications—so indiscriminately and on such a vast scale—that it is increasingly difficult for it to detect any actual national security threats. NSA whistle blower Adrienne Kinne, when exposing NSA eavesdropping abuses, warned of what ABC News described as “the waste of time spent listening to innocent Americans, instead of looking for the terrorist needle in the haystack.” As Kinne explained: By casting the net so wide and continuing to collect on Americans and aid organizations, it’s almost like they’re making the haystack bigger and it’s harder to find that piece of information that might actually be useful to somebody. You’re actually hurting our ability to effectively protect our national security. As the Post put it in its “Top Secret America” series: The NSA sorts a fraction of those [1.7 billion e-mails, phone calls and other types of daily collected communications] into 70 separate databases. The same problem bedevils every other intelligence agency, none of which have enough analysts and translators for all this work. That article details how ample information regarding alleged Ft. Hood shooter Nidal Hassan and attempted Christmas Day bomber Umar Abdulmutallab was collected but simply went unrecognized. Similarly, The Washington Post’s David Ignatius previously reported that Abdulmutallab was not placed on a no-fly list despite ample evidence of his terrorism connections because information overload “clogged” the surveillance system and prevented its being processed. Identically, Newsweek’s Mike Isikoff and Mark Hosenball documented that U.S. intelligence agencies intercept, gather and store so many emails, recorded telephone calls, and other communications that it’s simply impossible to sort through or understand what they have, quite possibly causing them to have missed crucial evidence in their possession about both the Fort Hood and Abdulmutallab plots: This deluge of Internet traffic—involving e-mailers whose true identity often is not apparent—is one indication of the volume of raw intelligence U.S. spy agencies have had to sort through . . . The large volume of messages also may help to explain how agencies can become so overwhelmed with data that sometimes it is difficult, if not impossible, to connect potentially important dots. As a result, our vaunted Surveillance State failed to stop the former attack and it was only an alert airplane passenger who thwarted the latter. So it isn’t that we keep sacrificing our privacy to an always-growing National Security State in exchange for greater security. The opposite is true: we keep sacrificing our privacy to the always-growing National Security State in exchange for less security.

Info overload will collapse the surveillance state

North 13 (Gary, American Christian Reconstructionist theorist and economic historian. 7/29, “Surveillance state will collapse; data overload increasingly blinds it”, <http://nooganomics.com/2013/07/surveillance-state-will-collapse-data-overload-increasingly-blinds-it//Tang>)

Wyden trusts in the wisdom and power of political democracy. He is naive. He should trust in the free market. People’s day-to-day economic decisions are the heart of the matter, not their occasional voting. The individual decisions of people in the market will ultimately thwart Congress and the surveillance state. The free market’s signals, not the phone

taps of the NSA, will shape the future. The bureaucrats' quest for omniscience and omnipotence will come to a well-deserved end, just as it did in the Soviet Union, and for the same reason. The state is inherently myopic: short-sighted. Computers make it blind. The state focuses on the short run. Computers overwhelm bureaucrats with short-run information. Let us not forget that the Internet was invented by DARPA: the military's research branch. It invented the Internet to protect the military's communications network from a nuclear attack by the USSR. Today, there is no USSR. There is the World Wide Web: the greatest technological enemy of the state since Gutenberg's printing press. The state is myopic. The fact that the NSA's two "computer farms" — in Utah and in Maryland — are seven times larger than the Pentagon will not change this fact. They have bitten off more than they can chew. Central planners are bureaucrats, and bureaucracy is blind. It cannot assess accurately the importance of the mountains of data that are hidden in government-collected and program-assessed digits. The knowledge possessed in the free market is always more relevant. Society is the result of human action, not of human design. The bureaucrats do not understand this principle, and even if they did, it would not change reality.

Turns aff - NCTC

The size of the NCTC should be reduced to more effectively combat terrorism

Storm 13 (Darlene, freelance writer, citing Bridget Nolan, sociology phd, worked as a CT analyst at the NCTC, 8/7 “Is US intelligence so big that counterterrorism is failing? ‘Yes’ say insiders”, <http://www.computerworld.com/article/2475096/security0/is-us-intelligence-so-big-that-counterterrorism-is-failing---yes--say-insiders.html//Tang>)

When might you consider quitting your job to be a “win”? When you work for the CIA and “the Company” tries to block the publication of your dissertation about the National Counterterrorism Center. Bridget Rose Nolan, a sociology PhD at the University of Pennsylvania, worked as a counterterrorism analyst at the National Counterterrorism Center (NCTC) from 2010 – 2011. Basically she worked as an analyst while also conducting “ethnographic observations” by interviewing 16 female and seven male analysts for her doctoral dissertation at the University of Pennsylvania. The Philadelphia Inquirer explained, “She set out to explore the culture of the terrorism center and how it, and its counterparts, share information – or fail to.” After three years of “fighting” the CIA over the right to publish, she won, but the “win” meant she had to resign. Instead of too big to fail, in essence, counterterrorism may be failing in some areas because it is too big, because counterterrorism analysts suffer from so much information overload that they are not effective in stopping terrorism. Fewer people in the system could help to streamline the bureaucracy and reduce the number of emails and documents that make the analysts feel overwhelmed with information. Other contributing factors that make terrorism harder to fight include sabotage among co-workers, stove-piping, confusion, bureaucracy that might make your head explode, and agencies that don’t play well together. Several people working in counterterrorism suggested that the solutions to be more effective include cutting out the bloat and making the intelligence community smaller, much smaller. NCTC was formed as a “knee-jerk reaction to 9/11.” The continuing War on Terror leads to more databases, more information which creates more stove-piping. There is no Google-like search to find information from one agency to the other, and each intelligence agency hoards the good secret stuff for itself. One analyst suggested that NCTC was “never intended to be real. That all along, it’s just been a CYA [‘cover your ass’] political maneuver.” Another CT analyst suggested that if NCTC were to continue, then it “should be about one-tenth its current size.” When it comes to intelligence information, analysts must “publish or perish;” but it’s more about quantity than quality. There are endless “turf battles” complete with paper ownership battles as well as “strategies of deception and sabotage.” Even analysts working for the same agency might try to stall in order to “scoop” another analyst, they also might try to “kill” the piece. That’s before the six months to two years for official reviews of the papers, “layers and layers of soul-crushing review.” There is also “a lack of faith in management both as qualified reviewers and as unbiased supporters.” One analyst said, “Information sharing is when YOU give ME your data.”

Turns aff – NSA

NSA failing now – their drowning in information – only the plan makes surveillance effective

Angwin 13 – staff writer (“NSA Struggles to Make Sense of Flood of Surveillance Data,” WSJ, 12/25/2013, <http://www.wsj.com/articles/SB10001424052702304202204579252022823658850>) //RGP

*Language edited

LAUSANNE, Switzerland— William Binney, creator of some of the computer code used by the National Security Agency to snoop on Internet traffic around the world, delivered an unusual message here in September to an audience worried that the spy agency knows too much. It knows so much, he said, that it can't understand what it has. “What they are doing is making themselves dysfunctional by taking all this data,” Mr. Binney said at a privacy conference here. The agency is drowning in useless data, which harms its ability to conduct legitimate surveillance, claims Mr. Binney, who rose to the civilian equivalent of a general during more than 30 years at the NSA before retiring in 2001. Analysts are swamped with so much information that they can't do their jobs effectively, and the enormous stockpile is an irresistible temptation for misuse. Mr. Binney's warning has gotten far less attention than legal questions raised by leaks from former NSA contractor Edward Snowden about the agency's mass collection of information around the world. Those revelations unleashed a re-examination of the spy agency's aggressive tactics. MORE Snowden Warns of Dangers of Citizen Surveillance But the NSA needs more room to store all the data it collects—and new phone records, data on money transfers and other information keep pouring in. A new storage center being built in Utah will eventually be able to hold more than 100,000 times as much as the contents of printed materials in the Library of Congress, according to outside experts. Some of the documents released by Mr. Snowden detail concerns inside the NSA about drowning in information. An internal briefing document in 2012 about foreign cellphone-location tracking by the agency said the efforts were "outpacing our ability to ingest, process and store" data. In March 2013, some NSA analysts asked for permission to collect less data through a program called Muscular because the “relatively small intelligence value it contains does not justify the sheer volume of collection,” another document shows. In response to questions about Mr. Binney's claims, an NSA spokeswoman says the agency is “not collecting everything, but we do need the tools to collect intelligence on foreign adversaries who wish to do harm to the nation and its allies.” Existing surveillance programs were approved by “all three branches of government,” and each branch “has a role in oversight,” she adds. In a statement through his lawyer, Mr. Snowden says: “When your working process every morning starts with poking around a haystack of seven billion innocent lives, you're going to miss things.” He adds: “We're blinding [overwhelming] people with data we don't need.”

Status quo NSA operations are ineffective due to information overload – makes preventing terrorism impossssible

Maass, acclaimed author and journalist on surveillance, 5/28 (PETER MAASS “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE” 05/28/2015 11:38 AM <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/>) //GY

AS MEMBERS OF CONGRESS struggle to agree on which surveillance programs to re-authorize before the Patriot Act expires, they might consider the unusual advice of an intelligence analyst at the National Security Agency who warned about the danger of collecting too much data. Imagine, the analyst wrote in a leaked document, that you are standing in a shopping aisle trying to decide between jam, jelly or fruit spread, which size, sugar-free or not, generic or Smucker's. It can be paralyzing. “We in the agency are at risk of a similar, collective paralysis in the face of a dizzying array of choices every single day,” the analyst wrote in 2011. “‘Analysis paralysis’ isn’t only a cute rhyme. It’s the term for what happens when you spend so much time

analyzing a situation that you ultimately stymie any outcome It's what happens in SIGINT [signals intelligence] when we have access to endless possibilities, but we struggle to prioritize, narrow, and exploit the best ones."¶ The document is one of about a dozen in which NSA intelligence experts express concerns usually heard from the agency's critics: that the U.S. government's "collect it all" strategy can undermine the effort to fight terrorism. The documents, provided to The Intercept by NSA whistleblower Edward Snowden, appear to contradict years of statements from senior officials who have claimed that pervasive surveillance of global communications helps the government identify terrorists before they strike or quickly find them after an attack.¶ The Patriot Act, portions of which expire on Sunday, has been used since 2001 to conduct a number of dragnet surveillance programs, including the bulk collection of phone metadata from American companies. But the documents suggest that analysts at the NSA have drowned in data since 9/11, making it more difficult for them to find the real threats. The titles of the documents capture their overall message: "Data Is Not Intelligence," "The Fallacies Behind the Scenes," "Cognitive Overflow?" "Summit Fever" and "In Praise of Not Knowing." Other titles include "Dealing With a 'Tsunami' of Intercept" and "Overcome by Overload?"¶ The documents are not uniform in their positions. Some acknowledge the overload problem but say the agency is adjusting well. They do not specifically mention the Patriot Act, just the larger dilemma of cutting through a flood of incoming data. But in an apparent sign of the scale of the problem, the documents confirm that the NSA even has a special category of programs that is called "Coping With Information Overload."¶ The jam vs. jelly document, titled "Too Many Choices," started off in a colorful way but ended with a fairly stark warning: "The SIGINT mission is far too vital to unnecessarily expand the haystacks while we search for the needles. Prioritization is key."¶ These doubts are infrequently heard from officials inside the NSA. These documents are a window into the private thinking of mid-level officials who are almost never permitted to discuss their concerns in public.¶ AN AMUSING PARABLE circulated at the NSA a few years ago. Two people go to a farm and purchase a truckload of melons for a dollar each. They then sell the melons along a busy road for the same price, a dollar. As they drive back to the farm for another load, they realize they aren't making a profit, so one of them suggests, "Do you think we need a bigger truck?"¶ The parable was written by an intelligence analyst in a document dated Jan. 23, 2012 that was titled, "Do We Need a Bigger SIGINT Truck?" It expresses, in a lively fashion, a critique of the agency's effort to collect what former NSA Director Keith Alexander referred to as "the whole haystack." The critique goes to the heart of the agency's drive to gather as much of the world's communications as possible: because it may not find what it needs in a partial haystack of data, the haystack is expanded as much as possible, on the assumption that more data will eventually yield useful information. The Snowden files show that in practice, it doesn't turn out that way: more is not necessarily better, and in fact, extreme volume creates its own challenges.¶ "Recently I tried to answer what seemed like a relatively straightforward question about which telephony metadata collection capabilities are the most important in case we need to shut something off when the metadata coffers get full," wrote the intelligence analyst. "By the end of the day, I felt like capitulating with the white flag of, 'We need COLOSSAL data storage so we don't have to worry about it,' (aka we need a bigger SIGINT truck)." The analyst added, "Without metrics, how do we know that we have improved something or made it worse? There's a running joke ... that we'll only know if collection is important by shutting it off and seeing if someone screams."¶ Another document, while not mentioning the dangers of collecting too much data, expressed concerns about pursuing entrenched but unproductive programs.¶ "How many times have you been watching a terrible movie, only to convince yourself to stick it out to the end and find out what happens, since you've

already invested too much time or money to simply walk away?" the document asked. "This 'gone too far to stop now' mentality is our built-in mechanism to help us allocate and ration resources. However, it can work to our detriment in prioritizing and deciding which projects or efforts are worth further expenditure of resources, regardless of how much has already been 'sunk.' As has been said before, insanity is doing the same thing over and over and expecting different results." Many of these documents were written by intelligence analysts who had regular columns distributed on NSANet, the agency's intranet. One of the columns was called "Signal v. Noise," another was called "The SIGINT Philosopher." Two of the documents cite the academic work of Herbert Simon, who won a Nobel Prize for his pioneering research on what's become known as the attention economy. Simon wrote that consumers and managers have trouble making smart choices because their exposure to more information decreases their ability to understand the information. Both documents mention the same passage from Simon's essay, Designing Organizations for an Information-Rich World: "In an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it." In addition to consulting Nobel-prize winning work, NSA analysts have turned to easier literature, such as Malcolm Gladwell's best-selling Blink: The Power of Thinking Without Thinking. The author of a 2011 document referenced Blink and stated, "The key to good decision making is not knowledge. It is understanding. We are swimming in the former. We are desperately lacking in the latter." The author added, "Gladwell has captured one of the biggest challenges facing SID today. Our costs associated with this information overload are not only financial, such as the need to build data warehouses large enough to store the mountain of data that arrives at our doorstep each day, but also include the more intangible costs of too much data to review, process, translate and report." Alexander, the NSA director from 2005 to 2014 and chief proponent of the agency's "collect it all" strategy, vigorously defended the bulk collection programs. "What we have, from my perspective, is a reasonable approach on how we can defend our nation and protect our civil liberties and privacy," he said at a security conference in Aspen in 2013. He added, "You need the haystack to find the needle." The same point has been made by other officials, including James Cole, the former deputy attorney general who told a congressional committee in 2013, "If you're looking for the needle in the haystack, you have to have the entire haystack to look through." The opposing viewpoint was voiced earlier this month by Snowden, who noted in an interview with the Guardian that the men who committed recent terrorist attacks in France, Canada and Australia were under surveillance—their data was in the haystack yet they weren't singled out. "It wasn't the fact that we weren't watching people or not," Snowden said. "It was the fact that we were watching people so much that we did not understand what we had. The problem is that when you collect it all, when you monitor everyone, you understand nothing." In a 2011 interview with SIDtoday, a deputy director in the Signals Intelligence Directorate was asked about "analytic modernization" at the agency. His response, while positive on the NSA's ability to surmount obstacles, noted that it faced difficulties, including the fact that some targets use encryption and switch phone numbers to avoid detection. He pointed to volume as a particular problem. "We live in an Information Age when we have massive reserves of information and don't have the capability to exploit it," he stated. "I was told that there are 2 petabytes of data in the SIGINT System at any given time. How much is that? That's equal to 20 million 4-drawer filing cabinets. How many cabinets per analyst is that? By the end of this year, we'll have 1 terabyte of data per second coming in. You can't crank that through the existing processes and be

effective.”¶ The documents noted the difficulty of sifting through the ever-growing haystack of data. For instance, a 2011 document titled “ELINT Analysts – Overcome by Overload? Help is Here with IM&S” outlined a half dozen computer tools that “are designed to invert the paradigm where an analyst spends more time searching for data than analyzing it.” Another document, written by an intelligence analyst in 2010, bluntly stated that “we are drowning in information. And yet we know nothing. For sure.” The analyst went on to ask, “Anyone know just how many tools are available at the Agency, alone? Would you know where to go to find out? Anyone ever start a new target...without the first clue where to begin? Did you ever start a project wondering if you were the sole person in the Intelligence Community to work this project? How would you find out?” The analyst, trying to encourage more sharing of tips about the best ways to find data in the haystack, concluded by writing, in boldface, “Don’t let those coming behind you suffer the way you have.”¶

Overload makes surveillance ineffective and infringes on civil rights

Ward, journalist, 5/18 (Stan Ward, correspondent for Best VPN ‘NSA swamped with data overload also trashes the Constitution’ 18 May 2015 <https://www.bestvpn.com/blog/19187/nsa-swamped-with-data-overload-also-trashes-the-constitution/>) //GY

Almost on the second anniversary of the Edward Snowden revelations, another (in)famous NSA whistleblower has again spoken up. This comes at a pivotal juncture in the legislative calendar as contentious debate about surveillance rages over the impending sunset of some of the Patriot Act.¶ It has long been an argument of the civil liberties crowd that bulk data gathering was counter-productive, if not counter-intuitive. The argument was couched in language suggesting that to “collect it all”, as the then NSA director James Clapper famously decried, was to, in effect, gather nothing, as the choking amounts of information collected would be so great as to be unable to be analyzed effectively.¶ This assertion is supported by William Binney, a founder of Contrast Security and a former NSA official, logging more than three decades at the agency. In alluding to what he termed “bulk data failure”, Binney said that an analyst today can run one simple query across the NSA’s various databases, only to become immediately overloaded with information.¶ With about four billion people (around two-thirds of the world’s population) under the NSA and partner agencies’ watchful eyes, according to his estimates, there is far too much data being collected.¶ “That’s why they couldn’t stop the Boston bombing, or the Paris shootings, because the data was all there... The data was all there... the NSA is great at going back over it forensically for years to see what they were doing before that. But that doesn’t stop it.”¶ Binney is in a position to know, earning his stripes during the terrorism build up that culminated with the 9/11 World Trade Center bombing in 2001. He left just days after the draconian legislation known as the USA Patriot Act was enacted by Congress on the heels of that attack. One of the reasons which prompted his leaving was the scrapping of a surveillance system on which he long worked, only to be replaced by more intrusive systems.¶ It is interesting to note here that Edward Snowden, in alluding to Binney, said he was inspired by Binney’s plight, and that this, in part, prodded him to leak thousands of classified documents to journalists. Little did Binney know that his work was to be but the tip of the iceberg in a program that eventually grew to indiscriminately “collect it all.”¶ What is worrisome is the complicity with the bulk data collection by dozens of private companies – maybe as many as 72. Yet this type of collection pales in comparison to that of the “Upstream” program in which the NSA tapped into undersea fiber optic cables. With the cooperation of Britain’s GCHQ, the NSA is able to sift more than 21 petabytes a day.¶ Gathering such enormous amounts of information is expensive and ineffective, according to Binney. But it gets lawmakers attention in a way that results in massive increases in NSA budgets. Binney warns

that, ¶ “They’re taking away half of the Constitution in secret.” ¶ President Obama has presided over this agency’s land grab, and has endorsed it, often referring to Upstream as a “critical national security tool.” His feckless approach to the spying build up is the reason for its proliferation, and is why Congress meanders rudderless in attempts to curtail it. ¶ The President’s anti-privacy stance is being “rewarded” by repudiation among members of his own party, and is reflected in their rejecting his latest legacy-building, pet piece of legislation – the Trans Pacific Partnership (TPP). But their constituents would be better served by producing legislation that would restore Constitutional rights trampled on by the NSA.

Turns off – NSA – grid collapse

Strain on surveillance systems threatens power disruptions – collapses the agency

Gorman, '06 (SIOBHAN GORMAN, senior reporter Baltimore Sun "NSA risking electrical overload" August 06, 2006 http://articles.baltimoresun.com/2006-08-06/news/0608060158_1_agency-power-surges-nsa/3) //GY

WASHINGTON -- The National Security Agency is running out of juice. The demand for electricity to operate its expanding intelligence systems has left the high-tech eavesdropping agency on the verge of exceeding its power supply, the lifeblood of its sprawling 350-acre Fort Meade headquarters, according to current and former intelligence officials. Agency officials anticipated the problem nearly a decade ago as they looked ahead at the technology needs of the agency, sources said, but it was never made a priority, and now the agency's ability to keep its operations going is threatened. The NSA is already unable to install some costly and sophisticated new equipment, including two new supercomputers, for fear of blowing out the electrical infrastructure, they said. At minimum, the problem could produce disruptions leading to outages and power surges at the Fort Meade headquarters, hampering the work of intelligence analysts and damaging equipment, they said. At worst, it could force a virtual shutdown of the agency, paralyzing the intelligence operation, erasing crucial intelligence data and causing irreparable damage to computer systems -- all detrimental to the fight against terrorism. Estimates on how long the agency has to stave off such an overload vary from just two months to less than two years. NSA officials "claim they will not be able to operate more than a month or two longer unless something is done," said a former senior NSA official familiar with the problem, who spoke on condition of anonymity. Agency leaders, meanwhile, are scrambling for stopgap measures to buy time while they develop a sustainable plan. Limitations of the electrical infrastructure in the main NSA complex and the substation serving the agency, along with growing demand in the region, prevent an immediate fix, according to current and former government officials. "If there's a major power failure out there, any backup systems would be inadequate to power the whole facility," said Michael Jacobs, who headed the NSA's information assurance division until 2002. "It's obviously worrisome, particularly on days like today," he said in an interview during last week's barrage of triple-digit temperatures. William Nolte, a former NSA executive who spent decades with the agency, said power disruptions would severely hamper the agency. "You've got an awfully big computer plant and a lot of precision equipment, and I don't think they would handle power surges and the like really well," he said. "Even re-calibrating equipment would be really time consuming -- with lost opportunities and lost up-time." Power surges can also wipe out analysts' hard drives, said Matthew Aid, a former NSA analyst who is writing a multivolume history of the agency. The information on those hard drives is so valuable that many NSA employees remove them from their computers and lock them in a safe when they leave each day, he said. A half-dozen current and former government officials knowledgeable about the energy problem discussed it with The Sun on condition of anonymity because of the sensitivity of the issue. NSA spokesman Don Weber declined to comment on specifics about the NSA's power needs or what is being done to address them, saying that even private companies consider such information proprietary. In a statement to The Sun, he said that "as new technologies become available, the demand for power increases and NSA must determine the best and most economical way to use our existing power and bring on additional capacity." Biggest BGE customer. The NSA is Baltimore Gas & Electric's largest customer, using

as much electricity as the city of Annapolis, according to James Bamford, an intelligence expert and author of two comprehensive books on the agency.¹ BGE spokeswoman Linda Foy acknowledged a power company project to deal with the rising energy demand at the NSA, but she referred questions about it to the NSA.² The agency got a taste of the potential for trouble Jan. 24, 2000, when an information overload, rather than a power shortage, caused the NSA's first-ever network crash. It took the agency 3 1/2 days to resume operations, but with a power outage it could take considerably longer to get the NSA humming again.³ The 2000 shutdown rendered the agency's headquarters "brain-dead," as then-NSA Director Gen. Michael V. Hayden told CBS's 60 Minutes in 2002.⁴ "I don't want to trivialize this. This was really bad," Hayden said. "We were dark. Our ability to process information was gone."⁵ As an immediate fallback measure, the NSA sent its incoming data to its counterpart in Great Britain, which stepped up efforts to process the NSA's information along with its own, said Bamford.⁶ The agency came under intense criticism from members of Congress after the crash, and the incident rapidly accelerated efforts to modernize the agency.⁷ One former NSA official familiar with the electricity problem noted a sense of déjà vu six years later. "To think that this was not a priority probably tells you more about the extent to which NSA has actually transformed," the former official said. "In the end, if you don't have power, you can't do [anything]."⁸ Already some equipment is not being sufficiently cooled, and agency leaders have forgone plugging in some new machinery, current and former government officials said. The power shortage will also delay the installation of two new, multimillion-dollar supercomputers, they said.⁹ To begin to alleviate pressure on the electrical grid, the NSA is considering buying additional generators and shutting down so-called "legacy" computer systems that are decades old and not considered crucial to the agency's operations, said three current and former government officials familiar with the situation.¹⁰

Turns aff – UPSTREAM

Information collected by UPSTREAM is ineffective and counterproductive – causes info overload which makes terror attacks less likely to be detected

Whittaker 4/30 (Zach, writer-editor for ZDNet, and sister sites CNET and CBS News., 4/30/15, “NSA is so overwhelmed with data, it's no longer effective, says whistleblower,” <http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective//Tang>)

A former National Security Agency official turned whistleblower has spent almost a decade and a half in civilian life. And he says he's still "pissed" by what he's seen leak in the past two years. In a lunch meeting hosted by Contrast Security founder Jeff Williams on Wednesday, William Binney, a former NSA official who spent more than three decades at the agency, said the US government's mass surveillance programs have become so engorged with data that they are no longer effective, losing vital intelligence in the fray. That, he said, can -- and has -- led to terrorist attacks succeeding. As the Snowden leaks began, there was "fear and panic" in Congress Just a few minutes after the first NSA leak was published, the phones of US lawmakers began to buzz, hours before most of America would find out over their morning coffee. Binney said that an analyst today can run one simple query across the NSA's various databases, only to become immediately overloaded with information. With about four billion people -- around two-thirds of the world's population -- under the NSA and partner agencies' watchful eyes, according to his estimates, there is too much data being collected. "That's why they couldn't stop the Boston bombing, or the Paris shootings, because the data was all there," said Binney. Because the agency isn't carefully and methodically setting its tools up for smart data collection, that leaves analysts to search for a needle in a haystack. "The data was all there... the NSA is great at going back over it forensically for years to see what they were doing before that," he said. "But that doesn't stop it." Binney called this a "bulk data failure" -- in that the NSA programs, leaked by Edward Snowden, are collecting too much for the agency to process. He said the problem runs deeper across law enforcement and other federal agencies, like the FBI, the CIA, and the Drug Enforcement Administration (DEA), which all have access to NSA intelligence. Binney left the NSA a month after the September 11 attacks in New York City in 2001, days after controversial counter-terrorism legislation was enacted -- the Patriot Act -- in the wake of the attacks. Binney stands jaded by his experience leaving the shadowy eavesdropping agency, but impassioned for the job he once had. He left after a program he helped develop was scrapped three weeks prior to September 11, replaced by a system he said was more expensive and more intrusive. Snowden said he was inspired by Binney's case, which in part inspired him to leak thousands of classified documents to journalists. Since then, the NSA has ramped up its intelligence gathering mission to indiscriminately "collect it all." Binney said the NSA is today not as interested in phone records -- such as who calls whom, when, and for how long. Although the Obama administration calls the program a "critical national security tool," the agency is increasingly looking at the content of communications, as the Snowden disclosures have shown. Binney said he estimated that a "maximum" of 72 companies were participating in the bulk records collection program -- including Verizon, but said it was a drop in the ocean. He also called PRISM, the clandestine surveillance program that grabs data from nine named Silicon Valley giants, including Apple, Google, Facebook, and Microsoft, just a "minor part" of the data collection process. The Upstream program is where the vast bulk of the information was being collected, said Binney, talking about how the NSA tapped undersea fiber optic cables. With help from its British counterparts at GCHQ, the NSA is able to "buffer" more than 21 petabytes a day. Binney said the "collect it all" mantra now may be the norm, but it's expensive and ineffective. "If you have to collect everything, there's an ever increasing need for more and more budget," he said. "That means you can build your empire." They say you never leave the intelligence community. Once you're a spy, you're always a spy -- it's a job for life, with few exceptions. One of those is blowing the whistle, which he did. Since then, he has spent his retirement lobbying for change and reform in industry and in Congress. "They're taking away half of the constitution in secret," said Binney. "If they want to change the constitution, there's a way to do that -- and it's in the constitution." An NSA spokesperson did not immediately comment.

Turns cyberterror

Mass surveillance collapses the internet and makes cyberterror likely

Bryant, VICE, 1/26 (Ben Bryant, VICE News "Mass Surveillance Does Not Stop Terrorists, Europe's Top Rights Body Says" January 26, 2015 <https://news.vice.com/article/mass-surveillance-does-not-stop-terrorists-europe-s-top-rights-body-says>) //GY

Mass surveillance is ineffective in the fight against terrorism, threatens human rights and violates the privacy enshrined in European law, Europe's top rights body has said. Among a raft of non-binding proposals, parliamentary watchdogs should be given the power to approve intelligence agencies' budgets and whistleblowers should be offered statutory protection, a report by the assembly of the Council of Europe said. The 35-page document drafted by Dutch parliamentarian Pieter Omtzigt proposes measures that should be taken by the assembly's 47 European member states before the "industrial-surveillance complex spins out of control." The assembly, which will now debate the report, provides recommendations to the European Court of Human Rights which are not legally binding but can be influential. European governments are free to ignore the assembly's recommendations, but must explain why if they choose to do so. The report also says that current British laws may be incompatible with the European convention on human rights, an internationally binding treaty. British surveillance may contradict Article 8, the right to privacy; Article 10, the right to freedom of expression; and Article 6, the right to a fair trial. In wake of Paris attacks, David Cameron calls for new powers to break encrypted communications. Read more here. The assembly has been investigating the question of surveillance since last year, and in April heard evidence via videolink from Edward Snowden, the fugitive US National Security Agency whistleblower. Its report was dismissive of the value of intelligence gleaned from mass surveillance, saying: "We have seen that mass surveillance is not even effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance." It does not specifically mention the recent Paris terrorist attacks in which 17 people were shot dead by terrorists, however. UK Prime Minister David Cameron has used the Paris shootings to call for widening surveillance powers, despite admissions from France that the attackers were known to the authorities, but that they discontinued eavesdropping last summer. Citing independent US reviews of mass surveillance, the report said "resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act." Some aspects of mass surveillance, such as the deliberate weakening of encryption, even present "a grave danger for national security" the report said, because such **weaknesses "can be detected and exploited by rogue states, terrorists cyber-terrorists and ordinary criminals."** Cameron has recently called for new powers to break encrypted communications. UK will ask preschool teachers to spy on children in latest counter-terror proposals. Read more here. Mass surveillance threatens "the very existence of the Internet as we know it" and "nobody and nothing is safe from snooping by our own countries' and even foreign intelligence services" without technology that safeguards privacy, the document added. The assembly also sent a letter to the German, British and US authorities asking if they had circumvented laws restricting domestic spying by getting a third party to do it for them. The Germans and British deny the accusation, but the US has failed to reply. The report concludes that the British response was probably true — because the UK's Data Retention and Investigatory Powers Act already allows for the wide-ranging collection of personal data. Eric King, deputy director of privacy NGO Privacy International, told VICE News: "This latest report highlights what has been said all along: intelligence agencies in the UK are in the business of mass, indiscriminate surveillance and there are few if any legal

safeguards in place to protect human rights. "It's embarrassing that the British government continues to neither confirm nor deny the essential facts behind this, limiting the opportunity for debate, limiting the opportunity for reform, and limiting proper accountability in the courts." "Secret interpretations of secret laws are plainly not a sustainable position, and place democracy and the rule of law in jeopardy."

Overload negates effectiveness of cybersecurity operations

Conti et al, Director of the Information Technology Operations Center, '06

(Gregory Conti, Kulsoom Abdullah, Julian Grizzard, John Stasko, John A. Copeland, Mustaque Ahamad, Henry L. Owen, and Chris Lee, Georgia Institute of Technology "Countering Security Information Overload through Alert and Packet Visualization" March/April 2006 Published by the IEEE Computer Society <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1607922> //GY

The massive amount of security data that network sensors and host-based applications generate can quickly overwhelm the operators charged with defending the network. Often, operators overlook important details, and it's difficult to gain a coherent picture of network health and security status by manually traversing textual logs, using commandline analysis scripts or traditional graphing and charting techniques. In many instances, this flood of data will actually reduce the overall level of security by consuming operators' available time or misdirecting their efforts. In extreme circumstances, the operators will become desensitized and ignore security warnings altogether, effectively negating the value of their security systems.

...

Information visualization of security-related data bears great promise in making our personal computers, servers, and networks more secure. Such work is both an art and a science requiring expertise from the computer graphics, information visualization, interface design, and security communities to turn the raw security data into insightful and actionable information and knowledge. There is no shortage of raw data—in fact there is far more than can be analyzed by today's best tools. Humans often cope with this torrent of data by using crude statistical techniques, textual displays, and outdated graphical techniques and by ignoring large portions of the data. We believe that security visualization, at its best, is both compelling as a video game and several orders of magnitude more effective than the tools we employ today. In this article, we moved toward this goal by exploring the design, implementation, and evaluation of two complementary systems springing from immediate, high-priority security needs and developed by an interdisciplinary team of researchers. By bringing together diverse ideas and expertise, we directly addressed significant problems facing the people who defend our information technology resources.

New CISA bill fails to effectively stop cyberattacks – gathering more information distracts officials from fixing structural problems

Castillo 5/7 (Andrea, program manager of the Technology Policy Program for the Mercatus Center at George Mason University, 5/7/15, "Cybersecurity bill more likely to promote information overload than prevent cyberattacks," <http://thehill.com/blogs/congress-blog/homeland-security/241242-cybersecurity-bill-more-likely-to-promote-information/Tang>)

A growing number of information security and hacking incidents emphasize the importance of improving U.S. cybersecurity practices. But many computer security experts are concerned that the Cybersecurity Information Sharing Act of 2015

(CISA) is unlikely to meaningfully prevent cyberattacks as supporters claim. Rather, it will provide another avenue for federal offices to extract private data without addressing our root cybersecurity vulnerabilities. The main premise of CISA is that cyber breaches can be prevented by encouraging private companies to share cyber threat data with the government. CISA would extend legal immunity to private entities that share sensitive information about security vulnerabilities—often containing personally identifiable information (PII) about users and customers—with federal offices like the Department of Justice (DOJ), Department of Homeland Security (DHS) and Director of National Intelligence (DNI). This concerns privacy advocates who point out that such data collection could serve as an alternative surveillance tool for the NSA. Section 5(A) of CISA authorizes federal agencies to “disclose, retain, and use” shared data for many purposes beyond promoting cybersecurity, like investigating terrorism, the sexual exploitation of children, violent felonies, fraud, identity theft, and trade secret violation. In other words, CISA would allow federal agencies to use data obtained under the auspices of “cybersecurity protection” in entirely unrelated criminal investigations—potentially indefinitely. Indeed, CISA is currently stalled in the Senate in deference to debate over the NSA’s controversial bulk collection programs. But the Senate cool-down should not let us forget that CISA does not just threaten civil liberties, it could actually undermine cybersecurity. Information security experts point out that existing information sharing measures run by private companies like IBM and Dell SecureWorks rarely prevent attacks like CISA advocates promise. One survey of information security professionals finds that 87 percent of responders did not believe information sharing measures such as CISA will significantly reduce privacy breaches. The federal government already operates at least 20 information sharing offices collaborating on cybersecurity with the private sector, as Eli Dourado and I found in our new analysis through the Mercatus Center at George Mason University. These numerous federal information-sharing initiatives have not stemmed the tidal wave of government cyberattacks. Another Mercatus Center analysis Dourado and I conducted finds that the number of reported federal information security failures has increased by an astounding 1,012 percent—from 5,502 in FY 2006 to 61,214 in FY 2013. Almost 40 percent of these involved the PII of federal employees and civilians. CISA could therefore have the unintended consequence of creating a juicy and unprepared target for one-stop hacking. The Office of Management and Budget reports that many of the federal agencies that would be given large data management responsibilities through CISA, like the DOJ and DHS, reported thousands of such breaches in FY 2014. These agencies’ own information security systems are unlikely to become miraculously impervious to external hacking upon CISA’s passing. In fact, the massive amounts of new data to manage could further overwhelm currently suboptimal practices. The federal government’s information security failures indicate a technocratic mindset that falsely equates the complexity of bureaucracy with the strength of a solution. In reality, the government’s brittle and redundant internal cybersecurity policies actively contribute to their security challenges. The Government Accountability Office (GAO) has reported for years that such overlapping and unclear responsibility in federal cybersecurity policy limits the offices’ ultimate effectiveness. A 2015 GAO investigation concludes that without significant change “the nation’s most critical federal and private sector infrastructure systems will remain at increased risk of attack from adversaries.” The federal government must get its own house in order before such comprehensive information sharing measures like CISA could be even technically feasible. But CISA would be a failure even if managed by the most well-managed government systems because it seeks to impose a technocratic structure on a dynamic system. Effective reform will promote a self-organizing “collaborative security approach” as outlined by groups like the Internet Society, an international nonprofit devoted to Internet policy and technology standards. Cybersecurity provision is too important a problem to be inadequately addressed by measures that will fail to improve security.

Turns terror

Overload makes terrorist attacks more likely to go unprevented

Eddington, 1/27 (Patrick Eddington, CATO institute, "No, Mass Surveillance Won't Stop Terrorist Attacks" January 27, 2015 <http://reason.com/archives/2015/01/27/mass-surveillance-and-terrorism#.19hszl:U8Io> //GY

The recent terrorist attack on the office of French satirical magazine Charlie Hebdo generated a now-familiar meme: Another terrorist attack means we need more surveillance.¶ Sen. Bob Corker (R-Tenn.) said that while "Congress having oversight certainly is important ... what is more important relative to these types of events is ensuring we don't overly hamstring the NSA's ability to collect this kind of information in advance and keep these kinds of activities from occurring." Similarly, Sen. Lindsey Graham (R-S.C.) spoke of his "fear" that "our intelligence capabilities, those designed to prevent such an attack from taking place on our shores, are quickly eroding," adding that the government surveillance "designed to prevent these types of attacks from occurring is under siege."¶ A recent poll demonstrates that their sentiments are widely shared in the wake of the attack.¶ But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the answer:¶ 2009: Umar Farouk Abdulmutallab—i.e., the "underwear bomber"—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community (IC) failed "to connect, integrate, and fully understand the intelligence" it had collected.¶ 2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation.¶ 2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency (NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS.¶ 2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine.¶ No, mass surveillance does not prevent terrorist attacks.¶ It's worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally-dubious ones—were premised on the belief that bin Laden's hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data. Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government's hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination. That malady perfectly describes every intelligence failure from Pearl Harbor to the present day.¶ The Office of the Director of National Intelligence (created by Congress in 2004) was supposed to be the answer to the "failure-to-connect-the-dots" problem. Ten years on, the problem remains, the IC bureaucracy is bigger than ever, and our government is continuing to rely on mass surveillance programs that have failed time and again to stop terrorists while simultaneously undermining the civil liberties and personal privacy of every American. The quest to "collect it all," to borrow a phrase from NSA Director Keith Alexander, only leads to the accumulation of masses of useless information, making it harder to find real threats and costing billions to store.¶ A recent Guardian editorial noted that such mass-surveillance myopia is spreading among European political leaders as well, despite the fact that "terrorists, from 9/11 to the Woolwich jihadists and the neo-Nazi Anders

Breivik, have almost always come to the authorities' attention before murdering." Mass surveillance is not only destructive of our liberties, its continued use is a virtual guarantee of more lethal intelligence failures. And our continued will to disbelieve those facts is a mental dodge we engage in at our peril.

Overload of data makes terrorism prevention impossible

Tufekci, assistant professor UNC, 2/3 (Zeynep Tufekci, assistant professor at the University of North Carolina, "Terror and the limits of mass surveillance" Feb 03, 2015 <http://blogs.ft.com/the-exchange/2015/02/03/zeynep-tufekci-terror-and-the-limits-of-mass-surveillance/>) //GY

But the assertion that big data is "what it's all about" when it comes to predicting rare events is not supported by what we know about how these methods work, and more importantly, don't work. Analytics on massive datasets can be powerful in analysing and identifying broad patterns, or events that occur regularly and frequently, but are singularly unsuited to finding unpredictable, erratic, and rare needles in huge haystacks. In fact, the bigger the haystack — the more massive the scale and the wider the scope of the surveillance — the less suited these methods are to finding such exceptional events, and the more they may serve to direct resources and attention away from appropriate tools and methods. After Rigby was killed, GCHQ, Britain's intelligence service, was criticised by many for failing to stop his killers, Michael Adebolajo and Michael Adebowale. A lengthy parliamentary inquiry was conducted, resulting in a 192-page report that lists all the ways in which Adebolajo and Adebowale had brushes with data surveillance, but were not flagged as two men who were about to kill a soldier on a London street. GCHQ defended itself by saying that some of the crucial online exchanges had taken place on a platform, believed to be Facebook, which had not alerted the agency about these men, or the nature of their postings. The men apparently had numerous exchanges that were extremist in nature, and their accounts were suspended repeatedly by the platform for violating its terms of service. If only Facebook had turned over more data," the thinking goes. But that is misleading, and makes sense only with the benefit of hindsight. Seeking larger volumes of data, such as asking Facebook to alert intelligence agencies every time that it detects a post containing violence, would deluge the agencies with multiple false leads that would lead to a data quagmire, rather than clues to impending crimes. For big data analytics to work, there needs to be a reliable connection between the signal (posting of violent content) and the event (killing someone). Otherwise, the signal is worse than useless. Millions of Facebook's billion-plus users post violent content every day, ranging from routinised movie violence to atrocious violent rhetoric. Turning over the data from all such occurrences would merely flood the agencies with "false positives" — erroneous indications for events that actually will not happen. Such data overload is not without cost, as it takes time and effort to sift through these millions of strands of hay to confirm that they are, indeed, not needles — especially when we don't even know what needles look like. All that the investigators would have would be a lot of open leads with no resolution, taking away resources from any real investigation. Besides, account suspensions carried out by platforms like Facebook's are haphazard, semi-automated and unreliable indicators. The flagging system misses a lot more violent content than it flags, and it often flags content as inappropriate even when it is not, and suffers from many biases. Relying on such a haphazard system is not a reasonable path at all. So is all the hype around big data analytics unjustified? Yes and no. There are appropriate use cases for which massive datasets are intensely useful, and perform much better than any alternative we can imagine using conventional methods. Successful examples include using Google searches to figure out drug interactions that would be too complex and too numerous to

analyse one clinical trial at a time, or using social media to detect national-level swings in our mood (we are indeed happier on Fridays than on Mondays).

Overload makes lone wolf terror prevention ineffective

Tufekci, assistant professor UNC, 2/3 (Zeynep Tufekci, assistant professor at the University of North Carolina, “Terror and the limits of mass surveillance” Feb 03, 2015 <http://blogs.ft.com/the-exchange/2015/02/03/zeynep-tufekci-terror-and-the-limits-of-mass-surveillance/>) //GY

In contrast, consider the “lone wolf” attacker who took hostages at, of all things, a “Lindt Chocolat Café” in Sydney. Chocolate shops are not regular targets of political violence, and random, crazed men attacking them is not a pattern on which we can base further identification. Yes, the Sydney attacker claimed jihadi ideology and brought a black flag with Islamic writing on it, but given the rarity of such events, it’s not always possible to separate the jihadi rhetoric from issues of mental health — every era’s mentally ill are affected by the cultural patterns around them. This isn’t a job for big data analytics. (The fact that the gunman was on bail facing various charges and was known for sending hate letters to the families of Australian soldiers killed overseas suggests it was a job for traditional policing). When confronted with their failures in predicting those rare acts of domestic terrorism, here’s what GCHQ, and indeed the NSA, should have said instead of asking for increased surveillance capabilities: stop asking us to collect more and more data to perform an impossible task. This glut of data is making our job harder, not easier, and the expectation that there will never be such incidents, ever, is not realistic. Attention should instead be focused on the causal chain that led the Kouachi brothers on their path. It seems that the French-born duo had an alienated, turbulent youth, and then spent years in French prisons, where they were transformed from confused and incompetent wannabe jihadis to hardliners who were both committed and a lot more capable of carrying out complex violence acts than when they entered the prison. Understanding such paths will almost certainly be more productive for preventing such events, and will also spare all of us from another real danger: governments that know too much about their citizens, and a misguided belief in what big data can do to find needles in too-large haystacks.

Mass data mining makes terror prevention impossible

Schneier, 3/24 (Bruce Schneier Advisory Board Member of the Electronic Privacy Information Center, “Why Mass Surveillance Can’t, Won’t, And Never Has Stopped A Terrorist” Mar 24 2015, 2:15 AM <http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist>) //GY

Data mining is offered as the technique that will enable us to connect those dots. But while corporations are successfully mining our personal data in order to target advertising, detect financial fraud, and perform other tasks, three critical issues make data mining an inappropriate tool for finding terrorists. The first, and most important, issue is error rates. For advertising, data mining can be successful even with a large error rate, but finding terrorists requires a much higher degree of accuracy than data-mining systems can possibly provide. Data mining works best when you’re searching for a well-defined profile, when there are a reasonable number of events per year, and when the cost of false alarms is low. Detecting credit card fraud is one of data mining’s security success stories: all credit card companies mine their transaction databases for spending

patterns that indicate a stolen card. There are over a billion active credit cards in circulation in the United States, and nearly 8% of those are fraudulently used each year. Many credit card thefts share a pattern — purchases in locations not normally frequented by the cardholder, and purchases of travel, luxury goods, and easily fenced items — and in many cases data-mining systems can minimize the losses by preventing fraudulent transactions. The only cost of a false alarm is a phone call to the cardholder asking her to verify a couple of her purchases.¶ Similarly, the IRS uses data mining to identify tax evaders, the police use it to predict crime hot spots, and banks use it to predict loan defaults. These applications have had mixed success, based on the data and the application, but they're all within the scope of what data mining can accomplish.¶ Terrorist plots are different, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless.¶ The reason lies in the mathematics of detection. All detection systems have errors, and system designers can tune them to minimize either false positives or false negatives. In a terrorist-detection system, a false positive occurs when the system mistakenly identifies something harmless as a threat. A false negative occurs when the system misses an actual attack. Depending on how you “tune” your detection system, you can increase the number of false positives to assure you are less likely to miss an attack, or you can reduce the number of false positives at the expense of missing attacks.¶ Because terrorist attacks are so rare, false positives completely overwhelm the system, no matter how well you tune. And I mean completely: millions of people will be falsely accused for every real terrorist plot the system finds, if it ever finds any.¶ We might be able to deal with all of the innocents being flagged by the system if the cost of false positives were minor. Think about the full-body scanners at airports. Those alert all the time when scanning people. But a TSA officer can easily check for a false alarm with a simple pat-down. This doesn't work for a more general data-based terrorism-detection system. Each alert requires a lengthy investigation to determine whether it's real or not. That takes time and money, and prevents intelligence officers from doing other productive work. Or, more pithily, when you're watching everything, you're not seeing anything.¶ The US intelligence community also likens finding a terrorist plot to looking for a needle in a haystack. And, as former NSA director General Keith Alexander said, “you need the haystack to find the needle.” That statement perfectly illustrates the problem with mass surveillance and bulk collection. When you're looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you're also adding much more noise. And despite the NSA's “collect it all” mentality, its own documents bear this out. The military intelligence community even talks about the problem of “drinking from a fire hose”: having so much irrelevant data that it's impossible to find the important bits. We saw this problem with the NSA's eavesdropping program: the false positives overwhelmed the system. In the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Suspicious Activity Reports —or SAR — database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent \$8,500 to a Somali group that posed no direct threat to the US — and that was probably trumped up so the NSA would have better talking points in front of Congress.¶ The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon

finish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportionate impact on the criteria used to decide who's a likely terrorist, leading to ineffective detection strategies.The third problem is that the people the NSA is trying to find are wily, and they're trying to avoid detection. In the world of personalized marketing, the typical surveillance subject isn't trying to hide his activities. That is not true in a police or national security context. An adversarial relationship makes the problem much harder, and means that most commercial big data analysis tools just don't work. A commercial tool can simply ignore people trying to hide and assume benign behavior on the part of everyone else. Government data-mining techniques can't do that, because those are the very people they're looking for.

Data overload risks terror attacks – whistleblowers confirm Whittaker, 15

Zack Whittaker is a writer-editor for ZDNet, and sister sites CNET and CBS News, citing an NSA whistleblower, "NSA is so overwhelmed with data, it's no longer effective, says whistleblower," ZDNet, 4/30/15, http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/?tag=nl.e539&s_cid=e539&ttag=e539&ftag=TRE17cf61 // IS

In a lunch meeting hosted by Contrast Security founder Jeff Williams on Wednesday, William Binney, a former NSA official who spent more than three decades at the agency, said the US government's mass surveillance programs have become so engorged with data that they are no longer effective, losing vital intelligence in the fray.

That, he said, can -- and has -- led to terrorist attacks succeeding.

Binney said that an analyst today can run one simple query across the NSA's various databases, only to become immediately overloaded with information. With about four billion people -- around two-thirds of the world's population -- under the NSA and partner agencies' watchful eyes, according to his estimates, there is too much data being collected.

"That's why they couldn't stop the Boston bombing, or the Paris shootings, because the data was all there," said Binney. Because the agency isn't carefully and methodically setting its tools up for smart data collection, that leaves analysts to search for a needle in a haystack.

"The data was all there... the NSA is great at going back over it forensically for years to see what they were doing before that," he said. "But that doesn't stop it."

Binney called this a "bulk data failure" -- in that the NSA programs, leaked by Edward Snowden, are collecting too much for the agency to process. He said the problem runs deeper across law enforcement and other federal agencies, like the FBI, the CIA, and the Drug Enforcement Administration (DEA), which all have access to NSA intelligence.

than government or law can keep up."

Overload kills attempts to stop Al Qaeda attacks

Robb, Air Force analyst, '06 (John Robb, Air Force analyst, "NSA: The Problems with Massively Automated Domestic Surveillance" May 11, 2006
http://globalguerrillas.typepad.com/johnrobb/2006/05/nsa_the_problem.html) //GY

Noah, at DefenseTech, tapped Valdis Krebs for his analysis of the problems with the slowly leaked details on the NSAs domestic surveillance efforts. Valdis makes the absolutely correct observation that:

The right thing to do is to look for the best haystack, not the biggest haystack. We knew exactly which haystack to look at in the year 2000 [before the 9/11 attacks]. We just didn't do it...

To me, it's pretty clear that the people working on this program aren't as smart as they think they are. Some top level thinking indicates that this will quickly become a rat hole for federal funds (due to wasted effort) and a major source of infringement of personal freedom. Here's some detail:

It will generate oodles of false positives. Al Qaeda is now in a phase where most domestic attacks will be generated by people not currently connected to the movement (like we saw in the London bombings). This means that in many respects they will look like you and me until they act. The large volume of false positives generated will not only be hugely inefficient, it will be a major infringement on US liberties. For example, a false positive will likely get you automatically added to a no-fly list, your boss may be visited (which will cause you to lose your job), etc.

It will be expanded to include to monitor domestic groups other than al Qaeda. As we have already seen in numerous incidents across the US, every group that opposes the war or deals with issues in the Middle East will eventually fall under surveillance. Eventually, this will begin to bump up the political process by targeting groups that are politically active in the opposition party.

The database and associated information will be used for purposes other than tracking groups. For example: finding who leaked a classified document to a reporter by reading the list of all calls made to that reporter (who is likely on the target list due to the subjects they cover).

Info overload creates redundancy – lack of info sharing makes it impossible to stop attacks

Priest and Arkin 10 (Dana Priest, American academic, journalist and writer, Washington Post, William Arkin, American political commentator, best-selling author, journalist, activist, blogger, and former United States Army soldier, 7/19, “Top Secret America,”

<http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print//Tang>)

And then came a problem that continues to this day, which has to do with the ODNI's rapid expansion. When it opened in the spring of 2005, Negroponte's office was all of 11 people stuffed into a secure vault with closet-size rooms a block from the White House. A year later, the budding agency moved to two floors of another building. In April 2008, it moved into its huge permanent home, Liberty Crossing. Today, many officials who work in the intelligence agencies say they remain unclear about what the ODNI is in charge of. To be sure, the ODNI has made some progress, especially in intelligence-sharing, information technology and budget reform. The DNI and his managers hold interagency meetings every day to promote collaboration. The last director, Blair, doggedly pursued such nitty-gritty issues as procurement reform, compatible computer networks, tradecraft standards and collegiality. But improvements have been overtaken by volume at the ODNI, as the increased flow of intelligence data overwhelms the system's ability to analyze and use it. Every day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications. The NSA sorts a fraction of those into 70 separate databases. The same problem bedevils every other intelligence agency, none of which have enough analysts and translators for all this work. The practical effect of this unwieldiness is visible, on a much smaller scale, in the office of Michael Leiter, the director of the National Counterterrorism Center. Leiter spends much of his day flipping among four computer monitors lined up on his desk. Six hard drives sit at his feet. The data flow is enormous, with dozens of databases feeding separate computer networks that cannot interact with one another. There is a long explanation for why these databases are still not connected, and it amounts to this: It's too hard, and some agency heads don't really want to give up the systems they have. But there's some progress: "All my e-mail on one computer now," Leiter says. "That's a big deal." To get

another view of how sprawling Top Secret America has become, just head west on the toll road toward Dulles International Airport. As a Michaels craft store and a Books-A-Million give way to the military intelligence giants Northrop Grumman and Lockheed Martin, find the off-ramp and turn left. Those two shimmering-blue five-story ice cubes belong to the National Geospatial-Intelligence Agency, which analyzes images and mapping data of the Earth's geography. A small sign obscured by a boxwood hedge says so. Across the street, in the chocolate-brown blocks, is Carahsoft, an intelligence agency contractor specializing in mapping, speech analysis and data harvesting. Nearby is the government's Underground Facility Analysis Center. It identifies overseas underground command centers associated with weapons of mass destruction and terrorist groups, and advises the military on how to destroy them. Clusters of top-secret work exist throughout the country, but the Washington region is the capital of Top Secret America. About half of the post-9/11 enterprise is anchored in an arc stretching from Leesburg south to Quantico, back north through Washington and curving northeast to Linthicum, just north of the Baltimore-Washington International Marshall Airport. Many buildings sit within off-limits government compounds or military bases. Others occupy business parks or are intermingled with neighborhoods, schools and shopping centers and go unnoticed by most people who live or play nearby. Many of the newest buildings are not just utilitarian offices but also edifices "on the order of the pyramids," in the words of one senior military intelligence officer. Not far from the Dulles Toll Road, the CIA has expanded into two buildings that will increase the agency's office space by one-third. To the south, Springfield is becoming home to the new \$1.8 billion National Geospatial-Intelligence Agency headquarters, which will be the fourth-largest federal building in the area and home to 8,500 employees. Economic stimulus money is paying hundreds of millions of dollars for this kind of

federal construction across the region. It's not only the number of buildings that suggests the size and cost of this expansion, it's also what is inside: banks of television monitors. "Escort-required" badges. X-ray machines and lockers to store cellphones and pagers.

Keypad door locks that open special rooms encased in metal or permanent dry wall, impenetrable to eavesdropping tools and protected by alarms and a security force capable of responding within 15 minutes. Every one of these buildings has at least one of these rooms, known as a SCIF, for sensitive compartmented information facility. Some are as small as a closet; others are four times the size of a football field. SCIF size has become a measure of status in Top Secret America, or at least in the Washington region of it. "In D.C., everyone talks SCIF, SCIF, SCIF," said Bruce Paquin, who moved to Florida from the Washington region several years ago to start a SCIF construction business. "They've got the penis envy thing going. You can't be a big boy unless you're a three-letter agency and you have a big SCIF." SCIFs are not the only must-have items people pay attention to. Command centers, internal television networks, video walls, armored SUVs and personal security guards have also become the bling of national security. "You can't find a four-star general without a security detail," said one three-star general now posted in Washington after years abroad. "Fear has caused everyone to have stuff. Then comes, 'If he has one, then I have to have one.' It's become a status symbol." Among the most important people inside the SCIFs are the low-paid employees carrying their lunches to work to save money. They are the analysts, the 20- and 30-year-olds making \$41,000 to \$65,000 a year, whose job is at the core of everything Top Secret America tries to do. At its best, analysis melds cultural understanding with snippets of conversations, coded dialogue, anonymous tips, even scraps of trash, turning them into clues that lead to individuals and groups trying to harm the United States. Their work is greatly enhanced by computers that sort through and categorize data.

But in the end, analysis requires human judgment, and half the analysts are relatively inexperienced, having been hired in the past several years, said a senior ODNI official. Contract analysts are often straight out of college and trained at corporate headquarters. When hired, a typical analyst knows very little about the priority countries - Iraq, Iran, Afghanistan and Pakistan - and is not fluent in their languages. Still, the number of intelligence reports they produce on these key countries is overwhelming, say current and former intelligence officials who try to cull them every day. The ODNI doesn't know exactly how many reports are issued each year, but in the process of trying to find out, the chief of analysis discovered 60 classified analytic Web sites still in operation that were supposed to

have been closed down for lack of usefulness. "Like a zombie, it keeps on living" is how one official describes the sites. The problem with many intelligence reports, say officers who read them, is that they simply re-slice the same facts already in circulation. "It's the soccer ball syndrome. Something happens, and they want to rush to cover it," said Richard H.

Immerman, who was the ODNI's assistant deputy director of national intelligence for analytic integrity and standards until early 2009. I saw tremendous overlap. Even the analysts at the National Counterterrorism Center (NCTC), which is supposed to be where the most sensitive, most difficult-to-obtain nuggets of information are fused together, get low marks from intelligence officials for not producing reports that are original, or at least better than the reports already written by the CIA, FBI, National Security Agency or Defense Intelligence Agency. When Maj. Gen. John M. Custer was the director of intelligence at U.S. Central Command, he grew angry at how little helpful information came out of the NCTC. In 2007, he visited its director at the time, retired Vice Adm. John Scott Redd, to tell him so. "I told him that after 41/2 years, this organization had never produced one shred of information that helped me prosecute three wars!" he said loudly, leaning over the table during an interview. Two years later, Custer, now head of the Army's intelligence school at Fort Huachuca, Ariz., still gets red-faced recalling that day, which reminds him of his frustration with

Washington's bureaucracy. Who has the mission of reducing redundancy and ensuring everybody doesn't gravitate to the lowest-hanging fruit?" he said. Who orchestrates what is produced so that everybody doesn't produce the same thing?" He's hardly the only one irritated. In a secure office in Washington, a senior intelligence officer was dealing with his own frustration. Seated at his computer, he began scrolling through some of the classified information he is expected to read every day: CIA World Intelligence Review, WIRE-CIA, Spot Intelligence Report, Daily Intelligence Summary, Weekly Intelligence Forecast, Weekly Warning Forecast, IC Terrorist Threat Assessments, NCTC Terrorism Dispatch, NCTC Spotlight . . . It's too much, he complained. The inbox on his desk was full, too. He threw up his arms, picked up a thick, glossy intelligence report and waved it around, yelling. "Jesus! Why does it take so long to produce?" "Why does it have to be so bulky?" "Why isn't it online?" The overload of hourly, daily, weekly, monthly and annual reports is actually counterproductive, say people who receive them. Some policymakers and senior officials don't dare delve into the backup clogging their computers. They rely instead on personal briefers, and those briefers usually rely on their own agency's analysis, re-creating the very problem identified as a main cause of the failure to thwart the attacks: a lack of information-sharing.

More surveillance fails to prevent terror attacks – multiple examples

Marlowe 10 (Lara, Paris Correspondent with The Irish Times., citing Top Secret America report, 7/24, “Information overload threatening to choke response to terror.”
<http://www.irishtimes.com/news/information-overload-threatening-to-choke-response-to-terror-1.626474//Tang>)

A report on the colossal counter-terrorism intelligence industry in the US shows that it may be drowning in an ocean of raw data THIS, I suspect, is how empires die: over-extended, asphyxiated by bureaucracy, drowning in information they cannot adequately assess or act upon. The Washington Post published a stunning, three-day series totalling 11 pages this week on “Top Secret America”. It was the result of an investigation over two years by Dana Priest and William Arkin into the explosion of the intelligence industry since September 11th, 2001. Consider the statistics: 1,271 government organisations and 1,931 private companies are now devoted to counter-terrorism, “homeland security” and intelligence, in 10,000 locations across the US. An estimated 854,000 Americans – 1.5 times the population of Washington DC – hold top secret security clearances. Nearly one-third of them are private contractors. About half of Top Secret America is concentrated in a swathe of land running diagonally from Virginia to the southwest, across Washington DC and into Maryland to the northeast. In the Washington area alone, 33 top-secret building complexes, some of them unmarked and windowless behind high fences, have been or are being built since 9/11. They total 1.6 million sq m (17 million sq ft), the equivalent of 22 US Capitol buildings. Turf battles between intelligence agencies, the habit of holding information close to the chest and the impossibility of co-ordinating so much activity makes for huge amounts of duplication. For example, 51 federal organisations and military commands are dedicated to tracking the money of terrorists. The volume of reporting generated by Top Secret America – 50,000 intelligence reports each year – means no one has a full grasp of what is known. As James Clapper, President Obama’s nominee for director of national intelligence, told the Post: “There’s only one entity in the entire universe that has visibility on all (top secret programmes) – that’s God.” “The complexity of this system defies description,” said another high-ranking source, retired army Lt Gen John Vines, commissioned to track intelligence at the Department of Defence. The Post concluded that despite a 250 per cent increase in intelligence spending since 9/11, despite the creation or restructuring of 263 organisations, “the problems that gusher of money and bureaucracy were meant to solve . . . have not been alleviated”. Agencies are still failing to share information or “connect the dots”. America may not be measurably safer for the more than \$75 billion (€58 billion) it spends each year on intelligence. The National Security Agency intercepts and stores 1.7 billion e-mails, phone calls and other communications daily. But the NSA and other agencies doing similar work don’t have enough analysts and translators to process the information they cull. One could argue that the absence of large-scale, lethal attacks on the US continent since 9/11 shows the system is working. But three recent cases show how Top Secret America failed to forestall real threats. Last November, US army Maj Nidal Hasan went on a shooting rampage at Fort Hood Texas, killing 13 people and wounding 30 others. When he was training as a psychiatrist at Walter Reed Army Medical Centre, Hasan had warned his superiors of “adverse events” if Muslims were not allowed to leave the army. And he exchanged e-mails with Anwar Awlaki, a radical cleric based in Yemen whom the US has targeted for assassination. But the army’s intelligence unit did not notice Hasan’s behaviour. Its programme, called RITA for Radical Islamic Threat to the Army, was too busy replicating work by the Department of Homeland Security and FBI on Islamist student groups in the US. Last autumn, President Obama signed a secret order to send dozens of commandos to Yemen, where they set up an intelligence centre bristling with hi-tech equipment. Their voluminous reports were bundled into the 5,000 pieces of data sent daily to the National Counter-terrorism Centre in Washington. Buried in the deluge was the news that a radical Nigerian student had visited Yemen, that a Nigerian father was worried about his son who’d gone to Yemen. But when Umar Farouk Abdulmutallab tried to blow himself up on a flight to Detroit on Christmas Day, the aircraft was saved by a passenger who saw smoke coming from Abdulmutallab’s underwear and tackled him, preventing him from detonating the device. Likewise, it was a vendor in Manhattan who alerted police to a home-made car bomb on Times Square at the beginning of

May. Faisal Shahzad, the Pakistani-born American citizen who concocted the mix of fertiliser and bleach, was also in contact with Anwar Awlaki. The Postreports that analysts working on the “priority countries” of Iraq, Iran, Afghanistan and Pakistan know little about them and do not speak their languages, yet produce an “overwhelming” number of reports. The many-tentacled intelligence community in the US seems blighted by two of the same woes as US journalism: the same information is rehashed over and over, and recipients are powerless to sift through the glut of material.

Info overload is counterproductive to counterterror efforts – cognitive burden

Maas 5/28 (Peter, written about war, media, and national security for The New York Times Magazine, The New Yorker, and The Washington Post. 5/28/15, “INSIDE NSA, OFFICIALS PRIVATELY CRITICIZE “COLLECT IT ALL” SURVEILLANCE,” <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance//Tang>)

AS MEMBERS OF CONGRESS struggle to agree on which surveillance programs to re-authorize before the Patriot Act expires, they might consider the unusual advice of an intelligence analyst at the National Security Agency who warned about the danger of collecting too much data. Imagine, the analyst wrote in a leaked document, that you are standing in a shopping aisle trying to decide between jam, jelly or fruit spread, which size, sugar-free or not, generic or Smucker’s. It can be paralyzing. “We in the agency are at risk of a similar, collective paralysis in the face of a dizzying array of choices every single day,” the analyst wrote in 2011. “Analysis paralysis’ isn’t only a cute rhyme. It’s the term for what happens when you spend so much time analyzing a situation that you ultimately stymie any outcome It’s what happens in SIGINT [signals intelligence] when we have access to endless possibilities, but we struggle to prioritize, narrow, and exploit the best ones.” The document is one of about a dozen in which NSA intelligence experts express concerns usually heard from the agency’s critics: that the U.S. government’s “collect it all” strategy can undermine the effort to fight terrorism. The documents, provided to The Intercept by NSA whistleblower Edward Snowden, appear to contradict years of statements from senior officials who have claimed that pervasive surveillance of global communications helps the government identify terrorists before they strike or quickly find them after an attack. The Patriot Act, portions of which expire on Sunday, has been used since 2001 to conduct a number of dragnet surveillance programs, including the bulk collection of phone metadata from American companies. But the documents suggest that analysts at the NSA have drowned in data since 9/11, making it more difficult for them to find the real threats. The titles of the documents capture their overall message: “Data Is Not Intelligence,” “The Fallacies Behind the Scenes,” “Cognitive Overflow?” “Summit Fever” and “In Praise of Not Knowing.” Other titles include “Dealing With a ‘Tsunami’ of Intercept” and “Overcome by Overload?” The documents are not uniform in their positions. Some acknowledge the overload problem but say the agency is adjusting well. They do not specifically mention the Patriot Act, just the larger dilemma of cutting through a flood of incoming data. But in an apparent sign of the scale of the problem, the documents confirm that the NSA even has a special category of programs that is called “Coping With Information Overload.” The jam vs. jelly document, titled “Too Many Choices,” started off in a colorful way but ended with a fairly stark warning: “The SIGINT mission is far too vital to unnecessarily expand the haystacks while we search for the needles. Prioritization is key.” These doubts are infrequently heard from officials inside the NSA. These documents are a window into the private thinking of mid-level officials who are almost never permitted to discuss their concerns in public. AN AMUSING PARABLE circulated at the NSA a few years ago. Two people go to a farm and purchase a truckload of melons for a dollar each. They then sell the melons along a busy road for the same price, a dollar. As they drive back to the farm for another load, they realize they aren’t making a profit, so one of them suggests, “Do you think we need a bigger truck?” The parable was written by an intelligence analyst in a document dated Jan. 23, 2012 that was titled, “Do We Need a Bigger SIGINT Truck?” It expresses, in a lively fashion, a critique of the agency’s effort to collect what former NSA Director Keith Alexander referred to as “the whole haystack.” The critique goes to the heart of the agency’s drive to gather as much of the world’s communications as possible: because it may not find what it needs in a partial haystack of data, the haystack is expanded as much as possible, on the assumption that more data will eventually yield useful information. “THE PROBLEM IS THAT WHEN YOU

COLLECT IT ALL, WHEN YOU MONITOR EVERYONE, YOU UNDERSTAND

NOTHING.” –EDWARD SNOWDEN The Snowden files show that in practice, it doesn’t turn out that way: more is not necessarily better, and in fact, extreme volume creates its own challenges. “Recently I tried to answer what seemed like a relatively straightforward question about which telephony metadata collection capabilities are the most important in case we need to shut something off when the metadata coffers get full,” wrote the intelligence analyst. “By the end of the day, I felt like capitulating with the white flag of, ‘We need COLOSSAL data storage so we don’t have to worry about it,’ (aka we need a bigger SIGINT truck).” The analyst added, “Without metrics, how do we know that we have improved something or made it worse? There’s a running joke … that we’ll only know if collection is important by shutting it off and seeing if someone screams.” Another document, while not mentioning the dangers of collecting too much data, expressed concerns about pursuing entrenched but unproductive programs. “How many times have you been watching a terrible movie, only to convince yourself to stick it out to the end and find out what happens, since you’ve already invested too much time or money to simply walk away?” the document asked. “This ‘gone too far to stop now’ mentality is our built-in mechanism to help us allocate and ration resources. However, it can work to our detriment in prioritizing and deciding which projects or efforts are worth further expenditure of resources, regardless of how much has already been ‘sunk.’ As has been said before, insanity is doing the same thing over and over and expecting different results.” “**WE ARE DROWNING IN INFORMATION. AND YET WE KNOW NOTHING. FOR SURE.**” –NSA INTELLIGENCE ANALYST Many of these documents were written by intelligence analysts who had regular columns distributed on NSANet, the agency’s intranet. One of the columns was called “Signal v. Noise,” another was called “The SIGINT Philosopher.” Two of the documents cite the academic work of Herbert Simon, who won a Nobel Prize for his pioneering research on what’s become known as the attention economy. Simon wrote that consumers and managers have trouble making smart choices because their exposure to more information decreases their ability to understand the information. Both documents mention the same passage from Simon’s essay, Designing Organizations for an Information-Rich World: In an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it.” In addition to consulting Nobel-prize winning work, NSA analysts have turned to easier literature, such as Malcolm Gladwell’s best-selling Blink: The Power of Thinking Without Thinking. The author of a 2011 document referenced Blink and stated, “The key to good decision making is not knowledge. It is understanding. We are swimming in the former. We are desperately lacking in the latter.” The author added, “Gladwell has captured one of the biggest challenges facing SID today. Our costs associated with this information overload are not only financial, such as the need to build data warehouses large enough to store the mountain of data that arrives at our doorstep each day, but also include the more intangible costs of too much data to review, process, translate and report.” Alexander, the NSA director from 2005 to 2014 and chief proponent of the agency’s “collect it all” strategy, vigorously defended the bulk collection programs. “What we have, from my perspective, is a reasonable approach on how we can defend our nation and protect our civil liberties and privacy,” he said at a security conference in Aspen in 2013. He added, “You need the haystack to find the needle.” The same point has been made by other officials, including James Cole, the former deputy attorney general who told a congressional committee in 2013, “If you’re looking for the needle in the haystack, you have to have the entire haystack to look through.” NSA Slide, May 2011 The opposing viewpoint was voiced earlier this month by Snowden, who noted in an interview with the Guardian that the men who committed recent terrorist attacks in France, Canada and Australia were under surveillance—their data was in the haystack yet they weren’t singled out. “It wasn’t the fact that we weren’t watching people or not,” Snowden said. “It was the fact that we were watching people so much that we did not understand what we had. The problem is that when you collect it all, when you monitor everyone, you understand nothing.” In a 2011 interview with SIDtoday, a deputy director in the Signals Intelligence Directorate was asked about analytic modernization at the agency. His response, while positive on the NSA’s ability to surmount obstacles, noted that it faced difficulties, including the fact that some targets use encryption and switch phone numbers to avoid detection. He pointed to volume as a particular problem. “We live in an Information Age when we have massive reserves of information and don’t have the capability to exploit it,” he stated. “I was told that there are 2 petabytes of data in the SIGINT System at any given time. How much is that? That’s equal to 20 million 4-drawer filing cabinets. How many cabinets per analyst is that? By the end of this year, we’ll have 1 terabyte of data per second coming in. You can’t crank that through the existing processes and be effective.” The documents noted the difficulty of sifting through the ever-growing haystack of data. For instance, a 2011 document titled “ELINT Analysts – Overcome by Overload? Help is Here with IM&S” outlined a half dozen computer tools that “are designed to invert the paradigm where an analyst spends more time searching for data than analyzing it.” Another document, written by an intelligence analyst in 2010, bluntly stated that “we are drowning in information. And yet we know nothing. For sure.” The analyst went on to ask, “Anyone know just how many tools are available at the Agency, alone? Would you know where to go to find out? Anyone ever start a new target...without the first clue where to begin? Did you ever start a project wondering if you were the sole person in the Intelligence Community to work this project? How would you find out?” The analyst, trying to encourage more sharing of tips about the best ways to find data in the haystack, concluded by writing, in boldface, “Don’t let those coming behind you suffer the way you have.” The agency appears to be spending significant sums of money to solve the haystack problem. The document

headlined “Dealing With a ‘Tsunami’ of Intercept,” written in 2006 by three NSA officials and previously published by The Intercept, outlined a series of programs to prepare for a near future in which the speed and volume of signals intelligence would explode “almost beyond imagination.” The document referred to a mysterious NSA entity—the “Coping With Information Overload Office.” This appears to be related to an item in the Intelligence Community’s 2013 Budget Justification to Congress, known as the “black budget”—\$48.6 million for projects related to “Coping with Information Overload.” The data glut is felt in the NSA’s partner agency in Britain, too. A slideshow entitled “A Short Introduction to SIGINT,” from GCHQ, the British intelligence agency, posed the following question: “How are people supposed to keep on top of all their targets and the new ones when they have far more than [they] could do in a day? How are they supposed to find the needle in the haystack and prioritise what is most important to look at?”

The slideshow continued, “Give an analyst three leads, one of which is interesting: they may have time to follow that up. Give them three hundred leads, ten of which are interesting: that's probably not much use.”

These documents tend to shy away from confrontation—they express concern with the status quo but do not blame senior officials or demand an abrupt change of course. They were written by agency staffers who appear to believe in the general mission of the NSA. For instance, the author of a “SIGINT Philosopher” column wrote that if the NSA was a corporation, it could have the following mission statement: “building informed decision makers — so that targets do not suffer our nation’s wrath unless they really deserve it — by exercising deity-like monitoring of the target.” On occasion, however, the veil of bureaucratic deference is lowered. In another “SIGINT Philosopher” column, “Cognitive Overflow?,” the author offered a forthright assessment of the haystack problem and the weakness of proposed solutions: “If an individual brain has finite ‘channel capacity,’ does the vast collective of SID, comprised of thousands of brilliant, yet limited, brains also have a definite ‘channel capacity?’ If so, what is it? How do we know when we’ve reached it? What if we’ve already exceeded it? In essence, could SID’s reach exceed its grasp? Can the combined cognitive power of SID connect all the necessary dots to avoid, predict, or advise when the improbable, complex, or unthinkable happens?” The column did not offer an optimistic view. “Take for example the number of tools, clearances, systems, compliances, and administrative requirements we encounter before we even begin to engage in the work of the mission itself,” the column continued.

“The mission then involves an ever-expanding set of complex issues, targets, accesses, and capabilities. The ‘cognitive burden,’ so to speak, must at times feel overwhelming to some of us.” The analyst who wrote the column dismissed, politely but firmly, the typical response of senior officials when they are asked in public about their ability to find needles in their expanding haystack. “Surely someone will point out that the burgeoning amalgam of technological advances will aid us in shouldering the burden,” he noted. “However, historically, this scenario doesn’t seem to completely bear out. The onslaught of more computer power—often intended to automate some processes—has in many respects demanded an expansion of our combined ‘channel capacity’ rather than curbing the flow of the information.”

Mass surveillance collects too much data – hurts the fight against terror

Angwin, award-winning senior reporter at the Wall Street Journal, ’13 (JULIA

ANGWIN, Wall Street Journal, “NSA Struggles to Make Sense of Flood of Surveillance Data”

Dec. 25, 2013 10:30 p.m. ET

<http://www.wsj.com/articles/SB10001424052702304202204579252022823658850> //GY

LAUSANNE, Switzerland— William Binney, creator of some of the computer code used by the National Security Agency to snoop on Internet traffic around the world, delivered an unusual message here in September to an audience worried that the spy agency knows too much.¶ It knows so much, he said, that it can’t understand what it has.¶ “What they are doing is making themselves dysfunctional by taking all this data,” Mr. Binney said at a privacy conference here.¶ The agency is drowning in useless data, which harms its ability to conduct legitimate surveillance, claims Mr. Binney, who rose to the civilian equivalent of a general during more than 30 years at the NSA before retiring in 2001. Analysts are swamped with so much information that they can't do their jobs effectively, and the enormous stockpile is an irresistible temptation for misuse.¶ Mr. Binney’s warning has gotten far less attention than legal questions raised by leaks from former NSA contractor Edward Snowden about the agency’s mass collection of information around the world. Those revelations unleashed a re-examination of the spy agency’s aggressive tactics.¶ But the NSA needs more room to store all the data it collects—and new phone records, data on money transfers and other information keep pouring in. A new storage center being built in Utah will eventually be able to hold more than 100,000 times as much as the contents of printed materials in the Library of Congress, according to outside experts.¶ Some of the documents released by Mr. Snowden detail concerns inside the NSA about drowning in information. An internal briefing

document in 2012 about foreign cellphone-location tracking by the agency said the efforts were "outpacing our ability to ingest, process and store" data.¶ In March 2013, some NSA analysts asked for permission to collect less data through a program called Muscular because the "relatively small intelligence value it contains does not justify the sheer volume of collection," another document shows.¶ In response to questions about Mr. Binney's claims, an NSA spokeswoman says the agency is "not collecting everything, but we do need the tools to collect intelligence on foreign adversaries who wish to do harm to the nation and its allies."¶ Existing surveillance programs were approved by "all three branches of government," and each branch "has a role in oversight," she adds.¶ In a statement through his lawyer, Mr. Snowden says: "When your working process every morning starts with poking around a haystack of seven billion innocent lives, you're going to miss things." He adds: "We're blinding people with data we don't need."¶ A presidential panel recommended earlier this month that the agency shut down its bulk collection of telephone-call records of all Americans. The federal government could accomplish the same goal by querying phone companies, the panel concluded.¶ The panel also recommended the creation of "smart software" that could sort data as the information is collected, rather than the current system where "vast amounts of data are swept up and the sorting is done after it has been copied" on to data-storage systems. Administration officials are reviewing the report.¶ A separate task force is expected to issue its own findings next year, and lawmakers have proposed several bills that would change how the NSA collects and uses data.¶ The 70-year-old Mr. Binney says he is generally underwhelmed by the panel's "bureaucratic" report, though "it would be something meaningful" if the controversy leads to adoption of the "smart software" strategy and creation of a technology oversight group with full access to "be in the knickers of the NSA" and Federal Bureau of Investigation.¶ Mr. Binney lives off his government pension and makes occasional appearances to talk about his work at the NSA.¶ The spy agency has defended its sweeping surveillance programs as essential in the fight against terrorism. But having too much data can hurt those efforts, according to Mr. Binney and a handful of colleagues who have raised concerns since losing an internal battle to build privacy-protecting Internet surveillance tools in the late 1990s.¶

Turns military readiness

Data overload wrecks military readiness and training

Erwin, National Defense Magazine, '12 (Sandra I. Erwin, National Defense Industrial Association, "Too Much Information, Not Enough Intelligence" May 2012, <http://www.nationaldefensemagazine.org/archive/2012/May/Pages/TooMuchInformation,NotEnoughIntelligence.aspx>) //GY

The Defense Department over the last decade has built up an inventory of billions of dollars worth of spy aircraft and battlefield sensors. Those systems create avalanches of data that clog military information networks and overwhelm analysts. ¶ Intelligence experts say the military is drowning in data but not able to convert that information into intelligible reports that break it down and analyze it. ¶ "The challenge for users of intelligence is that all the different types of information come in a stove-piped manner," says Michael W. Isherwood, a defense analyst and former Air Force fighter pilot. ¶ Intelligence feeds include electronic signals, satellite imagery, moving-target data and full-motion video. "How do you integrate this into a clear picture?" Isherwood asks. "That is one of the enduring challenges in the ISR [intelligence, surveillance and reconnaissance] arena for all the services." ¶ Isherwood, the author of a Mitchell Institute white paper, titled, "Layering ISR Forces," cautions that success in future operations hinges on "timely, astute combinations of ISR resources." ¶ The Pentagon would be wise to shift its future investments from sensors to data-analysis tools, he says. ¶ "The awareness gained from integrated, multi-source intelligence data is of supreme value," says Isherwood. ¶ In actual combat, a coherent picture of the battlefield is not a "routine event," he says. "Coalition forces in Afghanistan have suffered losses when they were surprised by a much larger insurgent force not detected in time by ISR assets." ¶ Military drone operators amass untold amounts of data that never is fully analyzed because it is simply too much, Isherwood says. ¶ In the Air Force alone, the buildup of data collectors has been dramatic. While its inventory of fighter, bomber, tanker and transport aircraft shrank by 11 percent over the past decade, ISR platforms — primarily unmanned air vehicles — increased by nearly 300 percent, says Isherwood. ¶ Air Force leaders have recognized this problem and recently decided to cut its future purchases of Reaper drones in half — from 48 to 24 — because there is not enough manpower to operate and process the data from more aircraft. "It didn't make sense to have the production out that far ahead of our ability to actually do the processing and exploitation and dissemination function," Deputy Assistant Secretary of the Air Force for Budget Marilyn Thomas says at a February news conference. ¶ The military services have funded programs to develop software algorithms to automate data analysis, but no silver bullet has emerged. ¶ "Industry is working on tools so you can pull a Google Earth image and incorporate the SIGINT [signals intelligence], the MTI [moving target indicator], visual imagery, full-motion video," Isherwood says. ¶ What the military needs is a "decathlete analyst" that can process multiple feeds, versus an operator for each type of data, he says. Defense Department leaders understand the problem, but the "acquisition community now needs to take that and translate it into systems" that tackle this challenge. ¶ The Air Force is "really good at building an airplane," Isherwood says. But he has yet to see a comparable requirements document or request for technology that meshes all the sensors, he adds. "They go after it piecemeal." ¶ The information deluge problem also is exacerbated by the military's organizational silos that zealously protect their data. ¶ "It's hard to get the community to plug their sensors in," says Gregory G. Wenzel, vice president of advanced enterprise integration at Booz Allen Hamilton. ¶ The so-called "PED" process — processing, exploitation and dissemination — has been a long-

standing challenge, he says. “It’s a really hard problem.” Automated analysis tools for video feeds are gradually entering the market, Wenzel says. The National Football League has developed software to search video archives that some defense contractors are using as a model. One of the more promising systems that could help military ISR operators manage data more efficiently is the DI2E, or defense intelligence information enterprise, says Wenzel. The entire Defense Department and intelligence community will be able to share information, he says. The DI2E is a cloud-based system that draws data from many sensors and databases. Technologies such as DI2E are part of a larger trend toward networking sources of information, says Richard Sterk, senior aerospace and defense analyst at Forecast International. “There’s still too many stand alone legacy systems.” Regardless of advances in technology, he says, a larger conundrum for the military is figuring out how to manage information so commanders and troops in the field don’t become overwhelmed. “They have to sort out how much information is enough,” says Sterk. The Office of Naval Research and the Marine Corps have been experimenting with another approach to analyzing data known as “semantic wiki.” It solves the “intelligence fusion” problem, says George Eanes, vice president of Modus Operandi, a small firm that developed the wiki tool. It’s a rather simple approach. “If I’m looking for something of interest, like a white van, I can search across all the data stores that I have access to,” Eanes says. “It presents it in a wiki format. … It’s a really good tool for pulling the data in from multiple sources and present it in one convenient application.” Semantic wiki can search video, human intelligence reports and satellite imagery. Streaming video could be added in the future, he says. The company has spent the past three to four years working on this technology under several small business innovation research contracts worth about \$5 million, says Eanes. “There has been a cultural shift within the Defense Department toward more desire to share information,” Eanes says. “First they thought the solution was to bring everything into a single database. But that proved impractical. There is too much data,” he says. “Now they’re looking at other solutions. You keep the data where it resides. You access only the data you need.” Former Marine Corps intelligence analyst Tony Barrett, who is now at Modus Operandi, says that during his time on active duty, his team was overwhelmed by data. He would have liked to have had software to scan unstructured data and provide relevant information, based on queries the analyst sets up, he says. “That frees up the analyst to do due diligence rather than extended periods of research,” he adds. “In Iraq, I had individual analysts that all they did was scan reports and find which ones were relevant. … Research is extremely frustrating. I would rather my guys spent more time thinking.” Because of the data overload, “What you end up doing is taking your smartest Marines who would be your biggest help in problem solving to work on your system’s problems,” Barrett says. “I had my smartest guys always be the principal researchers because I was more confident they would be able to discover more data than less talented analysts.” ISR experts also worry that the military has become addicted to full-motion video, at the expense of other intelligence disciplines that might gradually disappear as the number of skilled operators declines. Video imagery is the most “readily understood” intelligence, says Isherwood. For the Iraq and Afghanistan wars, full-motion video provided by aerial sensors was the preferred form of surveillance. But for other combat scenarios in the future, Isherwood says, the military might need to rely on other types of data such as signals intelligence (collection of electronic intercepts or emissions), moving target indicator data (Doppler shifts of moving objects to detect and track targets), radar imagery; and measurement and signals intelligence (combines radar, laser, optical, infrared, acoustic, electromagnetic and atmospheric mediums to identify objects). There is also “cyber-intelligence,” a new discipline that is based on electronic-warfare techniques, says Isherwood. “Full motion video is what everybody wants,” says Chief of Naval Operations Adm. Jonathan Greenert. “A

still picture is good but you still have to send it back, develop it quickly," he says. "Access to full-motion video, however, might not be feasible in every conflict. "Not all fights will be in the desert," says Mel French, vice president of development at Telephonics, a supplier of military sensors and electronic warfare systems. "The unmanned aircraft-mounted sensors that are favored today might not work in other environments. "The second you introduce rain to any of those systems, the range goes down, it limits utility," says French. "We need to think of where else we are going to go," he says. "Possibly places where we need foliage penetration. That's a hard problem to solve." The full-motion video soda straw view works when the area is not being defended by adversaries who can shoot down surveillance aircraft, he says. In instances when ISR assets might be in danger and rather kept at standoff ranges, the military will need analysts who can discern other forms of data such as synthetic aperture radar images, French says. Some field commanders might complain that they "don't understand the [SAR] shadows," he says. They might not realize that video camera pictures can't be obtained from 200 miles away. Images such as SAR require a trained eye. As to whether there will be a time when analysts will be able to produce "actionable" intelligence, French says there are no easy answers. "It's one of those problems that will require years of investments and focus," he says. "We fielded a lot of Band-Aids. Now it's getting back to rationalizing what we fielded."

Excess surveillance data hampers military effectiveness and creates a drag on the economy

Claburn 9 (Thomas, Editor at Large, Enterprise Mobility, 7/9, "Military Grapples With Information Overload," <http://www.informationweek.com/architecture/military-grapples-with-information-overload/d/d-id/1081209?//Tang>)

Surging surveillance data threatens to overwhelm the military's ability to deal with the information. A report from a defense advisory group is calling for new data analysis technology and for taking a cue from Google. Information overload has become a significant challenge for the U.S. military and will require new analysis software and a Google-style cloud infrastructure to manage massive data sets, a U.S. defense advisory group report finds. The December 2008 report, "Data Analysis Challenges," was initially withheld from the public. It was obtained by the Federation of American Scientists' Project on Government Secrecy through a Freedom of Information Act request. The report, written by JASON, a group that provides advice to the Department of Defense (DoD) through the non-profit MITRE Corporation, says that the massive amount of sensor and imagery data being gathered is becoming increasingly difficult to store, analyze, and integrate into defense systems. For example, a DoD surveillance system called Constant Hawk typically produces 10's to 100's of Terabytes of data over a period of a few hours. For that information to be useful, it has to be stored, analyzed, and distributed quickly. The report, however, cites concerns voiced by members of the defense and intelligence communities that much of the surveillance data gathered isn't made useful. "Seventy percent of the data we collect is falling on the floor," MIT defense research scientist Pete Rustan said, according to the report. And the problem is likely to get worse. "As the sensors associated with the various surveillance missions improve, the data volumes are increasing with a projection that sensor data volume could potentially increase to the level of Yottabytes (10^{24} Bytes) by 2015," the report says. Jonathan B. Spira, CEO and chief analyst at research consultancy Basex, author of the forthcoming book Overload!, and organizer of Information Overload Awareness Day on August 12, says information overload is a real problem in the workplace, in government and in the military. "We've seen on the military side, many instances where information overload can create a whole new kind of fog [of war]." he said. Information overload costs the U.S. economy \$900 billion per year, according to Basex. The JASON report discounts some of the more extreme projections about data volume growth and recommends that the DoD deploy infrastructure similar to that used by Google, Microsoft, and Yahoo. It also sees military applications for the Hive language used by Facebook for data warehousing. The major problem the DoD faces

will be in the area of automated information analysis. "The notion of fully automated analysis is today at best a distant reality, and for this reason, it is critical to invest in research to promote algorithmic advances," the report says. "One way to effectively engage the relevant research communities is through the use of grand challenges in the area of data analysis." Spira sees information overload as a broader problem, one that won't vanish with the development of improved automated information analysis technology. He described a cybersecurity conference at a Maxwell Airforce Base, where military brass had gathered to discuss cyber threats. Emerging from the talk, the generals found they had no e-mail, he said. It turned out that the base's e-mail system had been taken down, not by a cyber attack, but by an e-mail about a card game that got forwarded and, through too many reply-alls, multiplied until over a million messages overloaded the e-mail servers. "We need to address a lot of different aspects of data and information overload, not just things that sound sexy," said Spira.

Data collection has reached the neurological breaking point – additional data will make it impossible to function in the field

Shanker and Ritchel 11 (Thom and Matt, writers for the NYT, cites psychologists and neuroscientists, 1/16, "In New Military, Data Overload Can Be Deadly," http://www.nytimes.com/2011/01/17/technology/17brain.html?pagewanted=all&_r=0//Tang)

When military investigators looked into an attack by American helicopters last February that left 23 Afghan civilians dead, they found that the operator of a Predator drone had failed to pass along crucial information about the makeup of a gathering crowd of villagers. But Air Force and Army officials now say there was also an underlying cause for that mistake: information overload. At an Air Force base in Nevada, the drone operator and his team struggled to work out what was happening in the village, where a convoy was forming. They had to monitor the drone's video feeds while participating in dozens of instant-message and radio exchanges with intelligence analysts and troops on the ground. There were solid reports that the group included children, but the team did not adequately focus on them amid the swirl of data — much like a cubicle worker who loses track of an important e-mail under the mounting pile. The team was under intense pressure to protect American forces nearby, and in the end it determined, incorrectly, that the villagers' convoy posed an imminent threat, resulting in one of the worst losses of civilian lives in the war in Afghanistan. "Information overload — an accurate description," said one senior military officer, who was briefed on the inquiry and spoke on the condition of anonymity because the case might yet result in a court martial. The deaths would have been prevented, he said, "if we had just slowed things down and thought deliberately." Data is among the most potent weapons of the 21st century. Unprecedented amounts of raw information help the military determine what targets to hit and what to avoid. And drone-based sensors have given rise to a new class of wired warriors who must filter the information sea. But sometimes they are drowning. Research shows that the kind of intense multitasking required in such situations can make it hard to tell good information from bad. The military faces a balancing act: how to help soldiers exploit masses of data without succumbing to overload. Across the military, the data flow has surged; since the attacks of 9/11, the amount of intelligence gathered by remotely piloted drones and other surveillance technologies has risen 1,600 percent. On the ground, troops increasingly use hand-held devices to communicate, get directions and set bombing coordinates. And the screens in jets can be so packed with data that some pilots call them "drool buckets" because, they say, they can get lost staring into them. "There is information overload at every level of the military — from the general to the soldier on the ground," said Art Kramer, a neuroscientist and director of the Beckman Institute, a research lab at the University of Illinois. The military has engaged researchers like Mr. Kramer to help it understand the brain's limits and potential. Just as the military has long pushed technology forward, it is now at the forefront in figuring out how humans can cope with technology without being overwhelmed by it. At George Mason University in Virginia, researchers measure the brain waves of study subjects as they use a simulation of the work done at the Nevada Air Force base. On a computer screen, the subjects see a video feed from one drone and the locations of others, along with instructions on where to direct them. The subjects wear a cap with electrodes attached, measuring brain waves. As the number of drones and the pace of instructions increases, the brain shows sharp spikes in a kind of electrical activity called theta — cause for concern among the researchers. "It's usually an index of extreme overload," said Raja Parasuraman, a director of the

university's human factors and applied cognition program. As the technology allows soldiers to pull in more information, it strains their brains. And military researchers say the stress of combat makes matters worse. Some research even suggests that younger people wind up having more trouble focusing because they have grown up constantly switching their attention. For the soldier who has been using computers and phones all his life, "multitasking might actually have negative effects," said Michael Barnes, research psychologist at the Army Research Lab at Aberdeen, Md., citing several university studies on the subject. In tests at a base in Orlando, Mr. Barnes's group has found that when soldiers operate a tank while monitoring remote video feeds, they often fail to see targets right around them. Mr. Barnes said soldiers could be trained to use new technology, "but we're not going to improve the neurological capability." On the other hand, he said, the military should not shy away from improving the flow of data in combat. "It would be like saying we shouldn't have automobiles because we have 40,000 people die on the roads each year," he said. "The pluses of technology are too great." The military is trying novel approaches to helping soldiers focus. At an Army base on Oahu, Hawaii, researchers are training soldiers' brains with a program called "mindfulness-based mind fitness training." It asks soldiers to concentrate on a part of their body, the feeling of a foot on the floor or of sitting on a chair, and then move to another focus, like listening to the hum of the air-conditioner or passing cars. "The whole question we're asking is whether we can rewire the functioning of the attention system through mindfulness," said one of the researchers, Elizabeth A. Stanley, an assistant professor of security studies at Georgetown University. Recently she received financing to bring the training to a Marine base, and preliminary results from a related pilot study she did with Amishi Jha, a neuroscientist at the University of Miami, found that it helped Marines to focus. Even as it worries about digital overload, the Army is acknowledging that technology may be the best way to teach this new generation of soldiers — in particular, a technology that is already in their pockets. In Army basic training, new recruits can get instruction from iPhone apps on subjects as varied as first aid and military values. As part of the updated basic training regimen, recruits are actually forced into information overload — for example, testing first aid skills while running an obstacle course. "It's the way this generation learns," said Lt. Gen. Mark P. Hertling, who oversees initial training for every soldier. "It's a multitasking generation. So if they're multitasking and combining things, that's the way we should be training." The intensity of warfare in the computer age is on display at a secret intelligence and surveillance installation at Langley Air Force Base in Virginia, a massive, heavily air-conditioned warehouse where hundreds of TVs hang from black rafters. Every day across the Air Force's \$5 billion global surveillance network, cubicle warriors review 1,000 hours of video, 1,000 high-altitude spy photos and hundreds of hours of "signals intelligence" — usually cellphone calls. At the Langley center, officially called Distributed Common Ground System-1, heavy multitasking is a daily routine for people like Josh, a 25-year-old first lieutenant (for security reasons, the Air Force would not release his full name). For 12 hours a day, he monitors an avalanche of images on 10 overhead television screens. They deliver what Josh and his colleagues have nicknamed "Death TV" — live video streams from drones above Afghanistan showing Taliban movements, suspected insurgent safehouses and American combat units headed into battle. As he watches, Josh uses a classified instant-messaging system showing as many as 30 different chats with commanders at the front, troops in combat and headquarters at the rear. And he is hearing the voice of a pilot at the controls of a U-2 spy plane high in the stratosphere. "I'll have a phone in one ear, talking to a pilot on the headset in the other ear, typing in chat at the same time and watching screens," Josh says. "It's intense." The stress lingers when the shift is over. Josh works alongside Anthony, 23, an airman first class who says his brain hurts each night, the way feet ache after a long march. "You have so much information coming in that when you go home — how do you take that away? Sometimes I work out," Anthony said. "Actually, one of my things is just being able to enjoy a nice bowl of cereal with almond milk. I feel the tension is just gone and I can go back again." Video games don't do the trick. "I need something real," he said.

We've gotta deal with overload now to improve counterterrorism long term Shanker and Richtel, 11

(Thom and Matt, Graduate Tufts University - The Fletcher School of Law and Diplomacy, Pulitzer prize winning author, New York Times, 1-16-11, "In New Military, Data Overload Can Be Deadly", <http://www.umsl.edu/~sauterv/DSS4BI/links/17brain.pdf>, amp)

Mr. Barnes said soldiers could be trained to use new technology, "but we're not going to improve the neurological capability." On the other hand, he said, the military should not shy away from improving the flow of data in combat. "It would be like saying we shouldn't have automobiles because we have 40,000 people die on the roads each year," he said. "The pluses of technology are too great."

Internet Freedom

The NSA's PRISM program is being used to collect surveillance data from US companies – this overreach undermines US soft power and credibility on internet freedom

Wheeler, 14 - Marcy Wheeler is an independent journalist and PhD from the University of Michigan. She specializes in civil liberties, technology, and national security. (Marcy, "The Drama Ahead: Google versus America" 6/16, <http://www.cato-unbound.org/2014/06/16/marcy-wheeler/drama-ahead-google-versus-america>

This leaves one central drama to play out, in which Google and other tech companies (and to a much lesser extent, a few telecoms) begin to push back against the NSA's overreach. It's not just that U.S. cloud (and other tech) companies stand to lose billions as their clients choose to store data locally rather than expose it easily to the NSA. It's also that the NSA violated several aspects of the deal the Executive Branch made six years ago with the passage of the FISA Amendments Act (FAA), Section 702 of which authorizes the PRISM program and domestic upstream collection.

Congress passed the FISA Amendments Act several years after the New York Times' exposure of the illegal wiretap program, ostensibly to address a technical problem used to justify that program. Technology had changed since the analog and radio world in place when FISA was first passed in 1978. Now, much of the world's communications – including those of extremists who were targeting America – were sitting in Google's and Yahoo's and Microsoft's servers within the United States. So Congress authorized the NSA to conduct collection inside the United States on targets located outside of the country (which swept up those who communicated with those targets, wherever they were located). In exchange, the government and its supporters promised, it would extend protections to Americans who were overseas.

Yahoo and Google played by the rules, as the PRISM slide released last June revealed. The data of both Yahoo and Google have been readily available for any of the broad uses permitted by the law since January 2009. Yet, in spite of the fact that the NSA has a legal way to obtain this Internet data inside the United States using PRISM, the government also broke in to steal from Yahoo and Google fiber overseas.

That's an important implication of Sanchez' point that "modern communications networks obliterate many of the assumptions about the importance of geography." American tech companies now store data overseas, as well as in the United States. Americans' data is mixed in with foreigners' data overseas. Many of the more stunning programs described by Snowden's documents – the collection of 5 billion records a day showing cell location, NSA partner GCHQ's collection of millions of people's intimate webcam images, and, of course, the theft of data from Google and Yahoo's servers – may suck up Americans' records too.

Plus there's evidence the NSA is accessing U.S. person data overseas. The agency permits specially trained analysts to conduct Internet metadata contact chaining including the records of Americans from data collected overseas. And in a Senate Intelligence Committee hearing earlier

this year, Colorado Senator Mark Udall asked hypothetically what would happen with a “a vast trove of U.S. person information” collected overseas; the answer was such data would not get FISA protection (California Senator Dianne Feinstein, the Intelligence Committee Chair, asked an even more oblique question on the topic).

Udall and Feinstein’s questions show that a lot of this spying does not undergo the oversight Benjamin Wittes and Carrie Cordero point to. Last year, Feinstein admitted her committee gets less reporting on such spying. Even for programs overseen by FISA, the NSA has consistently refused to provide even its oversight committees and the FISA Court real numbers on how many Americans get sucked into various NSA dragnets.

Moreover, the government’s threat to tech companies exists not just overseas. When a group of tech companies withdrew their support for the USA Freedom Act, they argued the bill could permit the resumption of bulk collection of Internet users’ data domestically. In the past, that has always meant telecoms copying Internet metadata at telecom switches, another outside entity compromising tech companies’ services. As with the data stolen overseas, Internet metadata is available to the government legally under PRISM.

In response to the news that the government at times bypasses the legal means it has to access Google’s clients’ data, the tech giant and others have found new ways to protect their customers. That consists of the new encryption Sanchez described – both of that fiber compromised overseas and of emails sent using Google – but also the right to publish how much data the government collects. Even within the criminal context, tech companies (including telecoms Verizon and AT&T) are challenging the U.S. government’s efforts to use tech companies’ presence in the United States to get easy access to customers’ data overseas.

The conflict between Google and its home country embodies another trend that has accelerated since the start of the Snowden leaks. As the President of the Computer & Communications Industry Association, Edward Black, testified before the Senate last year, the disclosure of NSA overreach did not just damage some of America’s most successful companies, it also undermined the key role the Internet plays in America’s soft power projection around the world: as the leader in Internet governance, and as the forum for open speech and exchange once associated so positively with the United States.

The U.S. response to Snowden’s leaks has, to a significant degree, been to double down on hard power, on the imperative to “collect it all” and the insistence that the best cyberdefense is an aggressive cyberoffense. While President Obama paid lip service to stopping short of spying “because we can,” the Executive Branch has refused to do anything – especially legislatively – that would impose real controls on the surveillance system that undergirds raw power.

And that will likely bring additional costs, not just to America’s economic position in the world, but in the need to invest in programs to maintain that raw power advantage. Particularly given the paltry results the NSA has to show for its domestic phone dragnet – the single Somali taxi driver donating to al-Shabaab that Sanchez described. It’s not clear that the additional costs from doubling down on hard power bring the United States any greater security.

The perception that the NSA is using Executive Order 12333 to circumvent section 702 of the FISA Amendments Act is causing a backlash against US tech companies and driving global data localization. Limiting authority to Section 702 provides the oversight protections of the FISA, which the Executive Order leaves out

Eoyang, 14 - Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto) ("A Modest Proposal: FAA Exclusivity for Collection Involving U.S. Technology Companies" Lawfare, 11/24, <http://www.lawfareblog.com/modest-proposal-faa-exclusivity-collection-involving-us-technology-companies>

Beyond 215 and FAA, media reports have suggested that there have been collection programs that occur outside of the companies' knowledge. **American technology companies have been outraged about media stories of US government intrusions onto their networks overseas, and the spoofing of their web pages or products, all unbeknownst to the companies.** These stories suggest that the government is creating and sneaking through a back door to take the data. As one tech employee said to me, "the back door makes a mockery of the front door."

As a result of these allegations, companies are moving to encrypt their data against their own government; they are limiting their cooperation with NSA; and they are pushing for reform. Negative international reactions to media reports of certain kinds of intelligence collection abroad have resulted in a backlash against American technology companies, spurring data localization requirements, rejection or cancellation of American contracts, and raising the specter of major losses in the cloud computing industry. These allegations could dim one of the few bright spots in the American economic recovery: tech.

Without commenting on the accuracy of these media reports, **the perception is still a problem even if the media reports of these government collection programs are not true---or are only partly true. The tech industry believes them to be true**, and more importantly, **their customers at home and abroad believe them to be true, and that means they have huge impact on American business and huge impact as well on the relationship between these businesses and an intelligence community that depends on their cooperation.**

So, how should we think about reforms in response to this series of allegations the Executive Branch can't, or won't, address? **How about making the FAA the exclusive means for conducting electronic surveillance when the information being collected is in the custody of an American company? This could clarify that the executive branch could not play authority shell-games and claim that Executive Order 12333 allows it to obtain information on overseas non-US person targets that is in the custody of American companies**, unbeknownst to those companies.

As a policy matter, it seems to me that **if the information to be acquired is in the custody of an American company, the intelligence community should ask for it, rather than take it without asking. American companies should be entitled to a higher degree of forthrightness from their government than foreign companies, even when they are acting overseas. Under the FAA, we have a statutory regime that creates judicial oversight and accountability to conduct electronic**

surveillance outside the US for specific purposes: foreign intelligence (or traditional espionage), counter-terrorism, and prevention of WMD proliferation. It addresses protections for both non-US and US persons. It creates a front-door, though compelled, relationship under which the intelligence community can receive communications contents without individual warrants but with programmatic judicial oversight.

FAA exclusivity would say to the rest of the world that when the US conducts bulk electronic surveillance overseas, we are doing so for a particular, national security purpose. The FAA structure with FISC review provides an independent check that the statutory purposes are met. Through transparency agreements with the government, the American companies are able to provide their customers with some sense of how many requests are made.

This would not change the 12333 authorities with respect to non-US companies. It would also not change 12333 authorities when the Executive Branch seeks to obtain the information in some other way than through the US company (i.e. breaking into the target's laptop, parking a surveillance van outside their house, sending a spy, etc.).

Some have asked me what would happen if foreign companies tried to set up shop here in the US to seek these protections. I need to refine this part further, but would look to other statutory regimes that need to define the nationality of companies, like the Foreign Corrupt Practices Act, or the CFIUS process. Executive Order 12333 itself offers a partial answer, defining a US person to include "a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."

Others may argue that FAA provides inadequate civil liberties protections. This proposal says nothing about the adequacy of that statute. What it says is that for data held by an American company about a target that is not a US person, the checks within FAA are stronger than those under 12333 acting alone.

That perception prevents the US from stopping data localization globally

Kehl, 14 – Policy Analyst at New America's Open Technology Institute (Danielle, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

Costs to the Internet Freedom Agenda and U.S. Credibility in Internet Governance

"As the birthplace for so many of these technologies, including the internet itself, we have a responsibility to see them used for good," declared Secretary of State Hillary Clinton in January 2010.¹⁷⁵ Her speech at the Newseum in Washington DC effectively launched the United States' Internet Freedom agenda, articulating a leading role for the U.S. in using the Internet to promote freedom of expression, freedom of worship, and the freedom to connect around the world. Clinton went on to give two other major addresses on Internet Freedom, becoming the first global leader to emphasize Internet Freedom as a foreign policy priority and urging "countries everywhere... to join us in the bet we have made, a bet that an open internet will lead to stronger, more prosperous countries."¹⁷⁶ As Richard Fontaine and Will Rogers describe in a seminal paper

on the subject in June 2011, “Internet Freedom, broadly defined, is the notion that universal rights, including the freedoms of expression, assembly and association, extend to the digital sphere.”¹⁷⁷

Although there were questions from the beginning about whether the United States would hold itself to the same high standards domestically that it holds others to internationally,¹⁷⁸ the American government has successfully built up a policy and programming agenda in the past few years based on promoting an open Internet.¹⁷⁹ These efforts include raising concerns over Internet repression in bilateral dialogues with countries such as Vietnam and China,¹⁸⁰ supporting initiatives including the Freedom Online Coalition, and providing over \$120 million in funding for “groups working to advance Internet freedom – supporting counter-censorship and secure communications technology, digital safety training, and policy and research programs for people facing Internet repression.”¹⁸¹ However, the legitimacy of these efforts has been thrown into question since the NSA disclosures began. “Trust has been the principal casualty in this unfortunate affair,” wrote Ben FitzGerald and Richard Butler in December 2013. “The American public, our nation’s allies, leading businesses and Internet users around the world are losing faith in the U.S. government’s role as the leading proponent of a free, open and integrated global Internet.”¹⁸²

Prior to the NSA revelations, the United States was already facing an increasingly challenging political climate as it promoted the Internet Freedom agenda in global Internet governance conversations. At the 2012 World Conference on International Telecommunications (WCIT), the U.S. and diverse group of other countries refused to sign the updated International Telecommunications Regulations based on concerns that the document pushed for greater governmental control of the Internet and would ultimately harm Internet Freedom.¹⁸³ Many observers noted that the split hardened the division between two opposing camps in the Internet governance debate: proponents of a status quo multistakeholder Internet governance model, like the United States, who argued that the existing system was the best way to preserve key online freedoms, and those seeking to disrupt or challenge that multistakeholder model for a variety of political and economic reasons, including governments like Russia and China pushing for greater national sovereignty over the Internet.¹⁸⁴ Many of the proposals for more governmental control over the network could be understood as attempts by authoritarian countries to more effectively monitor and censor their citizens, which allowed the U.S. to reasonably maintain some moral high ground as its delegates walked out of the treaty conference.¹⁸⁵ Although few stakeholders seemed particularly pleased by the outcome of the WCIT, reports indicate that by the middle of 2013 the tone had shifted in a more collaborative and positive direction following the meetings of the 2013 World Telecommunications/ICT Policy Forum (WTPF) and the World Summit on Information Society + 10 (WSIS+10) review.¹⁸⁶

However, the Internet governance conversation took a dramatic turn after the Snowden disclosures. The annual meeting of the Freedom Online Coalition occurred in Tunis in June 2013, just a few weeks after the initial leaks. Unsurprisingly, surveillance dominated the conference even though the agenda covered a wide range of topics from Internet access and affordability to cybersecurity.¹⁸⁷ Throughout the two-day event, representatives from civil society used the platform to confront and criticize governments about their monitoring practices.¹⁸⁸ NSA surveillance would continue to be the focus of international convenings on Internet Freedom and Internet governance for months to come, making civil society representatives and foreign governments far less willing to embrace the United States’ Internet Freedom agenda or to accept

its defense of the multistakeholder model of Internet governance as anything other than self-serving. “One can come up with all kinds of excuses for why US surveillance is not hypocrisy. For example, one might argue that US policies are more benevolent than those of many other regimes... And one might recognize that in several cases, some branches of government don’t know what other branches are doing... and therefore US policy is not so much hypocritical as it is inadvertently contradictory,” wrote Eli Dourado, a researcher from the Mercatus Center at George Mason University in August 2013. “But the fact is that the NSA is galvanizing opposition to America’s internet freedom agenda.”¹⁸⁹ The scandal revived proposals from both Russia and Brazil for global management of technical standards and domain names, whether through the ITU or other avenues. Even developing countries, many of whom have traditionally aligned with the U.S. and prioritize access and affordability as top issues, “don’t want US assistance because they assume the equipment comes with a backdoor for the NSA. They are walking straight into the arms of Russia, China, and the ITU.”¹⁹⁰

Consequently, NSA surveillance has shifted the dynamics of the Internet governance debate in a potentially destabilizing manner. The Snowden revelations “have also been well-received by those who seek to discredit existing approaches to Internet governance,” wrote the Center for Democracy & Technology’s Matthew Shears. “There has been a long-running antipathy among a number of stakeholders to the United States government’s perceived control of the Internet and the dominance of US Internet companies. There has also been a long-running antipathy, particularly among some governments, to the distributed and open management of the Internet.”¹⁹¹ Shears points out that evidence of the NSA’s wide-ranging capabilities has fueled general concerns about the current Internet governance system, bolstering the arguments of those calling for a new government-centric governance order. At the UN Human Rights Council in September 2013, the representative from Pakistan—speaking on behalf of Cuba, Venezuela, Zimbabwe, Uganda, Ecuador, Russia, Indonesia, Bolivia, Iran, and China—explicitly linked the revelations about surveillance programs to the need for reforming Internet governance processes and institutions to give governments a larger role.¹⁹² Surveillance issues continued to dominate the conversation at the 2013 Internet Governance Forum in Bali as well, where “debates on child protection, education and infrastructure were overshadowed by widespread concerns from delegates who said the public’s trust in the internet was being undermined by reports of US and British government surveillance.”¹⁹³

Further complicating these conversations is the fact that several of the institutions that govern the technical functions of the Internet are either tied to the American government or are located in the United States. Internet governance scholar Milton Mueller has described how the reaction to the NSA disclosures has become entangled in an already contentious Internet governance landscape. Mueller argues that, in addition to revealing the scale and scope of state surveillance and the preeminent role of the United States and its partners, the NSA disclosures may push other states toward a more nationally partitioned Internet and “threaten... in a very fundamental way the claim that the US had a special status as neutral steward of Internet governance.”¹⁹⁴ These concerns were publicly voiced in October 2013 by the heads of a number of key organizations, including the President of the Internet Corporation for Assigned Names and Numbers (ICANN) and the chair of the Internet Engineering Task Force (IETF), in the Montevideo Statement on the Future of Internet Cooperation. Their statement expressed “strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance” and “called for accelerating the globalization of ICANN and Internet Assigned Numbers Authority (IANA) functions, towards an environment in which all

stakeholders, including all governments, participate on an equal footing.”¹⁹⁵ In particular, the process of internationalizing ICANN—which has had a contractual relationship with the Commerce Department’s National Telecommunications and Information Association (NTIA) since 1998—has progressed in recent months.¹⁹⁶

That will collapse the global internet

Chandler and Le, 15 - * Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND **Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, “DATA NATIONALISM” 64 Emory L.J. 677, <http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html> DOA: 7-31-15

The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, **breaking apart the World Wide Web.** The first generation of Internet border controls sought to keep information out of a country - from Nazi paraphernalia to copyright infringing material. n1 The new generation of Internet border controls seeks not to keep information out but rather to keep data in. Where the first generation was relatively narrow in the information excluded, the new generation seeks to keep all data about individuals within a country.

Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies. n2 Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands. n3 As the argument [*680] goes, placing data in other nations jeopardizes the security and privacy of such information. We define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms - including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data. We argue here that data localization will backfire and that it in fact undermines privacy and security, while still leaving data vulnerable to foreign surveillance. Even more importantly, data localization increases the ability of governments to surveil and even oppress their own populations.

Imagine an Internet where data must stop at national borders, examined to see whether it is allowed to leave the country and possibly taxed when it does. While this may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders. Countries around the world are in the process of creating Checkpoint Charlies - not just for highly secret national security data but for ordinary data about citizens. The very nature of the World Wide Web is at stake. We will show how countries across the world have implemented or have planned dramatic steps to curtail the flow of information outside their borders. By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. n4 The Internet

is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders. n5 Thus, the services built on the Internet, from email to the World [*681] Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making the physical locations for the storage and processing of their data largely invisible to users. Data localization would dramatically alter this fundamental architecture of the Internet.

Such a change poses a mortal threat to the new kind of international trade made possible by the Internet - information services such as those supplied by Bangalore or Silicon Valley. n6 Barriers of distance or immigration restrictions had long kept such services confined within national borders. But the new services of the Electronic Silk Road often depend on processing information about the user, information that crosses borders from the user's country to the service provider's country. Data localization would thus require the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs and other burdens enormously for both providers and consumers and rendering many of such global services impossible.

While others have observed some of the hazards of data localization, especially for American companies, n7 this Article offers three major advances over earlier work in the area. First, while the earlier analyses have referred to a data localization measure in a country in the most general of terms, our Article provides a detailed legal description of localization measures. Second, by examining a variety of key countries around the world, the study allows us to see the forms in which data localization is emerging and the justifications offered for such measures in both liberal and illiberal states. Third, the Article works to comprehensively refute the various arguments for data localization offered around the world, showing that data localization measures are in fact likely to undermine security, privacy, economic development, and innovation where adopted.

[*682] Our paper proceeds as follows. Part I describes the particular data localization measures in place or proposed in different countries around the world, as well as in the European Union. Part II then discusses the justifications commonly offered for these measures - such as avoiding foreign surveillance, enhancing security and privacy, promoting economic development, and facilitating domestic law enforcement. We appraise these arguments, concluding that, in fact, such measures are likely to backfire on all fronts. Data localization will erode privacy and security without rendering information free of foreign surveillance, while at the same time increasing the risks of domestic surveillance.

A free internet is vital to combating every existential threat

Eagleman, 10 - American neuroscientist and writer at Baylor College of Medicine, where he directs the Laboratory for Perception and Action and the Initiative on Neuroscience and Law (David, “Six ways the internet will save civilization” Wired, 9/10,
<http://www.wired.co.uk/magazine/archive/2010/12/start/apocalypse-no>

Many great civilisations have fallen, leaving nothing but cracked ruins and scattered genetics. Usually this results from: natural disasters, resource depletion, economic meltdown, disease, poor information flow and corruption. But we’re luckier than our predecessors because we command a

technology that no one else possessed: a rapid communication network that finds its highest expression in the internet. I propose that there are six ways in which the net has vastly reduced the threat of societal collapse.

Epidemics can be deflected by telepresence

One of our more dire prospects for collapse is an infectious-disease epidemic. Viral and bacterial epidemics precipitated the fall of the Golden Age of Athens, the Roman Empire and most of the empires of the Native Americans. The internet can be our key to survival because the ability to work telepresently can inhibit microbial transmission by reducing human-to-human contact. In the face of an otherwise devastating epidemic, businesses can keep supply chains running with the maximum number of employees working from home. This can reduce host density below the tipping point required for an epidemic. If we are well prepared when an epidemic arrives, we can fluidly shift into a self-quarantined society in which microbes fail due to host scarcity. Whatever the social ills of isolation, they are worse for the microbes than for us.

The internet will predict natural disasters

We are witnessing the downfall of slow central control in the media: news stories are increasingly becoming user-generated nets of up-to-the-minute information. During the recent California wildfires, locals went to the TV stations to learn whether their neighbourhoods were in danger. But the news stations appeared most concerned with the fate of celebrity mansions, so Californians changed their tack: they uploaded geotagged mobile-phone pictures, updated Facebook statuses and tweeted. The balance tipped: the internet carried news about the fire more quickly and accurately than any news station could. In this grass-roots, decentralised scheme, there were embedded reporters on every block, and the news shockwave kept ahead of the fire. This head start could provide the extra hours that save us. If the Pompeians had had the internet in 79AD, they could have easily marched 10km to safety, well ahead of the pyroclastic flow from Mount Vesuvius. If the Indian Ocean had the Pacific's networked tsunami-warning system, South-East Asia would look quite different today.

Discoveries are retained and shared

Historically, critical information has required constant rediscovery. Collections of learning -- from the library at Alexandria to the entire Minoan civilisation -- have fallen to the bonfires of invaders or the wrecking ball of natural disaster. Knowledge is hard won but easily lost. And information that survives often does not spread. Consider smallpox inoculation: this was under way in India, China and Africa centuries before it made its way to Europe. By the time the idea reached North America, native civilisations who needed it had already collapsed. The net solved the problem. New discoveries catch on immediately; information spreads widely. In this way, societies can optimally ratchet up, using the latest bricks of knowledge in their fortification against risk.

Tyranny is mitigated

Censorship of ideas was a familiar spectre in the last century, with state-approved news outlets ruling the press, airwaves and copying machines in the USSR, Romania, Cuba, China, Iraq and elsewhere. In many cases, such as Lysenko's agricultural despotism in the USSR, it directly contributed to the collapse of the nation. Historically, a more successful strategy has been to confront free speech with free speech -- and the internet allows this in a natural way. It

democratises the flow of information by offering access to the newspapers of the world, the photographers of every nation, the bloggers of every political stripe. Some posts are full of doctoring and dishonesty whereas others strive for independence and impartiality -- but all are available to us to sift through. Given the attempts by some governments to build firewalls, it's clear that this benefit of the net requires constant vigilance.

Human capital is vastly increased

Crowdsourcing brings people together to solve problems. Yet far fewer than one per cent of the world's population is involved. We need expand human capital. Most of the world not have access to the education afforded a small minority. For every Albert Einstein, Yo-Yo Ma or Barack Obama who has educational opportunities, uncountable others do not. This squandering of talent translates into reduced economic output and a smaller pool of problem solvers. The net opens the gates education to anyone with a computer. A motivated teen anywhere on the planet can walk through the world's knowledge -- from the webs of Wikipedia to the curriculum of MIT's OpenCourseWare. The new human capital will serve us well when we confront existential threats we've never imagined before.

Energy expenditure is reduced

Societal collapse can often be understood in terms of an energy budget: when energy spend outweighs energy return, collapse ensues. This has taken the form of deforestation or soil erosion; currently, the worry involves fossil-fuel depletion. The internet addresses the energy problem with a natural ease. Consider the massive energy savings inherent in the shift from paper to electrons -- as seen in the transition from the post to email. Ecommerce reduces the need to drive long distances to purchase products. Delivery trucks are more eco-friendly than individuals driving around, not least because of tight packaging and optimisation algorithms for driving routes. Of course, there are energy costs to the banks of computers that underpin the internet -- but these costs are less than the wood, coal and oil that would be expended for the same quantity of information flow.

The tangle of events that triggers societal collapse can be complex, and there are several threats the net does not address. But vast, networked communication can be an antidote to several of the most deadly diseases threatening civilisation. The next time your coworker laments internet addiction, the banality of tweeting or the decline of face-to-face conversation, you may want to suggest that the net may just be the technology that saves us.

Surveillance overreach spills over to gut overall US global legitimacy

Kehl, 14 – Policy Analyst at New America's Open Technology Institute (Danielle, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

Broader Foreign Policy Costs

Beyond Internet Freedom, the NSA disclosures "have badly undermined U.S. credibility with many of its allies," Ian Bremmer argued in Foreign Policy in November 2013.²¹⁴ Similarly, as

Georg Mascolo and Ben Scott point out about the post-Snowden world, “the shift from an open secret to a published secret is a game changer... it exposes the gap between what governments will tolerate from one another under cover of darkness and what publics will tolerate from other governments in the light of day.”²¹⁵ From stifled negotiations with close allies like France and Germany to more tense relations with emerging powers including Brazil and China, the leaks have undoubtedly weakened the American position in international relations, opening up the United States to new criticism and political maneuvering that would have been far less likely a year ago.²¹⁶

U.S. allies like France, Israel, and Germany are upset by the NSA’s actions, as their reactions to the disclosures make clear.²¹⁷ Early reports about close allies threatening to walk out of negotiations with the United States—such as calls by the French government to delay EU-U.S. trade talks in July 2013 until the U.S. government answered European questions about the spying allegations²¹⁸—appear to be exaggerated, but there has certainly been fallout from the disclosures. For months after the first Snowden leaks, German Chancellor Angela Merkel would not visit the United States until the two countries signed a “no-spy” agreement—a document essentially requiring the NSA to respect German law and rights of German citizens in its activities. When Merkel finally agreed come to Washington, D.C. in May 2014, tensions rose quickly because the two countries were unable to reach an agreement on intelligence sharing, despite the outrage provoked by news that the NSA had monitored Merkel’s own communications.²¹⁹ Even as Obama and Merkel attempted to present a unified front while they threatened additional sanctions against Russia over the crisis in the Ukraine, it was evident that relations are still strained between the two countries. While President Obama tried to keep up the appearance of cordial relations at a joint press conference, Merkel suggested that it was too soon to return to “business as usual” when tensions still remain over U.S. spying allegations.²²⁰ The Guardian called the visit “frosty” and “awkward.”²²¹ The German Parliament has also begun hearings to investigate the revelations and suggested that it is weighing further action against the United States.²²²

Moreover, the disclosures have weakened the United States’ relationship with emerging powers like Brazil, where the fallout from NSA surveillance threatens to do more lasting damage. Brazilian President Dilma Rousseff has seized on the NSA disclosures as an opportunity to broaden Brazil’s influence not only in the Internet governance field, but also on a broader range of geopolitical issues. Her decision not to attend an October 2013 meeting with President Barack Obama at the White House was a direct response to NSA spying—and a serious, high-profile snub. In addition to cancelling what would have been the first state visit by a Brazilian president to the White House in nearly 20 years, Rousseff’s decision marked the first time a world leader had turned down a state dinner with the President of the United States.²²³ In his statement on the postponement, President Obama was forced to address the issue of NSA surveillance directly, acknowledging “that he understands and regrets the concerns disclosures of alleged U.S. intelligence activities have generated in Brazil and made clear that he is committed to working together with President Rousseff and her government in diplomatic channels to move beyond this issue as a source of tension in our bilateral relationship.”²²⁴

Many observers have noted that the Internet Freedom agenda could be one of the first casualties of the NSA disclosures. The U.S. government is fighting an uphill battle at the moment to regain credibility in international Internet governance debates and to defend its moral high ground as a critic of authoritarian regimes that limit freedom of expression and violate human rights online.

Moreover, the fallout from the NSA's surveillance activities has spilled over into other areas of U.S. foreign policy and currently threatens bilateral relations with a number of key allies. Going forward, it is critical that decisions about U.S. spying are made in consideration of a broader set of interests so that they do not impede—or, in some cases, completely undermine U.S. foreign policy goals.

Legitimacy key to global stability - prevents great power war

Fujimoto 12 (Kevin Fujimoto 12, Lt. Colonel, U.S. Army, January 11, 2012, "Preserving U.S. National Security Interests Through a Liberal World Construct," online: <http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Preserving-US-National-Security-Interests-Liberal-World-Construct/2012/1/11>)

The emergence of peer competitors, not terrorism, presents the greatest long-term threat to our national security. Over the past decade, while the United States concentrated its geopolitical focus on fighting two land wars in Iraq and Afghanistan, China has quietly begun implementing a strategy to emerge as the dominant imperial power within Southeast Asia and the Indian Ocean. Within the next 2 decades, China will likely replace the United States as the Asia-Pacific regional hegemonic power, if not replace us as the global superpower.¹ Although China presents its rise as peaceful and non-hegemonic, its construction of naval bases in neighboring countries and military expansion in the region contradict that argument.

With a credible threat to its leading position in a unipolar global order, the United States should adopt a grand strategy of “investment,” building legitimacy and capacity in the very institutions that will protect our interests in a liberal global construct of the future when we are no longer the dominant imperial power. Similar to the Clinton era's grand strategy of “enlargement,”² investment supports a world order predicated upon a system of basic rules and principles, however, it differs in that the United States should concentrate on the institutions (i.e., United Nations, World Trade Organization, ASEAN, alliances, etc.) that support a world order, as opposed to expanding democracy as a system of governance for other sovereign nations.

Despite its claims of a benevolent expansion, China is already executing a strategy of expansion similar to that of Imperial Japan's Manchukuo policy during the 1930s.³ This three-part strategy involves: “(i) (providing) significant investments in economic infrastructure for extracting natural resources; (ii) (conducting) military interventions (to) protect economic interests; and, (iii) . . . (annexing) via installation of puppet governments.”⁴ China has already solidified its control over neighboring North Korea and Burma, and has similarly begun more ambitious engagements in Africa and Central Asia where it seeks to expand its frontier.⁵

Noted political scientist Samuel P. Huntington provides further analysis of the motives behind China's imperial aspirations. He contends that “China (has) historically conceived itself as encompassing a ‘‘Sinic Zone’’ . . . (with) two goals: to become the champion of Chinese culture . . . and to resume its historical position, which it lost in the nineteenth century, as the hegemonic power in East Asia.”⁶ Furthermore, China holds one quarter of the world's population, and rapid economic growth will increase its demand for natural resources from outside its borders as its people seek a standard of living comparable to that of Western civilization.

The rise of peer competitors has historically resulted in regional instability and one should compare “the emergence of China to the rise of . . . Germany as the dominant power in Europe in the late nineteenth century.”⁷ Furthermore, the rise of another peer competitor on the level of the Soviet Union of the Cold War ultimately threatens U.S. global influence, challenging its concepts of human rights, liberalism, and democracy; as well as its ability to co-opt other nations to accept them.⁸ This decline in influence, while initially limited to the Asia-Pacific region, threatens to result in significant conflict if it ultimately leads to a paradigm shift in the ideas and principles that govern the existing world order.

A grand strategy of investment to address the threat of China requires investing in institutions, addressing ungoverned states, and building legitimacy through multilateralism. The United States must build capacity in the existing institutions and alliances accepted globally as legitimate representative bodies of the world's governments. For true legitimacy, the United States must support these institutions, not only when convenient, in order to avoid the appearance of unilateralism, which would ultimately undermine the very organizations upon whom it will rely when it is no longer the global hegemon.

The United States must also address ungoverned states, not only as breeding grounds for terrorism, but as conflicts that threaten to spread into regional instability, thereby drawing in superpowers with competing interests. Huntington proposes that the greatest source of conflict will come from what he defines as one “core” nation's involvement in a conflict between another core nation and a minor state within its immediate sphere of influence.⁹ For example, regional instability in South Asia¹⁰ threatens to involve combatants from the United States, India, China, and the surrounding nations. Appropriately, the United States, as a global power, must apply all elements of its national power now to address the problem of weak and failing states, which threaten to serve as the principal catalysts of future global conflicts.¹¹

NSA surveillance wrecks US cred in promoting Internet Freedom and spills over to larger foreign policy cred

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

Mandatory data localization proposals are just one of a number of ways that foreign governments have reacted to NSA surveillance in a manner that threatens U.S. foreign policy interests, particularly with regard to Internet Freedom. There has been a quiet tension between how the U.S. approaches freedom of expression online in its foreign policy and its domestic laws ever since Secretary of State Hillary Clinton effectively launched the Internet Freedom agenda in January 2010.¹⁷⁰ But the NSA disclosures shined a bright spotlight on the contradiction: the U.S. government promotes free expression abroad and aims to prevent repressive governments from monitoring and censoring their citizens while simultaneously supporting domestic laws that authorize surveillance and bulk data collection. As cybersecurity expert and Internet governance scholar Ron Deibert wrote a few days after the first revelations: “There are unintended consequences of the NSA scandal that will undermine U.S. foreign policy interests – in particular,

the ‘Internet Freedom’ agenda espoused by the U.S. State Department and its allies.”¹⁷¹ Deibert accurately predicted that the news would trigger reactions from both policymakers and ordinary citizens abroad, who would begin to question their dependence on American technologies and the hidden motivations behind the United States’ promotion of Internet Freedom. In some countries, the scandal would be used as an excuse to revive dormant debates about dropping American companies from official contracts, score political points at the expense of the United States, and even justify local monitoring and surveillance. Deibert’s speculation has so far proven quite prescient. As we will describe in this section, the ongoing revelations have done significant damage to the credibility of the U.S. Internet Freedom agenda and further jeopardized the United States’ position in the global Internet governance debates. Moreover, the repercussions from NSA spying have bled over from the Internet policy realm to impact broader U.S. foreign policy goals and relationships with government officials and a range of other important stakeholders abroad. In an essay entitled, “The End of Hypocrisy: American Foreign Policy in the Age of Leaks,” international relations scholars Henry Farrell and Martha Finnemore argue that a critical, lasting impact of information provided by leakers like Edward Snowden is “the documented confirmation they provide of what the United States is actually doing and why. When these deeds turn out to clash with the government’s public rhetoric, as they so often do, it becomes harder for U.S. allies to overlook Washington’s covert behavior and easier for U.S. adversaries to justify their own.”¹⁷² Toward the end of the essay, Farrell and Finnemore suggest, “The U.S. government, its friends, and its foes can no longer plausibly deny the dark side of U.S. foreign policy and will have to address it head-on.” Indeed, the U.S. is currently working to repair damaged bilateral and multilateral relations with countries from Germany and France to Russia and Israel,¹⁷³ and it is likely that the effects of the NSA disclosures will be felt for years in fields far beyond Internet policy.¹⁷⁴

Wrecks overall internet freedom globally

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

The effects of the NSA disclosures on the Internet Freedom agenda go beyond the realm of Internet governance. The loss of the United States as a model on Internet Freedom issues has made it harder for local civil society groups around the world—including the groups that the State Department’s Internet Freedom programs typically support²⁰³—to advocate for Internet Freedom within their own governments.²⁰⁴ The Committee to Protect Journalists, for example, reports that in Pakistan, “where freedom of expression is largely perceived as a Western notion, the Snowden revelations have had a damaging effect. The deeply polarized narrative has become starker as the corridors of power push back on attempts to curb government surveillance.”²⁰⁵ For some of these groups, in fact, even the appearance of collaboration with or support from the U.S. government can diminish credibility, making it harder for them to achieve local goals that align with U.S. foreign policy interests.²⁰⁶ The gap in trust is particularly significant for individuals and organizations that receive funding from the U.S. government for free expression activities or circumvention tools. Technology supported by or exported from the United States is, in some

cases, inherently suspect due to the revelations about the NSA's surveillance dragnet and the agency's attempts to covertly influence product development.

Moreover, revelations of what the NSA has been doing in the past decade are eroding the moral high ground that the United States has often relied upon when putting public pressure on authoritarian countries like China, Russia, and Iran to change their behavior. In 2014, Reporters Without Borders added the United States to its “Enemies of the Internet” list for the first time, explicitly linking the inclusion to NSA surveillance. “The main player in [the United States’] vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden’s revelations, has come to symbolize the abuses by the world’s intelligence agencies,” noted the 2014 report.²⁰⁷ The damaged perception of the United States²⁰⁸ as a leader on Internet Freedom and its diminished ability to legitimately criticize other countries for censorship and surveillance opens the door

for foreign leaders to justify—and even expand—their own efforts.²⁰⁹ For example, the Egyptian government recently announced plans to monitor social media for potential terrorist activity, prompting backlash from a number of advocates for free expression and privacy.²¹⁰ When a spokesman for the Egyptian Interior Ministry, Abdel Fatah Uthman, appeared on television to explain the policy, one justification that he offered in response to privacy concerns was that “the US listens in to phone calls, and supervises anyone who could threaten its national security.”²¹¹ This type of rhetoric makes it difficult for the U.S. to effectively criticize such a policy. Similarly, India’s comparatively mild response to allegations of NSA surveillance have been seen by some critics “as a reflection of India’s own aspirations in the world of surveillance,” a further indication that U.S. spying may now make it easier for foreign governments to quietly defend their own behavior.²¹² It is even more difficult for the United States to credibly indict Chinese hackers for breaking into U.S. government and commercial targets without fear of retribution in light of the NSA revelations.²¹³ These challenges reflect an overall decline in U.S. soft power on free expression issues.

Surveillance kills soft power

NSA overreach wrecks US smart power

Donahoe, 14 - Eileen Donahoe served as U.S. ambassador to the United Nations Human Rights Council. She is a visiting scholar at Stanford University's Freeman Spogli Institute for International Studies ("Why the NSA undermines national security" Reuters, 3/6, <http://blogs.reuters.com/great-debate/2014/03/06/why-nsa-surveillance-undermines-national-security/>)

But this zero-sum framework ignores the significant damage that the NSA's practices have done to U.S. national security. In a global digital world, national security depends on many factors beyond surveillance capacities, and over-reliance on global data collection can create unintended security vulnerabilities.

There's a better framework than security-versus-privacy for evaluating the national security implications of mass-surveillance practices. Former Secretary of State Hillary Clinton called it "smart power."

Her idea acknowledges that as global political power has become more diffuse, U.S. interests and security increasingly depend on our ability to persuade partners to join us on important global security actions. But how do we motivate disparate groups of people and nations to join us? We exercise smart power by inspiring trust and building credibility in the global community.

Developing these abilities is as important to U.S. national security as superior military power or intelligence capabilities.

I adopted the smart-power approach when serving as U.S. ambassador to the United Nations Human Rights Council. Our task at the council was to work with allies, emerging democracies and human rights-friendly governments to build coalitions to protect international human rights. We also built alliances with civil society actors, who serve as powerful countervailing forces in authoritarian systems. These partnerships can reinforce stable relationships, which enhances U.S. security.

The NSA's arbitrary global surveillance methods fly in the face of smart power. In the pursuit of information, the spy agency has invaded the privacy of foreign citizens and political leaders, undermining their sense of freedom and security. NSA methods also undercut U.S. credibility as a champion of universal human rights.

The U.S. model of mass surveillance will be followed by others and could unintentionally invert the democratic relationship between citizens and their governments. Under the cover of preventing terrorism, authoritarian governments may now increase surveillance of political opponents. Governments that collect and monitor digital information to intimidate or squelch political opposition and dissent can more justifiably claim they are acting with legitimacy.

For human rights defenders and democracy activists worldwide, the potential consequences of the widespread use by governments of mass surveillance techniques are dark and clear.

Superior information is powerful, but sometimes it comes at greater cost than previously recognized. When trust and credibility are eroded, the opportunity for collaboration and partnership with other nations on difficult global issues collapses. The ramifications of this loss of trust have not been adequately factored into our national security calculus.

What is most disconcerting is that the NSA's mass surveillance techniques have compromised the security of telecommunication networks, social media platforms, private-sector data storage and public infrastructure security systems. Authoritarian governments and hackers now have a roadmap to surreptitiously tap into private networks for their own nefarious purposes.

By weakening encryption programs and planting backdoor entries to encryption software, the NSA has demonstrated how it is possible to infiltrate and violate information-security systems. In effect, the spy agency has modeled anarchic behavior that makes everyone less safe.

Some have argued, though, that there is a big difference between the U.S. government engaging in mass-surveillance activities and authoritarian governments doing so. That “big difference” is supposed to be democratic checks and balances, transparency and adherence to the rule of law. Current NSA programs, however, do not operate within these constraints.

With global standards for digital surveillance now being set, our political leaders must remember that U.S. security depends upon much more than unimpeded surveillance capabilities. As German Chancellor Angela Merkel, one of President Barack Obama’s most trusted international partners, has wisely reminded us, just because we can do something does not mean that we should do it.

National security policies that fail to calculate the real costs of arbitrary mass surveillance threaten to make us less secure. Without trusted and trusting partners, U.S. priority initiatives in complex global negotiations will be non-starters.

The president, his advisers and our political leaders should reassess the costs of the NSA’s spy programs on our national security, our freedom and our democracy. By evaluating these programs through a smart-power lens, we will be in a stronger position to regain the global trust and credibility so central to our national security.

Economy

The perception of NSA overreaching wrecks global trust in the US tech sector – that wrecks the US economy and competitiveness

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

“It is becoming clear that the post-9/11 surveillance apparatus may be at cross-purposes with our high-tech economic growth,” declared Third Way’s Mieke Eoyang and Gabriel Horowitz in December 2013. “The economic consequences [of the recent revelations] could be staggering.”²⁵ A TIME magazine headline projected that “NSA Spying Could Cost U.S. Tech Giants Billions,” predicting losses based on the increased scrutiny that economic titans like Google, Microsoft, Facebook, and Yahoo have faced both at home and abroad since last June.²⁶ The NSA’s actions pose a serious threat to the current value and future stability of the information technology industry, which has been a key driver of economic growth and productivity in the United States in the past decade.²⁷ In this section, we examine how emerging evidence about the NSA’s extensive surveillance apparatus has already hurt and will likely continue to hurt the American tech sector in a number of ways, from dwindling U.S. market share in industries like cloud computing and webhosting to dropping tech sales overseas. The impact of individual users turning away from American companies in favor of foreign alternatives is a concern. However, the major losses will likely result from diminishing confidence in U.S. companies as trustworthy choices for foreign government procurement of products and services and changing behavior in the business-to-business market.

Costs to the U.S. Cloud Computing Industry and Related Business

Trust in American businesses has taken a significant hit since the initial reports on the PRISM program suggested that the NSA was directly tapping into the servers of nine U.S. companies to obtain customer data for national security investigations.²⁸ The Washington Post’s original story on the program provoked an uproar in the media and prompted the CEOs of several major companies to deny knowledge of or participation in the program.²⁹ The exact nature of the requests made through the PRISM program was later clarified,³⁰ but the public attention on the relationship between American companies and the NSA still created a significant trust gap, especially in industries where users entrust companies to store sensitive personal and commercial data. “Last year’s national security leaks have also had a commercial and financial impact on American technology companies that have provided these records,” noted Representative Bob Goodlatte, a prominent Republican leader and Chairman of the House Judiciary Committee, in May 2014. “They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global marketplace damaged.”³¹

Given heightened concerns about the NSA’s ability to access data stored by U.S. companies, it is no surprise that American companies offering cloud computing and webhosting services are among those experiencing the most acute economic fallout from NSA surveillance. Within just a few weeks of the first disclosures, reports began to emerge that American cloud computing companies like Dropbox and Amazon Web Services were starting to lose business to overseas

competitors.³² The CEO of Artmotion, one of Switzerland's largest offshore hosting providers, reported in July 2013 that his company had seen a 45 percent jump in revenue since the first leaks,³³ an early sign that the country's perceived neutrality and strong data and privacy protections³⁴ could potentially be turned into a serious competitive advantage.³⁵ Foreign companies are clearly poised to benefit from growing fears about the security ramifications of keeping data in the United States. In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014,³⁶ 25 percent of respondents indicated that they were moving data outside of the U.S. as a result of the NSA revelations. An overwhelming number of the companies surveyed indicated that security and data privacy were their top concerns, with 81 percent stating that they "want to know exactly where their data is being hosted." Seventy percent were even willing to sacrifice performance in order to ensure that their data was protected.³⁷

It appears that little consideration was given over the past decade to the potential economic repercussions if the NSA's secret programs were revealed.³⁸ This failure was acutely demonstrated by the Obama Administration's initial focus on reassuring the public that its programs primarily affect non-Americans, even though non-Americans are also heavy users of American companies' products. Facebook CEO Mark Zuckerberg put a fine point on the issue, saying that the government "blew it" in its response to the scandal. He noted sarcastically: "The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies [like Facebook] trying to serve people around the world, and that's really going to inspire confidence in American internet companies."³⁹ As Zuckerberg's comments reflect, certain parts of the American technology industry are particularly vulnerable to international backlash since growth is heavily dependent on foreign markets. For example, the U.S. cloud computing industry has grown from an estimated \$46 billion in 2008 to \$150 billion in 2014, with nearly 50 percent of worldwide cloud-computing revenues coming from the U.S.⁴⁰ R Street Institute's January 2014 policy study concluded that in the next few years, new products and services that rely on cloud computing will become increasingly pervasive. "Cloud computing is also the root of development for the emerging generation of Web-based applications—home security, outpatient care, mobile payment, distance learning, efficient energy use and driverless cars," writes R Street's Steven Titch in the study. "And it is a research area where the United States is an undisputed leader."⁴¹ This trajectory may be dramatically altered, however, as a consequence of the NSA's surveillance programs.

Economic forecasts after the Snowden leaks have predicted significant, ongoing losses for the cloud-computing industry in the next few years. An August 2013 study by the Information Technology and Innovation Foundation (ITIF) estimated that revelations about the NSA's PRISM program could cost the American cloud computing industry \$22 to \$35 billion over the next three years.⁴² On the low end, the ITIF projection suggests that U.S. cloud computing providers would lose 10 percent of the foreign market share to European or Asian competitors, totaling in about \$21.5 billion in losses; on the high-end, the \$35 billion figure represents about 20 percent of the companies' foreign market share. Because the cloud computing industry is undergoing rapid growth right now—a 2012 Gartner study predicted global spending on cloud computing would increase by 100 percent from 2012 to 2016, compared to a 3 percent overall growth rate in the tech industry as a whole⁴³—vendors in this sector are particularly vulnerable to shifts in the market. Failing to recruit new customers or losing a competitive advantage due to exploitation by rival companies in other countries can quickly lead to a dwindling market share. The ITIF study further notes that "the percentage lost to foreign competitors could go higher if foreign governments enact protectionist trade barriers that effectively cut out U.S. providers," citing early

calls from German data protection authorities to suspend the U.S.-EU Safe Harbor program (which will be discussed at length in the next section).⁴⁴ As the R Street Policy Study highlights, “Ironically, the NSA turned the competitive edge U.S. companies have in cloud computing into a liability, especially in Europe.”⁴⁵

In a follow up to the ITIF study, Forrester Research analyst James Staten argued that the think tank’s estimates were low, suggesting that the actual figure could be as high as \$180 billion over three years.⁴⁶ Staten highlighted two additional impacts not considered in the ITIF study. The first is that U.S. customers—not just foreign companies—would also avoid US cloud providers, especially for international and overseas business. The ITIF study predicted that American companies would retain their domestic market share, but Staten argued that the economic blowback from the revelations would be felt at home, too. “You don’t have to be a French company, for example, to be worried about the US government snooping in the data about your French clients,” he wrote.⁴⁷ Moreover, the analysis highlighted a second and “far more costly” impact: that foreign cloud providers, too, would lose as much as 20 percent of overseas and domestic business because of similar spying programs conducted by other governments. Indeed, the NSA disclosures “have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance,” according to a November 2013 report by Privacy International on the “Five Eyes” intelligence partnership between the United States, the United Kingdom, Canada, Australia, and New Zealand.⁴⁸ Staten predicts that as the surveillance landscape around the world becomes more clear, it could have a serious negative impact on all hosting and outsourcing services, resulting in a 25 percent decline in the overall IT services market, or about \$180 billion in losses.⁴⁹

Recent reports suggest that things are, in fact, moving in the direction that analysts like Castro and Staten suggested.⁵⁰ A survey of 1,000 “[Information and Communications Technology (ICT)] decision-makers” from France, Germany, Hong Kong, the UK, and the USA in February and March 2014 found that the disclosures “have had a direct impact on how companies around the world think about ICT and cloud computing in particular.”⁵¹ According to the data from NTT Communications, 88 percent of decision-makers are changing their purchasing behavior when it comes to the cloud, with the vast majority indicating that the location of the data is very important. The results do not bode well for recruitment of new customers, either—62 percent of those currently not storing data in the cloud indicated that the revelations have since prevented them from moving their ICT systems there. And finally, 82 percent suggested that they agree with proposals made by German Chancellor Angela Merkel in February 2014 to have separate data networks for Europe, which will be discussed in further detail in Part III of this report. Providing direct evidence of this trend, Servint, a Virginia-based webhosting company, reported in June 2014 that international clients have declined by as much as half, dropping from approximately 60 percent of its business to 30 percent since the leaks began.⁵²

With faith in U.S. companies on the decline, foreign companies are stepping in to take advantage of shifting public perceptions. As Georg Mascolo and Ben Scott predicted in a joint paper published by the Wilson Center and the New America Foundation in October 2013, “Major commercial actors on both continents are preparing offensive and defensive strategies to battle in the market for a competitive advantage drawn from Snowden’s revelations.”⁵³ For example, Runbox, a small Norwegian company that offers secure email service, reported a 34 percent jump in customers since June 2013.⁵⁴ Runbox markets itself as a safer email and webhosting provider for both individual and commercial customers, promising that it “will never disclose any user

data unauthorized, track your usage, or display any advertisements.”⁵⁵ Since the NSA revelations, the company has touted its privacy-centric design and the fact that its servers are located in Norway as a competitive advantage. “Being firmly located in Norway, the Runbox email service is governed by strict privacy regulations and is a safe alternative to American email services as well as cloud-based services that move data across borders and jurisdictions,” company representatives wrote on its blog in early 2014.⁵⁶ F-Secure, a Finnish cloud storage company, similarly emphasizes the fact that “its roots [are] in Finland, where privacy is a fiercely guarded value.”⁵⁷ Presenting products and services as ‘NSA-proof’ or ‘safer’ alternatives to American-made goods is an increasingly viable strategy for foreign companies hoping to chip away at U.S. tech competitiveness.⁵⁸

It has ripple effects that will destroy global economic growth

Chandler and Le, 15 - * Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND **Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, “DATA NATIONALISM” 64 Emory L.J. 677, lexis)

C. Economic Development

Many governments believe that by forcing companies to localize data within national borders, they will increase investment at home. Thus, data localization measures are often motivated, whether explicitly or not, by desires to promote local economic development. In fact, however, data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances.

In an Information Age, the global flow of data has become the lifeblood of economies across the world. While some in Europe have raised concerns about the transfer of data abroad, the European Commission has recognized “the critical importance of data flows notably for the transatlantic economy.”ⁿ²⁰⁹ The Commission observes that international data transfers "form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US.”ⁿ²¹⁰ Worried about the effect of constraints on data flows on both global information sharing and economic development, the Organisation for Economic Co-operation and Development (OECD) has urged nations to avoid “barriers to the location, access and use of cross-border [*722] data facilities and functions” when consistent with other fundamental rights, in order to “ensure cost effectiveness and other efficiencies.”ⁿ²¹¹

The worry about the impact of data localization is widely shared in the business community as well. The value of the Internet to national economies has been widely noted. n212 Regarding Brazil’s attempt to require data localization, the Information Technology Industry Council, an industry association representing more than forty major Internet companies, had argued that “in-country data storage requirements would detrimentally impact all economic activity that depends on data flows.”ⁿ²¹³ The Swedish government agency, the National Board of Trade, recently interviewed fifteen local companies of various sizes across sectors and concluded succinctly that “trade cannot happen without data being moved from one location to another.”ⁿ²¹⁴

Data localization, like most protectionist measures, leads only to small gains for a few local enterprises and workers, while causing significant harms spread across the entire economy. The domestic benefits of data localization go to the few owners and employees of data centers and the few companies servicing these centers locally. Meanwhile, the harms of data localization are widespread, felt by small, medium, and large businesses that are denied access to global services that might improve productivity. In response to Russia's recently passed localization law, the NGO Russian Association for Electronic Communications stressed the potential economic consequences, pointing to the withdrawal of global services and substantial economic losses caused by the passing of similar laws in other countries. n215 For example, besides the loss of international social media platforms, localization would make it impossible for [*723] Russians to order airline tickets or consumer goods through online services. Localization requirements also seriously affect Russian companies like Aeroflot because the airline depends on foreign ticket-booking systems. n216

Critics worried, at the time, that the Brazilian data localization requirement would "deny[] Brazilian users access to great services that are provided by US and other international companies." n217 Marilia Marciel, a digital policy expert at Fundacao Getulio Vargas in Rio de Janeiro, observes, "Even Brazilian companies prefer to host their data outside of Brazil." n218 Data localization affects domestic innovation by denying entrepreneurs the ability to build on top of global services based abroad. Brasscom, the Brazilian Association of Information Technology and Communication Companies, argues that such obligations would "hurt[] the country's ability to create, innovate, create jobs and collect taxes from the proper use of the Internet." n219

Governments implementing in-country data mandates imagine that the various global services used in their country will now build infrastructure locally. Many services, however, will find it uneconomical and even too risky to establish local servers in certain territories. n220 Data centers are expensive, all the more so if they have the highest levels of security. One study finds Brazil to be the most expensive country in the Western hemisphere in which to build data centers. n221 Building a data center in Brazil costs \$ 60.9 million on average, [*724] while building one in Chile and the United States costs \$ 51.2 million and \$ 43 million, respectively. n222 Operating such a data center remains expensive because of enormous energy and other expenses - averaging \$ 950,000 in Brazil, \$ 710,000 in Chile, and \$ 510,000 in the United States each month. n223 This cost discrepancy is mostly due to high electricity costs and heavy import taxes on the equipment needed for the center. n224 Data centers employ few workers, with energy making up three-quarters of the costs of operations. n225 According to the 2013 Data Centre Risk Index - a study of thirty countries on the risks affecting successful data center operations - Australia, Russia, China, Indonesia, India, and Brazil are among the riskiest countries for running data centers. n226

Not only are there significant economic costs to data localization, the potential gains are more limited than governments imagine. Data server farms are hardly significant generators of employment, populated instead by thousands of computers and few human beings. The significant initial outlay they require is largely in capital goods, the bulk of which is often imported into a country. The diesel generators, cooling systems, servers, and power supply devices tend to be imported from global suppliers. n227 Ironically, it is often American suppliers of servers and other hardware that stand to be the beneficiaries of data localization mandates. n228 One study notes, "Brazilian suppliers of components did not benefit from this [data localization requirement], since the imported products dominate the market." n229 By increasing

capital purchases from abroad, data localization requirements can in fact increase merchandise trade deficits. Furthermore, large data farms are [*725] enormous consumers of energy, n230 and thus often further **burden overtaxed energy grids.** They thereby harm other industries that must now compete for this energy, paying higher prices while potentially suffering limitations in supply of already scarce power.

Cost, as well as access to the latest innovations, drives many e-commerce enterprises in Indonesia to use foreign data centers. Daniel Tumiwa, head of the Indonesian E-Commerce Association (IdEA), states that "the cost can double easily in Indonesia." n231 Indonesia's Internet start-ups have accordingly often turned to foreign countries such as Australia, Singapore, or the United States to host their services. One report suggests that "many of the "tools" that start-up online media have relied on elsewhere are not fully available yet in Indonesia." n232 The same report also suggests that a weak local hosting infrastructure in Indonesia means that sites hosted locally experience delayed loading time. n233 Similarly, as the Vietnamese government attempts to foster entrepreneurship and innovation, n234 localization requirements effectively bar start-ups from utilizing cheap and powerful platforms abroad and potentially handicap Vietnam from "joining in the technology race." n235

Governments worried about transferring data abroad at the same time hope, somewhat contradictorily, to bring foreign data within their borders. Many countries seek to become leaders in providing data centers for companies operating across their regions. In 2010, Malaysia announced its Economic Transformation Program n236 to transform Malaysia into a world-class data [*726] center hub for the Asia-Pacific region. n237 Brazil hopes to accomplish the same for Latin America, while France seeks to stimulate its economy via a "Made in France" digital industry. n238 Instead of spurring local investment, data localization can lead to the loss of investment. First, there's the retaliation effect. Would countries send data to Brazil if Brazil declares that data is unsafe if sent abroad? Brasscom notes that the Brazilian Internet industry's growth would be hampered if other countries engage in similar reactive policies, which "can stimulate the migration of datacenters based here, or at least part of them, to other countries." n239 Some in the European Union sympathize with this concern. European Commissioner for the Digital Agenda, Neelie Kroes, has expressed similar doubts, worrying about the results for European global competitiveness if each country has its own separate Internet. n240 Then there's the avoidance effect. Rio de Janeiro State University Law Professor Ronaldo Lemos, who helped write the original Marco Civil and is currently Director of the Rio Institute for Technology and Society, warns that the localization provision would have caused foreign companies to avoid the country altogether: "It could end up having the opposite effect to what is intended, and scare away companies that want to do business in Brazil." n241 Indeed, such burdensome local laws often lead companies to launch overseas, in order to try to avoid these rules entirely. Foreign companies, too, might well steer clear of the country in order to avoid entanglement with cumbersome rules. For example, Yahoo!, while very popular in Vietnam, places its servers for the [*727] country in Singapore. n242 In these ways we see that data localization mandates can backfire entirely, leading to avoidance instead of investment.

Data localization requirements place burdens on domestic enterprises not faced by those operating in more liberal jurisdictions. Countries that require data to be cordoned off complicate matters for their own enterprises, which must turn to domestic services if they are to comply with the law. Such companies must also develop mechanisms to segregate the data they hold by the nationality of the data subject. The limitations may impede development of new, global services.

Critics argue that South Korea's ban on the export of mapping data, for example, impedes the development of next-generation services in Korea: Technology services, such as Google Glass, driverless cars, and information programs for visually-impaired users, are unlikely to develop and grow in Korea. Laws made in the 1960s are preventing many venture enterprises from advancing to foreign markets via location/navigation services. n243

The harms of data localization for local businesses are not restricted to Internet enterprises or to consumers denied access to global services. As it turns out, most of the economic benefits from Internet technologies accrue to traditional businesses. A McKinsey study estimates that about seventy-five percent of the value added created by the Internet and data flow is in traditional industries, in part through increases in productivity. n244 The potential economic impact across the major sectors - healthcare, manufacturing, electricity, urban infra-structure, security, agriculture, retail, etc. - is estimated at \$ 2.7 to \$ 6.2 trillion per year. n245 This is particularly important for emerging economies, in which traditional industries remain predominant. The Internet raises profits as well, due to increased revenues, lower costs of goods sold, and lower administrative costs. n246 With data localization mandates, traditional businesses [*728] will lose access to the many global services that would store or process information offshore.

Data localization requirements also interfere with the most important trends in computing today. They limit access to the disruptive technologies of the future, such as cloud computing, the "Internet of Things," and data-driven innovations (especially those relying on "big data"). Data localization sacrifices the innovations made possible by building on top of global Internet platforms based on cloud computing. This is particularly important for entrepreneurs operating in emerging economies that might lack the infrastructure already developed elsewhere. And it places great impediments to the development of both the Internet of Things and big data analytics, requiring costly separation of data by political boundaries and often denying the possibility of aggregating data across borders. We discuss the impacts on these trends below.

That causes World War 3

James, 14 - Professor of history at Princeton University's Woodrow Wilson School who specializes in European economic history (Harold, "Debate: Is 2014, like 1914, a prelude to world war?" 7/3, <http://www.theglobeandmail.com/globe-debate/read-and-vote-is-2014-like-1914-a-prelude-to-world-war/article19325504/>)

Some of the dynamics of the pre-1914 financial world are now re-emerging. Then an economically declining power, Britain, wanted to use finance as a weapon against its larger and faster growing competitors, Germany and the United States. Now America is in turn obsessed by being overtaken by China – according to some calculations, set to become the world's largest economy in 2014.

In the aftermath of the 2008 financial crisis, financial institutions appear both as dangerous weapons of mass destruction, but also as potential instruments for the application of national power.

In managing the 2008 crisis, the dependence of foreign banks on U.S. dollar funding constituted a major weakness, and required the provision of large swap lines by the Federal Reserve. The

United States provided that support to some countries, but not others, on the basis of an explicitly political logic, as Eswar Prasad demonstrates in his new book on the “Dollar Trap.”

Geo-politics is intruding into banking practice elsewhere. Before the Ukraine crisis, Russian banks were trying to acquire assets in Central and Eastern Europe. European and U.S. banks are playing a much reduced role in Asian trade finance. Chinese banks are being pushed to expand their role in global commerce. After the financial crisis, China started to build up the renminbi as a major international currency. Russia and China have just proposed to create a new credit rating agency to avoid what they regard as the political bias of the existing (American-based) agencies.

The next stage in this logic is to think about how financial power can be directed to national advantage in the case of a diplomatic tussle. Sanctions are a routine (and not terribly successful) part of the pressure applied to rogue states such as Iran and North Korea. But financial pressure can be much more powerfully applied to countries that are deeply embedded in the world economy.

The test is in the Western imposition of sanctions after the Russian annexation of Crimea. President Vladimir Putin’s calculation in response is that the European Union and the United States cannot possibly be serious about the financial war. It would turn into a boomerang: Russia would be less affected than the more developed and complex financial markets of Europe and America.

The threat of systemic disruption generates a new sort of uncertainty, one that mirrors the decisive feature of the crisis of the summer of 1914. At that time, no one could really know whether clashes would escalate or not. That feature contrasts remarkably with almost the entirety of the Cold War, especially since the 1960s, when the strategic doctrine of Mutually Assured Destruction left no doubt that any superpower conflict would inevitably escalate.

The idea of network disruption relies on the ability to achieve advantage by surprise, and to win at no or low cost. But it is inevitably a gamble, and raises prospect that others might, but also might not be able to, mount the same sort of operation. Just as in 1914, there is an enhanced temptation to roll the dice, even though the game may be fatal.

Curtailing the use of surveillance on US-based servers to national security interests and increasing transparency regarding surveillance is vital to restoring trust and US credibility

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

The NSA mass surveillance programs described in the introduction, conducted domestically pursuant to USA PATRIOT Act Section 215 and FISA Amendments Act Section 702 and conducted outside the U.S. under Executive Order 12333, have arguably had the greatest and most immediate impact on America's tech industry and global standing. Strictly limiting the scope and purpose of surveillance under these authorities—not just in regard to surveillance of Americans **but of non-Americans as well**—will be critical to regaining the trust of individuals, companies and countries around the world, as well as stemming the economic and political costs of the NSA programs.

The President's NSA Review Group acknowledged the need for such reform in its report on surveillance programs, affirming that “the right of privacy has been recognized as a basic human right that all nations should respect,” and cautioned that “unrestrained American surveillance of non-United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries.”³²⁴ In addition to recommending a variety new protections for U.S. persons, the Review Group urged in its Recommendation 13 that surveillance of non-U.S. persons under Section 702 or “any other authority”—a reference intended to include Executive Order 12333325 — should be strictly limited to the purpose of protecting national security, should not be used for economic espionage, should not be targeted based solely on a person’s political or religious views, and should be subject to careful oversight and the highest degree of transparency possible.³²⁶ Fully implementing this recommendation—and particularly restricting Section 702 and Executive Order 12333 surveillance to specific national security purposes rather than foreign intelligence collection generally—would indicate significant progress toward addressing the concerns raised in the recent Report of the Office of the United Nations High Commissioner for Human Rights on “The Right to Privacy in the Digital Age.” The UN report highlights how, despite the universality of human rights, the common distinction between “‘foreigners’ and ‘citizens’ ...within national security surveillance oversight regimes” has resulted in “significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.”³²⁷

The leading legislative reform proposal in the U.S. Congress, the USA FREEDOM Act, would go a long way to protecting both U.S. and non-U.S. persons against the bulk collection under Section 215 of records held by American telephone and Internet companies.³²⁸ On that basis, passage of the law would very much help address the trust gap that the NSA programs have created. However, with regard to Section 702, the bill as originally introduced only added new protections for U.S. persons or for wholly domestic communications,³²⁹ and even those protections were stripped out or weakened in the version of the bill that was passed by the House of Representatives in May 2014.³³⁰ Meanwhile, neither the bill as introduced nor as passed by the House addresses surveillance conducted extraterritorially under Executive Order 12333. Therefore, even if USA FREEDOM is eventually approved by both the House and the Senate and signed into law by the President, much more will ultimately need to be done to reassure foreign users of U.S.-based communications networks, services, and products that their rights are being respected.

Provide for increased transparency around government surveillance, both from the government and companies.

Increased transparency about how the NSA is using its authorities, and how U.S. companies do—or do not—respond when the NSA demands their data is critical to rebuilding the trust that has been lost in the wake of the Snowden disclosures. In July 2013, a coalition of large Internet companies and advocacy groups provided a blueprint for the necessary transparency reforms, in a letter to the Obama Administration and Congress calling for “greater transparency around national security-related requests by the US government to Internet, telephone, and web-based service providers for information about their users and subscribers.”³³¹ Major companies including Facebook, Google, and Microsoft—joined by organizations such as the Center for Democracy and Technology, New America’s Open Technology Institute, and the American Civil Liberties Union—demanded that the companies be allowed to publish aggregate numbers about the specific types of government requests they receive, the types of data requested, and the number of people affected. They also urged the government to issue its own transparency reports to provide greater clarity about the scope of the NSA’s surveillance programs.³³² “This information about how and how often the government is using these legal authorities is important to the American people, who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of US-based service providers who are concerned about the privacy and security of their communications,” the letter stated.³³³

Two months later, many of the same companies and organizations issued another letter supporting surveillance transparency legislation proposed by Senator Al Franken (D-MN) and Representative Zoe Lofgren (D-CA) that would have implemented many of the original letter’s recommendations.³³⁴ Elements of both bills, consistent with the coalition’s recommendations, were included in the original version of the USA FREEDOM Act introduced in the House and the Senate—as were new strong transparency provisions requiring the FISA court to declassify key legal opinions to better educate the public and policymakers about how it is interpreting and implementing the law. Such strong new transparency requirements are consistent with several recommendations of the President’s Review Group³³⁵ and would help address concerns about lack of transparency raised by the UN High Commissioner for Human Rights.³³⁶

Unfortunately, all of these transparency provisions from the original USA FREEDOM Act were substantially weakened in the version of the bill that was passed by the House of Representatives in May 2014.³³⁷ Congress will need to include stronger transparency provisions in any final version of the USA FREEDOM Act if it intends to meaningfully restore trust in the U.S. Internet and telecommunications industries and stem the loss of business that has begun as a result of the NSA programs. As commentator Mieke Eoyang put it, “If reforms do not deliver sufficient protections and transparency for [tech companies’] customers, especially those abroad who have the least constitutional protections, they will vote with their feet.”³³⁸

Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance, including moving toward international human-rights based standards on surveillance.

The United States must act immediately to restore the credibility of the Internet Freedom agenda, lest it become another casualty of the NSA’s surveillance programs. As described in Part IV, various agencies within the U.S. government have taken initial steps to demonstrate goodwill in this area, particularly through the NTIA’s announcement that it intends to transition stewardship of the IANA functions to a global multistakeholder organization and the State Department’s speech outlining six principles to guide signals intelligence collection grounded in international

human rights norms. However, it will take a broader effort from across the government to demonstrate that the United States is fully committed to Internet Freedom, including firmly establishing the nature of its support for the evolving multistakeholder system of Internet governance and directly engaging with issues raised by the NSA surveillance programs in international conversations.

Supporting international norms that increase confidence in the security of online communications and respect for the rights of Internet users all around the world is integral to restoring U.S. credibility in this area. “We have surveillance programmes that abuse human rights and lack in transparency and accountability precisely because we do not have sufficiently robust, open, and inclusive debates around surveillance and national security policy,” writes Matthew Shears of the Center for Democracy & Technology.³³⁹ It is time to begin having those conversations on both a national and an international level, particularly at key upcoming Internet governance convenings including the 2014 Internet Governance Forum, the International Telecommunications Union’s plenipotentiary meeting, and the upcoming WSIS+10 review process.³⁴⁰ Certainly, the United States will not be able to continue promoting the Internet Freedom agenda at these meetings without addressing its national security apparatus and the impact of NSA surveillance on individuals around the world. Rather than being a problem, this presents an opportunity for the U.S. to assume a leadership role in the promotion of better international standards around surveillance practices.

NSA killing tech competitiveness

Loss of overseas markets wrecks tech competitiveness

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

The economic impact of NSA spying does not end with the American cloud computing industry. According to The New York Times, “Even as Washington grapples with the diplomatic and political fallout of Mr. Snowden’s leaks, the more urgent issue, companies and analysts say, is economic.”⁵⁹ In the past year, a number of American companies have reported declining sales in overseas markets like China (where, it must be noted, suspicion of the American government was already high before the NSA disclosures), loss of customers including foreign governments, and increased competition from non-U.S. services marketing themselves as ‘secure’ alternatives to popular American products.

There is already significant evidence linking NSA surveillance to direct harm to U.S. economic interests. In November 2013, Cisco became one of the first companies to publicly discuss the impact of the NSA on its business, reporting that orders from China fell 18 percent and that its worldwide revenue would decline 8 to 10 percent in the fourth quarter, in part because of continued sales weakness in China.⁶⁰ New orders in the developing world fell 12 percent in the third quarter, with the Brazilian market dropping roughly 25 percent of its Cisco sales.⁶¹ Although John Chambers, Cisco’s CEO, was hesitant to blame all losses on the NSA, he acknowledged that it was likely a factor in declining Chinese sales⁶² and later admitted that he had never seen as fast a decline in an emerging market as the drop in China in late 2013.⁶³ These numbers were also released before documents in May 2014 revealed that the NSA’s Tailored Access Operations unit had intercepted network gear—including Cisco routers—being shipped to target organizations in order to covertly install implant firmware on them before they were delivered.⁶⁴ In response, Chambers wrote in a letter to the Obama Administration that “if these allegations are true, these actions will undermine confidence in our industry and in the ability of technology companies to deliver products globally.”⁶⁵

Much like Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard all reported in late 2013 that sales were down in China as a result of the NSA revelations.⁶⁶ Sanford C. Bernstein analyst Toni Sacconaghi has predicted that after the NSA revelations, “US technology companies face the most revenue risk in China by a wide margin, followed by Brazil and other emerging markets.”⁶⁷ Industry observers have also questioned whether companies like Apple—which hopes to bring in significant revenue from iPhone sales in China—will feel the impact overseas.⁶⁸ Even AT&T reportedly faced intense scrutiny regarding its proposed acquisition of Vodafone, a European wireless carrier, after journalists revealed the extent of AT&T’s collaboration with the NSA.⁶⁹

American companies are also losing out on business opportunities and contracts with large companies and foreign governments as a result of NSA spying. According to an article in The New York Times, “American businesses are being left off some requests for proposals from foreign customers that previously would have included them.”⁷⁰ This refers to German

companies, for example, that are increasingly uncomfortable giving their business to American firms. Meanwhile, the German government plans to change its procurement rules to prevent American companies that cooperate with the NSA or other intelligence organizations from being awarded federal IT contracts.⁷¹ The government has already announced it intends to end its contract with Verizon, which provides Internet service to a number of government departments.⁷² “There are indications that Verizon is legally required to provide certain things to the NSA, and that’s one of the reasons the cooperation with Verizon won’t continue,” a spokesman for the German Interior Ministry told the Associated Press in June.⁷³

The NSA disclosures have similarly been blamed for Brazil’s December 2013 decision to award a \$4.5 billion contract to Saab over Boeing, an American company that had previously been the frontrunner in a deal to replace Brazil’s fleet of fighter jets.⁷⁴ Welber Barral, a former Brazilian trade secretary, suggested to Bloomberg News that Boeing would have won the contract a year earlier,⁷⁵ while a source in the Brazilian government told Reuters that “the NSA problem ruined it for the Americans.”⁷⁶ As we will discuss in greater depth in the next section, Germany and Brazil are also considering data localization proposals that could harm U.S. business interests and prevent American companies from entering into new markets because of high compliance costs.

Wrecks the economy and industry reforms alone won’t solve

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

It is abundantly clear that the NSA surveillance programs are currently having a serious, negative impact on the U.S. economy and threatening the future competitiveness of American technology companies. Not only are U.S. companies losing overseas sales and getting dropped from contracts with foreign companies and governments—they are also watching their competitive advantage in fast-growing industries like cloud computing and webhosting disappear, opening the door for foreign companies who claim to offer “more secure” alternative products to poach their business. Industry efforts to increase transparency and accountability as well as concrete steps to promote better security by adopting encryption and other best practices are positive signs, but U.S. companies cannot solve this problem alone. “It’s not blowing over,” said Microsoft General Counsel Brad Smith at a recent conference. “In June of 2014, it is clear it is getting worse, not better.”⁹⁸ Without meaningful government reform and better oversight, concerns about the breadth of NSA surveillance could lead to permanent shifts in the global technology market and do lasting damage to the U.S. economy.

Perception key

The widespread perception that the NSA is acting beyond the established legislative framework is destroying the reputation of U.S. tech companies

Eoyang and Bishai, 15 - *Mieke Eoyang is the Director of the National Security Program at Third Way, a center-left think tank. She previously served as Defense Policy Advisor to Senator Edward M. Kennedy, and a subcommittee staff director on the House Permanent Select Committee on Intelligence, as well as as Chief of Staff to Rep. Anna Eshoo (D-Palo Alto);

**Chrissy Bishai is a Fellow at Third Way (“Restoring Trust between U.S. Companies and Their Government on Surveillance Issues” 3/19, <http://www.thirdway.org/report/restoring-trust-between-us-companies-and-their-government-on-surveillance-issues>

Allegations of intrusive U.S. government electronic surveillance activities have raised international outcry and created antagonism between U.S. technology companies and the government. Without a bold and enduring reform, American companies will continue to suffer a competitive disadvantage from perceptions of U.S. government intrusion into their data. We propose bringing electronic surveillance collection from U.S. companies into an existing statutory framework in order to reassure international customers and to respect the rights of U.S. companies operating abroad.

The Problem

In the wake of the Snowden revelations, people around the world have become uneasy about the security of their communications that flow through the servers of American companies.1 They now fear—not without reason—that the NSA has broad access to a wide range of their data that may not have any direct relevance to the core foreign policy or security concerns of the United States.²

Snowden has also alleged that the NSA accessed American companies’ data without their knowledge.³ American technology companies reacted with outrage to media reports that, unbeknownst to them, the U.S. government had intruded onto their networks overseas and spoofed their web pages or products.⁴ These stories suggested that the government created and snuck through back doors to take the data rather than come through well-established front doors.⁵

Beyond the broad implications for civil liberties and diplomacy, these fears led to two immediate consequences for the industry: First, many U.S. companies shifted to an adversarial relationship with their own government. They moved to secure and encrypt their data to protect the privacy rights of their customers.⁶ They are pushing for reform.⁷ They are building state-of-the-art data centers in Europe and staffing their high-paying jobs with Europeans, not Americans.⁸ They are challenging the government in court.⁹

Second, international customers of U.S. technology and communications companies began taking their business elsewhere. Brazil decided against a \$4.5 billion Boeing deal and cancelled Microsoft contracts.¹⁰ Germany dropped Verizon in favor of Deutsche Telekom.¹¹ Both of these examples suggest that if even friendly governments can go to the expense and trouble of dropping American companies, foreign individual and corporate customers could certainly decide to switch their data providers for greater privacy protection. Simply put, the reputational harm had a direct

impact on American companies' competitiveness—some estimate that it has cost U.S. tech firms \$180 billion thus far.¹²

Defenders of the programs may argue that the Snowden allegations are overblown or that foreign companies are just using the revelations for their own protectionist purposes. But it doesn't matter if the allegations are actually true because the global public believes them to be true, and they are therefore real in their consequences.

In many ways, the Snowden revelations have created a sense of betrayal among American companies. Some had been providing information to the NSA through existing legislative means – either under Section 215 of the USA Patriot Act,¹³ or under Section 702 of the FISA Amendments Act (FAA).¹⁴ It was unsettling to read stories that, outside of this statutorily compelled cooperation, the government had been getting access to huge amounts of their data in other unauthorized ways. As one tech employee said, “the back door makes a mockery of the front door.”

AT: Doesn't hurt cloud computing

Data localization is an independent internal link

Chandler and Le, 15 - * Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND **Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, "DATA NATIONALISM" 64 Emory L.J. 677, lexis)

Cloud Computing. Data localization requirements will often prevent access to global cloud computing services. As we have indicated, while governments assume that global services will simply erect local data server farms, such hopes are likely to prove unwarranted. Thus, local companies will be denied access to the many companies that might help them scale up, or to go global. n247 Many companies around the world are built on top of existing global services. Highly successful companies with Indian origins such as Slideshare and Zoho relied on global services such as Amazon Web Services and Google Apps. n248 A Slideshare employee cites the scalability made possible by the use of Amazon's cloud services, noting, "Sometimes I need 100 servers, sometimes I only need 10." n249 A company like Zoho can use Google Apps, while at the same time competing with Google in higher value-added services. n250 [*729] Accessing such global services thus allows a small company to maintain a global presence without having to deploy the vast infrastructure that would be necessary to scale as needed.

The Internet of Things. As the world shifts to Internet-connected devices, data localization will require data flows to be staunched at national borders, requiring expensive and cumbersome national infrastructures for such devices. This erodes the promise of the Internet of Things - where everyday objects and our physical surroundings are Internet-enabled and connected - for both consumers and businesses. Consumer devices include wearable technologies that "measure some sort of detail about you, and log it." n251 Devices such as Sony's Smartband allied with a Lifelog application to track and analyze both physical movements and social interactions n252 or the Fitbit n253 device from an innovative start-up suggest the revolutionary possibilities for both large and small manufacturers. The connected home and wearable computing devices are becoming increasingly important consumer items. n254 A heart monitoring system collects data from patients and physicians around the world and uses the anonymized data to advance cardiac care. n255 Such devices collect data for analysis typically on the company's own or outsourced computer servers, which could be located anywhere across the world. Over this coming decade, the Internet of Things is estimated to generate \$ 14.4 trillion in value that is "up for grabs" for global enterprises. n256 Companies are also adding Internet sensors not just to consumer products but to their own equipment and facilities around the world through RFID tags or through other devices. The oil industry has embraced what has come to be known as the "digital oil field," where real-time [*730] data is collected and analyzed remotely. n257 While data about oil flows would hardly constitute personal information, such data might be controlled under laws protecting sensitive national security information. The Internet of Things shows the risks of data localization for consumers, who may be denied access to many of the best services the world has to offer. It also shows the risk of data localization for companies seeking to better monitor their systems around the world.

Data Driven Innovation (Big Data). Many analysts believe that data-driven innovations will be a key basis of competition, innovation, and productivity in the years to come, though many note the importance of protecting privacy in the process of assembling ever-larger databases. n258 McKinsey even reclassifies data as a new kind of factor of production for the Information Age. n259 Data localization threatens big data in at least two ways. First, by limiting data aggregation by country, it increases costs and adds complexity to the collection and maintenance of data. Second, data localization requirements can reduce the size of potential data sets, eroding the informational value that can be gained by cross-jurisdictional studies. Large-scale, global experiments technically possible through big data analytics, especially on the web, may have to give way to narrower, localized studies. Perhaps anonymization will suffice to comport with data localization laws and thus still permit cross-border data flow, but this will depend on the specifics of the law.

Cyber Security - Encryption

What is Encryption?

Encryption defined

Omar El Akkad, January 19, 2015 Technology firms are caught between the need for better encryption against hackers and politicians' calls for surveillance measures, Globe & Mail, <http://penny2.theglobeandmail.com/servlet/ArticleNews/story/gam/20150119/RBIBSOFTWAREENCRYPTION DOA: 3-21-15>

Encryption is, at its most basic level, a means of keeping information secret using very large numbers. Just as a 15-digit PIN is harder to guess than a four-digit PIN, high-grade encryption algorithms that manipulate larger numbers are usually harder to break. As such, all things being equal, encryption is not only a fairly effective means of keeping data private, its effectiveness can also be mathematically measured.

How encryption works

The Observer (England), June 8, 2014, John Naughton: Even a password on steroids won't keep the spies out

So Google has decided to provide end-to-end encryption for any of its Gmail users who wants it. One could ask "what took you so long?" but that would be churlish. (Some of us were unkind enough to suspect that the reluctance might have been due to, er, commercial considerations: after all, if Gmail messages are properly encrypted, then Google's computers can't read the content in order to decide what ads to display alongside them.) But let us be charitable and thankful for small mercies. The code for the service is out for testing and won't be made freely available until it's passed the scrutiny of the geek community, but still it's a significant moment, for which we have Edward Snowden to thank. The technology that Google will use is public key encryption, and it's been around for a long time and publicly available ever since 1991, when Phil Zimmermann created PGP (which stands for pretty good privacy). From then on, anyone who really wanted to communicate securely could have used PGP. The problem was (and is) that it's technically fiddly and you have to know what you're doing. And the persons with whom you wish to communicate securely also need to know what they're doing, and have PGP software installed at their end. Public key encryption is one of the great inventions of the 20th century. At its heart is a simple idea - that while it's trivially easy to multiply two very large numbers together, it's computationally very difficult to factorise the resulting product - ie to deduce what the original two numbers were. Each user has two large numbers, which serve as keys - one kept private, and the other made publicly available to anyone who wishes to communicate with him or her. PGP is terrific, but user-friendly it ain't, which is why most internet users balked at deploying it. The result was that the world's electronic communications flowed back and forth on media that were about as confidential as seaside postcards, thereby making it trivially easy for snoopers, both official and unofficial, to do their dastardly work. Google's plan is to make PGP user-friendly by incorporating it as an extension in its Chrome browser so that encryption (and decryption) are never more than a click or two away. In principle, it's a great idea. We will have to see how it

works in practice. Users will still have to manage their private keys, both in terms of keeping them secret and being able to locate them when needed. So the private-key problem will become like our current password problem, but on steroids. At this stage, nobody has any idea of how many Gmail users would want to use encryption, and one cynical way of interpreting the initiative is that Google is betting that it will only be a minority, so that its Adsense business will therefore be largely unaffected by it. If that turns out to be the case then the company will be able to claim - justifiably - that it is doing good (or at any rate, not being evil) without incurring any significant financial downside. Neat, eh? As I said, we have Edward Snowden to thank for this. His revelations about the vulnerability of the internet to surveillance has stimulated many people to recalibrate their assumptions about how the online world should be configured. All over the place, engineers like the guys at Google have been working out ways of building serious encryption into every device and channel on the internet to reduce the vulnerabilities inherent in a system that was originally built for a community of trustworthy researchers.

Encryption is Surveillance

Encryption cracking is a form of surveillance

Karin Lillington, January 22, 2015, Irish Times, World Without Data Encryption unimaginable, <http://www.highbeam.com/doc/1P2-37591772.html> DOA: 2-21-15

If the national legislatures of the United Kingdom and United States decide their leaders are right, and laws are passed to cripple encryption and permit other forms of mass surveillance, the world - especially the business world - will become a very strange, more vulnerable and difficult-to- regulate place.

Backdoors create unique vulnerabilities – intentionally weakened encryption cause the majority of malicious attacks

Castillo 6/16 Andrea Castillo, program manager for the Technology Policy Program at the Mercatus Center, “Giving Government ‘Backdoor’ Access to Encrypted Data Threatens Personal Privacy and National Security”, <http://reason.com/archives/2015/06/16/crypto-wars-weaken-encryption-security>

The War on Terror provides plenty of rhetorical ammunition to these anti-encryption officials, who seem to believe that purposefully sabotaging our strongest defenses against "cyberterrorists" is an effective way to promote national security. But they are dangerously wrong, as recent revelations of decades-old security vulnerabilities imposed by encryption restrictions make all too clear.¹

Encryption allows people to securely send data that can only be accessed by verified parties. Mathematical techniques convert the content of a message into a scrambled jumble, called a ciphertext, which looks like nonsense in electronic transit until it is decoded by the intended recipient. Simple ciphers have been used to secure communications since the days of the Egyptian Old Kingdom, when a particularly devoted scribe took to fancying up the tomb of Khnumhotep II with cryptic funeral prose. Our own Thomas Jefferson regularly used ciphers in communications with James Madison, John Adams, and James Monroe to "keep matters merely personal to ourselves."¹ State military and research offices were the main 20th century beneficiaries of advanced encryption techniques until the development of public-key cryptography in the 1970s, which afforded commercial and private users a means to protect their data against unwanted infiltration. Now, what was once a mere means to share secrets has become an indispensable component of personal and national data security.¹ An estimated 40 million cyberattacks occurred in 2014, imposing millions in costs and weeks of frustration for organizations and individual users alike. Many of these costly breaches could be prevented through encryption techniques that regulate data access, authenticate users, and secure sensitive information. A secret report from the U.S. National Intelligence Council—ironically, leaked by Edward Snowden thanks to the government's own poor authentication practices—even made the case that encryption was the "best defense" to protect private data. Yet intelligence agencies and their allies have consistently set out to limit encryption technologies (many of which they developed or relied upon themselves previously).¹ The seeds of the first Crypto Wars were sown during the Cold War, when the U.S. imposed strong export controls on encryption techniques to keep them away from the Russkies. Only a small set of relatively weak techniques approved by the Commerce and State Departments could be used in international business. But this practice was dangerously self-defeating. Compelling foreign users to settle for weakened encryption standards ultimately made U.S. users more vulnerable by introducing unnecessary fragility.¹ A timely case in point is the recent revelations of security vulnerabilities in thousands of Web browsers and mail servers—vulnerabilities that were directly introduced by the artificially weak encryption

programs compelled by the earlier export ban. In March, a massive vulnerability affecting the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols ubiquitous to most users' Internet experiences, called "FREAK," was discovered. Later in May, researchers discovered a similar TLS vulnerability, LOGJAM, which attacked a different kind of key exchange technique. These dual security bugs exposed countless Internet users to potential "man-in-the middle-attacks," allowing malicious hackers (or tight-lipped intelligence agents) access to supposedly secure data for decades.³¹ Export controls on encryption were easier to enforce before the advent of personal computing, when only institutional (and usually government-connected) organizations operating huge supercomputers would be effected by such bans—although academics did not exactly hide their discontent at the inconvenience dealt to their research projects. The rise of the home computer dramatically changed the calculus. The export ban on encryption imposed arbitrary boundaries on a network that is borderless by definition.³² Enter the cypherpunks: a ragtag, homebrew crew of anti-authoritarian hackers hell-bent on subverting spooks and protecting privacy on the 'Net. These luminaries developed the tools and rhetoric to make bad laws irrelevant by making them unenforceable. For example, Phil Zimmerman's Pretty Good Privacy (PGP) program, a mainstay of modern email delivery, which Zimmerman posted to Usenet in 1991. After a three-year criminal investigation, the U.S. Attorney's Office decided not to prosecute Zimmerman for sharing the encryption protocol. Throughout the '90s, federal officials continued to ease strict export restrictions, and the future of encryption seemed secure. Edward Snowden's 2013 revelations, however, made it clear that the so-called "Crypto Wars" were actually far from settled. Snowden revealed that the NSA worked with foreign spooks to compromise encryption by controlling international standards for their own purposes and even out-and-out colluded with technology firms through the "BULLRUN" program. Only after these outrageous methods were exposed to the world did the forces of surveillance bother attempting to legitimize these practices through less illegal public means—albeit with the rhetorical gall of concealing obvious spying ambitions in the more reasonable garb of genuine law enforcement concerns.

Surveillance enables cyberterrorism by creating backdoors in our critical infrastructure while allowing hackers to model our technological capabilities—it's only a matter of time before our vulnerabilities are exploited

Seneque, ICT professional with a particular focus on UNIX Architecture & Design, 14

Gareth, holds a degree in Philosophy/Politics from the University of Sydney, Alex Comninos, an independent researcher focusing on information and communications technology and politics, a Doctoral Candidate at Justus-Liebig University in Giessen, Germany at the Department of Geography, where he is conducting doctoral research on the challenges and constraints of the use of user-generated geographic information systems in Egypt, Libya, and North and Sudan in 2010 to 2011, "Cyber security, civil society and vulnerability in an age of communications surveillance", 2014, Justus-Liebig University Giessen and Geist Consulting, giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur

The relevance of Snowden's disclosures to cyber security The scope and reach of the NSA's surveillance is important. The NSA's surveillance posture is – as has been repeated by General Keith Alexander, and is reflected in the NSA slide in Figure 1 – to "collect it all":³² from undersea cable taps, to Yahoo video chats, to in-flight Wi-Fi, to virtual worlds and online multiplayer games like Second Life and World of Warcraft. The NSA has at least three different programmes to get Yahoo and Google user data. This shows that they try to get the same data from multiple mechanisms.³³ With the GCHQ under the MUSCULAR programme it hacked into the internal data links of Google and Yahoo³⁴ for information that it could mostly have gotten through the PRISM programme. In addition to highlighting the NSA's massive institutional overreach and global privacy invasion, Snowden's disclosures also highlight the many points at which our data is insecure, and the vast numbers of vulnerabilities to surveillance that exist throughout our digital world. However, while the NSA is the largest threat in the surveillance game, it is not the only threat. Governments all around the world are using the internet to surveil their citizens. Considering the rate of technological change, it is not unforeseeable that the methods, tools and vulnerabilities used by the NSA will be the tools of states, cyber criminals and low-skilled hackers of the future. Regardless of who the perceived attacker or surveillance operative may be, and whether it is the NSA or not, large-scale, mass surveillance is a growing cyber security threat. It has also been

disclosed that the NSA and GCHQ have actively worked to make internet and technology users around the world less secure. **The NSA has placed backdoors in routers running vital internet infrastructures.**³⁵ The GCHQ has impersonated social networking websites like LinkedIn in order to target system administrators of internet service providers.³⁶ **The NSA has been working with the GCHQ to hack into Google and Yahoo data centres.**³⁷ **The NSA also works to undermine encryption technologies, by covertly influencing the use of weak algorithms and random number generators in encryption products and standards.**³⁸ The NSA in its own words is working under the BULLRUN programme to "insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets" and to "influence policies, standards and specifications for commercial [encryption] technologies."³⁹ **The NSA is also believed to hoard knowledge about vulnerabilities rather than sharing them with developers, vendors and the general public,**⁴⁰ as well as even maintaining a catalogue of these vulnerabilities for use in surveillance and cyber attacks.⁴¹ None of these activities serve to make the internet more secure. In fact, they do the very opposite. As US Congresswoman Zoe Lofgren commented: "When any industry or organisation builds a backdoor to assist with electronic surveillance into their product, they put all of our data security at risk. If a backdoor is created for law enforcement purposes, it's only a matter of time before a hacker exploits it, in fact we have already seen it happen."⁴²

The risk of cyberterrorism is high—experts agree that adversaries have the technical skills and political motivation to carry out a dangerous cyberattack

Burg, Principal US & Global Cybersecurity Leader, 14

David, Michael Compton Principal, Cybersecurity Strategy & Operations, Peter Harries Principal, Health Industries, John Hunt Principal, Public Sector, Mark Lobel Principal, Technology, Entertainment, Media & Communications, Gary Loveland Principal, Consumer and Industrial Products & Services, Joe Nocera Principal, Financial Services, Dave Roath Partner, Risk Assurance, "US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey", June 2014, co-sponsored by The CERT Division of the Software Engineering Institute at Carnegie Mellon University, CSO magazine, United States Secret Service, www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

The risks and repercussions of cybercrime In this 12th survey of cybercrime trends, more than 500 US executives, security experts, and others from the public and private sectors offered a look into their cybersecurity practices and state of risk and readiness to combat evolving cyber threats and threat agents. One thing is very clear: **The cybersecurity programs of US organizations do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries.** Today, common criminals, organized crime rings, and nation-states leverage sophisticated techniques to launch attacks that are highly targeted and very difficult to detect.

Particularly worrisome are attacks by tremendously skilled threat actors that attempt to steal highly sensitive—and often very valuable—intellectual property, private communications, and other strategic assets and information. It is a threat that is nothing short of formidable. In fact, **the US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction.** Underscoring the threat, the FBI last year notified 3,000 US companies—ranging from small banks, major defense

contractors, and leading retailers—that they had been victims of cyber intrusions. “**The United States faces real [cybersecurity] threats from criminals, terrorists, spies, and malicious cyber actors,**” said FBI Director James B. Comey at a recent security conference.² “The playground is a very dangerous place right now.” **Nation-state actors pose a particularly pernicious threat**, according to Sean Joyce, a PwC principal and former FBI deputy director who frequently testified before the US House and Senate Intelligence committees. “**We are seeing increased activity from nation-state actors, which could escalate due to unrest in Syria, Iran, and Russia,**” he said. “**These groups may target financial services and other critical infrastructure entities.**” In today’s volatile cybercrime environment, nation-states and other criminals continually and rapidly update their tactics to maintain an advantage against advances in security safeguards implemented by businesses and government agencies. Recently, for instance, hackers engineered a new round of distributed denial of service (DDoS) attacks that can generate traffic rated at a staggering 400 gigabits per second, the most powerful DDoS assaults to date.

3 Internal links

1. Norm-Building—Curtailing surveillance is key to effective norms-building—that prevents cyber-warfare

Farrell 2015, Henry Farrell, PhD in Government from Georgetown University, Associate Professor of Political Science and International Affairs, April 2015, Promoting Norms for Cyberspace, Council on Foreign Relations, http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358?cid=nlc-press_release-press_note--link2-20150406&sp_mid=48385113&sp_rid=YWtpbWVyeUBoc3RvZGF5LnVzS0

U.S. policymakers argue that **the United States and others need to build norms to mitigate cybersecurity problems**. Admiral Michael S. Rogers, head of the National Security Agency (NSA) and Cyber Command, has argued that shared norms are a basic building block for cybersecurity. He has called on actors in academia and civil society to help design them and to assist in their spread.[¶] It may seem strange that Pentagon officials are arguing for **soft tools rather than hard military options**, but there are four good reasons why norms **are the best option available**. First, **the United States is vulnerable to cyberattacks** and **this weakness is difficult to address using conventional tools of military statecraft**. Second, **it is difficult to ensure that complex information systems are fully defended**, since **they may have subtle technical weaknesses**. Third, **classical deterrence is not easy in a world where it is often challenging to identify sophisticated attackers**, or even to know when an attack has taken place. Lastly, **treaties are hard to enforce because it is so difficult to verify compliance—particularly in cyberspace**, where weapons are software, not missiles.[¶] Although norms are hazier than treaty rules, they may still have important consequences. Norms against the use of nuclear weapons have taken hold since the 1950s, making their use nearly unthinkable in ordinary circumstances. **Robust cybersecurity norms might, over time, rule out some kinds of attacks as normatively inappropriate. They might encourage other states to see norm breaches as attacks on their security, too, spurring cooperation** to prevent or stop attacks. Finally, **norms can provide shared understandings between states that allow them to work together** where they have shared interests and manage relations where their interests clash.[¶] Challenges to Norm Promotion **It is hard to spread norms, even in the best circumstances**. Unfortunately, **these are far from the best circumstances for the United States**. U.S. policymakers face three major problems. First, it is easiest to promote norms when one can invoke common values to support them, yet the world’s cyber powers have different—and radically incompatible—values over how to protect cyberspace. The clashing interests between democratic and authoritarian regimes on the value of an open Internet and definitions of security make effective global treaties impossible.[¶] Second, the potential **adopters of norms are likely to be more receptive if they do not think the proponent of the norms is acting in bad faith**. To be sure, **many states were happy to use the Snowden revelations as a cover for opposition to any rules of behavior Washington might offer**. But for others, **efforts at persuasion have been damaged by the exposed gap between U.S. rhetoric and actions**. At the very least, other states must be persuaded that following a norm is in their national interest. The disclosures, however, reinforced the view of many states that the United States disproportionately benefits from an open, global, and

secure Internet, and is only committed to these values to the extent that they further U.S. economic, political, and military objectives.[¶] In light of the Snowden disclosures, the United States is poorly placed to persuade other actors of its good faith or its commitment to shared interests and values. The extent of the damage to the U.S. reputation was revealed when the United States accused North Korea of hacking into Sony's servers and announced its intention to retaliate against North Korea through low-level sanctions. Building on previous indictments of Chinese soldiers for hacking into U.S. firms, U.S. officials followed an approach of "naming and shaming" cyberattackers while pursuing sanctions and possible criminal charges. These actions are highly unlikely to result in successful prosecutions, but potentially serve a normative purpose by signaling to the world that some actions are unacceptable. Although a few states criticized North Korea, many did not buy U.S. claims that Pyongyang was responsible. Members of the business and technology communities also expressed polite skepticism over the evidence supplied by the Federal Bureau of Investigation.

2. Trust- Requiring the government to get a warrant solves while maintaining intelligence capabilities – the government has to engage companies to access information instead of taking it

Ackerman 7/8 Spencer Ackerman, national security editor for the Guardian, 7/8/15, "FBI chief wants 'backdoor access' to encrypted communications to fight Isis", <http://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis>

The director of the Federal Bureau of Investigation has warned US senators that the threat from the Islamic State merits a "debate" about limiting commercial encryption – the lynchpin of digital security – despite a growing chorus of technical experts who say that undermining encryption would prove an enormous boon for hackers, cybercriminals, foreign spies and terrorists.[¶] In a twin pair of appearances before the Senate's judiciary and intelligence committees on Wednesday, James Comey testified that Isis's use of end-to-end encryption, whereby the messaging service being used to send information does not have access to the decryption keys of those who receive it, helped the group place a "devil" on the shoulders of potential recruits "saying kill, kill, kill, kill".[¶] Comey said that while the FBI is thus far disrupting Isis plots, "I cannot see me stopping these indefinitely". He added: "I am not trying to scare folks."[¶] Since October, following Apple's decision to bolster its mobile-device security, Comey has called for a "debate" about inserting "back doors" – or "front doors", as he prefers to call them – into encryption software, warning that "encryption threatens to lead us all to a very, very dark place".[¶] But Comey and deputy attorney general Sally Quillian Yates testified that they do not at the moment envision proposing legislation to mandate surreptitious or backdoor access to law enforcement. Both said they did not wish the government to itself hold user encryption keys and preferred to "engage" communications providers for access, though technicians have stated that what

Comey and Yates seek is fundamentally incompatible with end-to-end encryption.[¶] Comey, who is not a software engineer, said his response to that was: "Really?" He framed himself as an advocate of commercial encryption to protect personal data who believed that the finest minds of Silicon Valley can invent new modes of encryption that can work for US law enforcement and intelligence agencies without inevitably introducing security flaws.[¶] While the FBI director did not specifically cite which encrypted messaging apps Isis uses, the Guardian reported in December that its grand mufti used WhatsApp to communicate with his former mentor. WhatsApp adopted end-to-end encryption last year. "I think we need to provide a court-ordered process for obtaining that data," said Dianne Feinstein, the California Democrat and former intelligence committee chair who represents Silicon Valley.[¶] But Comey's campaign against encryption

has run into a wall of opposition from digital security experts and engineers. Their response is that there is no technical way to insert a back door into security systems for governments that does not leave the door ajar for anyone – hackers, criminals, foreign intelligence services – to exploit and gain access to enormous treasure troves of user data, including medical records, financial information and much more.

3. Plan solves backdoors-makes them get a warrant

James Ball and Spencer Ackerman 8/9/13 (James Ball is special projects editor of the Guardian. Spencer Ackerman is national security editor for Guardian US. A former senior writer for Wired, he won the 2012 National Magazine Award for Digital Reporting “NSA loophole allows warrantless search for US citizens' emails and phone calls”

<http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls>
accessed 7/26/15 BP))

The National Security Agency has a secret backdoor into its vast databases under a legal authority enabling it to search for US citizens' email and phone calls without a warrant, according to a top-secret document passed to the Guardian by Edward Snowden. The previously undisclosed rule change allows NSA operatives to hunt for individual Americans' communications using their name or other identifying information. Senator Ron Wyden told the Guardian that **the law provides the NSA with a loophole potentially allowing "warrantless searches for the phone calls or emails of law-abiding Americans".** The authority, approved in 2011, appears to contrast with repeated assurances from Barack Obama and senior intelligence officials to both Congress and the American public that the privacy of US citizens is protected from the NSA's dragnet surveillance programs. The intelligence data is being gathered under Section 702 of the Fisa Amendments Act (FAA), which gives the NSA authority to target without warrant the communications of foreign targets, who must be non-US citizens and outside the US at the point of collection. **The communications of Americans in direct contact with foreign targets can also be collected without a warrant, and the intelligence agencies acknowledge that purely domestic communications can also be inadvertently swept into its databases. That process is known as "incidental collection" in surveillance parlance. But this is the first evidence that the NSA has permission to search those databases for specific US individuals' communications.** A secret glossary document provided to operatives in the NSA's Special Source Operations division – which runs the Prism program and large-scale cable intercepts through corporate partnerships with technology companies – details an update to the "minimization" procedures that govern how the agency must handle the communications of US persons. That group is defined as both American citizens and foreigners located in the US. "While the FAA 702 minimization procedures approved on 3 October 2011 now allow for use of certain United States person names and identifiers as query terms when reviewing collected FAA 702 data," the glossary states, "analysts may NOT/NOT [not repeat not] implement any USP [US persons] queries until an effective oversight process has been developed by NSA and agreed to by DOJ/ODNI [Office of the Director of National Intelligence]." The term "identifiers" is NSA jargon for information relating to an individual, such as telephone number, email address, IP address and username as well as their name. The document – which is undated, though metadata suggests this version was last updated in June 2012 – does not say whether the oversight process it mentions has been established or whether any searches against US person names have taken place. Ron Wyden Senator Ron Wyden. Photograph: Jacquelyn Martin/AP Wyden, an Oregon Democrat on the Senate intelligence committee, has obliquely warned for months that the NSA's retention of Americans' communications incidentally collected and **its ability to search through**

it has been far more extensive than intelligence officials have stated publicly. Speaking this week, Wyden told the Guardian **it amounts to a "backdoor search" through Americans' communications data..**

A cyber-attack would trigger military retaliation and escalate to nuclear war

Robert Tilford 12, Graduate US Army Airborne School, Ft. Benning, Georgia, “Cyber attackers could shut down the electric grid for the entire east coast” 2012,
<http://www.examiner.com/article/cyber-attackers-could-easily-shut-down-the-electric-grid-for-the-entire-east-coast> ***we don’t agree with the ableist language

To make matters worse **a cyber attack that can take out a civilian power grid**, for example **could also cripple (destroy) the U.S. military**. The senator notes that is that **the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power every military base in our country.** “Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out”, he said. Which means **military command and control centers could go dark, Radar systems that detect air threats to our country would shut Down completely.** “Communication between commanders and their troops would also go silent. And many weapons systems would be left without either fuel or electric power”, said Senator Grassley. “So **in a few short hours** or days, **the mightiest military in the world would be left scrambling to maintain base functions**”, he said. We contacted the Pentagon and officials confirmed the threat of a cyber attack is something very real. Top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director—have said, “**preventing a cyber attack** and improving the nation’s electric grids **is among the most urgent priorities** of our country” (source: Congressional Record). So how serious is the Pentagon taking all this? Enough to start, or end a war over it, for sure. **A cyber attack today against the US could** very well **be seen as an “Act of War”** and could be met with a “full scale” US military response. That could include the use of “**nuclear weapons**”, if authorized by the President.

Cyber-attacks could shut down the power grid for years

Daly, columnist @ The Daily Beast, 13

Michael, "U.S. Not Ready for Cyberwar Hostile Hackers Could Launch", Feb 21 2013,
www.thedailybeast.com/articles/2013/02/21/u-s-not-ready-for-cyber-war-hostile-hackers-could-launch.html

If the nightmare scenario becomes suddenly real ... **If hackers shut down much of the electrical grid and the rest of the critical infrastructure goes with it ... If we are plunged into chaos and suffer more physical destruction than 50 monster hurricanes and economic damage that dwarfs the Great Depression ... Then we will wonder why we failed to guard against what** outgoing Defense Secretary Leon Panetta has termed a “cyber-Pearl Harbor.” “**An aggressor nation or extremist group could use these kinds of cybertools to gain control of critical switches,**” Panetta said in a speech in October. “**They could** derail passenger trains or, even more dangerous, **derail** passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities or **shut down the power grid across large parts of the country.**” And **Panetta was hardly being an alarmist.** He could have added that cybersecurity experts such as Joe Weiss of Applied Control Solutions suggest a **full-on cyberattack would seek not simply to shut down systems, but wreck them**, using software to destroy hardware. Some believe **we could then be sent into chaos not just for days of even weeks, but for months.** The mother of all nightmare scenarios would

see electric, oil, gas, water, chemical, and transit, our entire essential infrastructure, knocked out as we sought to replace equipment that can take more than a year to manufacture and is in many cases no longer made in the U.S. Lights would stay out. Gas stations would be unable to pump and would have nothing to pump anyway. There would be no heat, no fuel, in many places no running water, no sewage treatment, no garbage, no traffic lights, no air-traffic control, minimal communication, and of course, no Wi-Fi. Neighborhoods around chemical plants could become Bhopals.

A long-term loss of electrical power would cause nuclear reactor meltdowns—guarantees extinction

Hodges 14

Dave, an established award winning psychology, statistics and research professor as he teaches college and university classes at both the undergraduate and graduate level, an established author as his articles are published on many major websites, citing Judy Haar, a recognized expert in nuclear plant failure analyses, "Nuclear Power Plants Will Become America's Extinction Level Event", April 18 2014, www.thelibertybeacon.com/2014/04/18/nuclear-power-plants-will-become-americas-extinction-level-event/

Fukushima is often spoken of by many, as a possible extinction level event because of the **radiation threat**. Fukushima continues to wreak havoc upon the world and in the United States as we are being bathed in deadly radiation from this event. **Because of Fukushima, fish are becoming inedible and the ocean currents as well as the prevailing ocean winds are carrying deadly radiation. Undoubtedly**, by this time, **the radioactivity has made its way into the transpiration cycle which means that crops are being dowsed with deadly radiation. The radiation has undoubtedly made its way into the water table in many areas and impacts every aspect of the food supply. The health costs to human beings is incalculable**. However, **this article** is not about the devastation at Fukushima, instead, this article **focuses on the fact that North America could have** a total of **124 Fukushima events** if the necessary conditions were present. A festering problem **Long before Fukushima, American regulators knew that a power failure lasting for days involving the power grid connected to a nuclear plant**, regardless of the cause, **would most likely lead to a dangerous radioactive leak in at least several nuclear power plants. A complete loss of electrical power poses a major problem for nuclear power plants** because **the reactor core must be kept cool as well as the back-up cooling systems, all of which require massive amounts of power to work**. Heretofore, **all the NERC drills which test the readiness of a nuclear power plant are predicated on the notion that a blackout will only last 24 hours or less**.

Amazingly, this is the sum total of a NERC litmus test. Although we have the technology needed to harden and protect our grid from an EMP event, whether natural or man-made, we have failed to do so. The cost for protecting the entire grid is placed at about the cost for one B-1 Stealth Bomber. Yet, as a nation, we have done nothing. This is inexplicable and inexcusable. Our collective inaction against protecting the grid prompted Congressman Franks to write a scathing letter to the top officials of NERC. However, the good Congressman failed to mention the most important aspect of this problem. **The problem is entirely fixable and NERC and the US government are leaving the American people and its infrastructure totally unprotected from a total meltdown of nuclear power plants as a result of a prolonged power failure**.

Critical Analyses According to Judy Haar, a recognized expert in nuclear plant failure analyses, **when a nuclear power plant loses access to off-grid electricity, the event is referred to as a “station blackout”**. Haar states that all 104 US nuclear power plants are built to withstand electrical outages without experiencing any core damage, through the activation of an automatic start up of emergency generators powered by diesel. Further, **when emergency power kicks in, an automatic shutdown of the nuclear power plant commences**. The dangerous control rods are dropped into the core, while water is pumped by the diesel power generators into

the reactor to reduce the heat and thus, prevent a meltdown. Here is the catch in this process, the spent fuel rods are encased in both a primary and secondary containment structure which is designed to withstand a core meltdown. However, should the pumps stop because either the generators fail or diesel fuel is not available, the fuel rods are subsequently uncovered and a Fukushima type of core meltdown commences immediately. At this point, I took Judy Haar's comments to a source of mine at the Palo Verde Nuclear power plant. My source informed me that as per NERC policy, nuclear power plants are required to have enough diesel fuel to run for a period of seven days. Some plants have thirty days of diesel. This is the good news, but it is all downhill from here. The Unresolved Power Blackout Problem **A long-term loss of outside electrical power will most certainly interrupt the circulation of cooling water to the pools.** Another one of my Palo Verde nuclear power plant sources informed me that there is no long term solution to a power blackout and that all bets are off if the blackout is due to an EMP attack. A more detailed analysis reveals that the spent fuel pools carry depleted fuel for the reactor. Normally, this spent fuel has had time to considerably decay and therefore, reducing radioactivity and heat. However, the newer discharged fuel still produces heat and needs cooling. Housed in high density storage racks, contained in buildings that vent directly into the atmosphere, radiation containment is not accounted for with regard to the spent fuel racks. In other words, there is no capture mechanism. In this scenario, accompanied by a lengthy electrical outage, and with the emergency power waning due to either generator failure or a lack of diesel needed to power the generators, the plant could lose the ability to provide cooling. The water will subsequently heat up, boil away and uncover the spent fuel rods which required being covered in at least 25 feet of water to remain benign from any deleterious effects. Ultimately, this would lead to fires as well and the release of radioactivity into the atmosphere. This would be the beginning of another Fukushima event right here on American soil. Both my source and Haar shared exactly the same scenario about how a meltdown would occur. Subsequently, I spoke with Roger Landry who worked for Raytheon in various Department of Defense projects for 28 years, many of them in this arena and Roger also confirmed this information and that the above information is well known in the industry. When I examine Congressman Franks letter to NERC and I read between the lines, it is clear that Franks knows of this risk as well, he just stops short of specifically mentioning it in his letter. Placing Odds On a Failure Is a Fools Errand An analysis of individual plant risks released in 2003 by the Nuclear Regulatory Commission shows that for 39 of the 104 nuclear reactors, the risk of core damage from a blackout was greater than 1 in 100,000. At 45 other plants the risk is greater than 1 in 1 million, the threshold NRC is using to determine which severe accidents should be evaluated in its latest analysis. According to the Nuclear Regulatory Commission, the Beaver Valley Power Station, Unit 1, in Pennsylvania has the greatest risk of experiencing a core meltdown, 6.5 in 100,000, according to the analysis. These odds don't sound like much until you consider that we have 124 nuclear power generating plants in the US and Canada and when we consider each individual facility, the odds of failure climb. How many meltdowns would it take in this country before our citizens would be condemned to the hellish nightmare, or worse, being experienced by the Japanese? The Question That's Not Being Asked None of the NERC, or the Nuclear Regulatory tests of handling a prolonged blackout at a nuclear power plant has answered two critical questions, "What happens when these nuclear power plants run out of diesel fuel needed to run the generators", and "What happens when some of these generators fail?" In the event of an EMP attack, can tanker trucks with diesel fuel get to all of the nuclear power plants in the US in time to re-fuel them before they stop running? Will tanker trucks even be running themselves in the aftermath of an EMP attack? And in the event of an EMP attack, it is not likely that any plant which runs low on fuel, or has a generator malfunctions, will ever get any help to mitigate the crisis prior to a plethora of meltdowns occurring. Thus, every nuclear power plant in the country has the potential to cause a Chernobyl or Fukushima type accident if our country is hit by an EMP attack. **CAN YOU EVEN IMAGINE 124 FUKUSHIMA EVENTS IN NORTH AMERICA HAPPENING AT THE SAME TIME? THIS WOULD CONSTITUTE THE ULTIMATE DEPOPULATION EVENT.** ...And There Is More... The ramifications raised in the previous paragraphs are significant. What if the blackout lasts longer than 24 hours? What if the reason for the blackout is an EMP burst caused by a high altitude nuclear blast and transportation comes to a standstill? In this instance, the cavalry is not coming. Adding fuel to the fire lies in the fact that the power transformers presently take at least one year to replace. Today, there is a three year backlog on ordering because so many have been ordered by China. This makes one

wonder what the Chinese are preparing for with these multiple orders for both transformers and generators. In short, our unpreparedness is a prescription for disaster. As a byproduct of my investigation, I have discovered that most, if not all, of the nuclear power plants are on known earthquake fault lines. All of California's nuclear power plants are located on an earthquake fault line. Can anyone tell me why would anyone in their right mind build a nuclear power plant on a fault line? To see the depth of this threat you can visit an interactive, overlay map at this site. Conclusion I have studied this issue for almost nine months and this is the most elusive topic that I have ever investigated. The more facts I gather about the threat of a mass nuclear meltdown in this country, the more questions I realize that are going unanswered. With regard to the nuclear power industry we have the proverbial tiger by the tail. Last August, Big Sis stated that it is not matter of if we have a mass power grid take down, but it is a matter of when. I would echo her concerns and apply the “not if, but when” admonition to the possibility of a mass meltdown in this country. It is only a matter of time until this scenario for disaster comes to fruition. Our collective negligence and high level of extreme depraved indifference on the part of NERC is criminal because this is indeed an Extinction Level Event. At the end of the day, can anyone tell me why would any country be so negligent as to not provide its nuclear plants a fool proof method to cool the secondary processes of its nuclear materials at all of its plants? Why would ANY nuclear power plant be built on an earthquake fault line? Why are we even using nuclear energy under these circumstances? And why are we allowing the Chinese to park right next door to so many nuclear power plants?

Hacking devastates the economy – the average cost per attack is over twelve million dollars

Ponemon 2014 Ponemon Institute, conducts independent research on privacy, data protection and information security policy, October 2014, “2014 Global Report on the Cost of Cyber Crime”, <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf>, p. 2-4

During the period we conducted interviews and analyzed the findings, mega cyber crimes took place. Most notable was the Target cyber breach, which was reported to result in the theft of 40 million payment cards. More recently, Chinese hackers launched a cyber attack against Canada's National Research Council as well as commercial entities in Pennsylvania, including Westinghouse Electric Company, U.S. Steel and the United Steel Workers Union. Russian hackers recently stole the largest collection of Internet credentials ever: 1.2 billion user names and passwords, plus 500 million email addresses. While the companies represented in this research did not have cyber attacks as devastating as these were, they did experience incidents that were expensive to resolve and disruptive to their operations. For purposes of this study, we refer to cyber attacks as criminal activity conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure. Our goal is to quantify the economic impact of cyber attacks and observe cost trends over time. We believe a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the consequences of an attack.[¶] In our experience, a traditional survey approach does not capture the necessary details required to extrapolate cyber crime costs. Therefore, we conduct field-based research that involves interviewing senior-level personnel about their organizations' actual cyber crime incidents. Approximately 10 months of effort is required to recruit companies, build an activity-based cost model to analyze the data, collect source information and complete the analysis.[¶] For consistency purposes, our benchmark sample consists of only larger-sized organizations (i.e., more than 1,000 enterprise seats¹). The study examines the total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.[¶] Global at a glance[¶] This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, France and for the first time, the Russian Federation, with a total benchmark sample of 257 organizations. Country-specific results are presented in seven separate reports.[¶] Figure 1 presents the estimated average cost of cyber crime for seven country samples involving 257 separate companies, with comparison to last year's country averages. Cost figures are converted into U.S. dollars for comparative purposes. ^{2¶} As shown, there is significant variation in total cyber crime costs among

participating companies in the benchmark samples. The US sample reports the highest total average cost at \$12.7 million and the Russian sample reports the lowest total average cost at \$3.3 million. It is also interesting to note that all six countries experienced a net increase in the cost of cyber crime cost over the past year – ranging from 2.7 percent for Japan to 22.7 percent for the United Kingdom. The percentage net change between FY 2014 and FY 2013 (excluding Russia) is 10.4 percent.¹ Summary of global findings¹ Following are the most salient findings for a sample of 257 organizations requiring 2,081 separate interviews to gather cyber crime cost results. In several places in this report, we compare the present findings to last year's average of benchmark studies.¹ **Cyber crimes continue to be on the rise for organizations.** We found that the mean annualized cost for 257 benchmarked organizations is \$7.6 million per year, with a range from \$0.5 million to \$61 million per company each year. Last year's mean cost for 235 benchmarked organizations was \$7.2 million. **We observe a 10.4 percent net change from last year** (excluding the Russian sample).¹ **Cyber crime cost varies by organizational size.** Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost.³ However, **based on enterprise seats, we determined that small organizations incur a significantly higher per capita cost than larger organizations** (\$1,601 versus \$437).¹ **All industries fall victim to cybercrime**, but to different degrees. **The average annualized cost of cyber crime appears to vary by industry segment, where organizations in energy & utilities and financial services experience substantially higher cyber crime costs than organizations in media, life sciences and healthcare.**¹ The most costly cyber crimes are those caused by malicious insiders, denial of services and web-based attacks. These account for more than 55 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, applications security testing solutions and enterprise GRC solutions.¹ **Cyber attacks can get costly if not resolved quickly.** Results show a positive relationship between the time to contain an attack and organizational cost. Please note that resolution does not necessarily mean that the attack has been completely stopped. For example, **some attacks remain dormant and undetected (i.e., modern day attacks).** **The average time to contain a cyber attack was 31 days, with an average cost to participating organizations of \$639,462 during this 31-day period. This represents a 23 percent increase from last year's estimated average cost of \$509,665, which was based upon a 27-day remediation period.** Results show that malicious insider attacks can take more than 58 days on average to contain.¹ **Business disruption represent the highest external cost, followed by the costs associated with information loss.**⁴ On an annualized basis, **business disruption accounts for 38 percent of total external costs**, which include costs associated with business process failures and lost employee productivity. **Detection is the most costly internal activity followed by recovery**. On an annualized basis, **detection and recovery costs combined account for 53 percent of the total internal activity cost with cash outlays and direct labor representing the majority of these costs.** Activities relating to IT security in the network layer receive the highest budget allocation. In contrast, the host layer receives the lowest funding level.

Econ decline causes nuclear war

Hutchinson 14 (Martin, Business and Economics Editor at United Press International, MBA from Harvard Business School, former international merchant banker, 1-3-14, “The chilling echoes of 1914, a century on” Wall Street Journal) <http://online.wsj.com/articles/william-galston-secular-stagnation-may-be-for-real-1409095263>,

The years before 1914 saw the formation of trade blocs separated by high tariff barriers. Back then, the world was dominated by several roughly equivalent powers, albeit with different strengths and weaknesses. Today, the world is similarly multi-polar. The United States is in a position of clear leadership, but China is coming up fast. Europe is weaker than it was, but is still a force to be reckoned with. Japan, Russia, Brazil, India are also too powerful to ignore. A hundred years ago, big international infrastructure projects such as the Berlin-Baghdad Railway, and before it the Suez Canal, were built to protect favored trading. Today's equivalent may be the bilateral mining partnerships forged between, for instance, China and mineral-rich African states. Today, the World Trade Organization offers some defence against tariffs. But protectionism could become entrenched if prolonged economic stagnation leads countries to pursue their own narrow interests. Germany, Austria, Russia and France lost between 20 and 35 percent of national output between 1913 and 1918, according to Angus Maddison's data used in Stephen Broadberry's “The Economics of World War One: A Comparative Analysis”. British GDP declined in 1914 and 1915, but grew 15 percent over the four years, as did the U.S. economy. The 37 million military and civilian casualties may tell a more accurate story but **if history were to repeat itself, the global conflict could be both more universal and more destructive. Nuclear weapons proliferate.** Warped diplomatic anger could lead to the deployment of chemical and biological devices. **Electromagnetic pulses could wipe out our fragile electronic networks.** Like the assassination of Archduke

Ferdinand that sparked World War One, the catalyst for cataclysm might be something quite surprising. A global run on bank and other investment assets or an outbreak of hyperinflation, maybe? These threats get more serious the more policymakers pump up equity, bond, property and banking bubbles. If global wealth evaporates, or is proven to be an illusion, today's largely cordial global entente could be smashed with precipitous speed.

Inherency – Encryption Cracking Now

The NSA is permitted to crack encryption in the status quo

David Sanger, April 12, 2014, Obama lets N.S.A. exploit online security flaws, officials say,
<http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html> DOA: 3-21-15

Stepping into a heated debate within the United States intelligence agencies, President **Obama** has decided that when the National Security Agency discovers major flaws in Internet security, it should - in most circumstances - reveal them to assure that they will be fixed, rather than keep mum so that the flaws can be used in espionage or cyberattacks, senior administration officials said over the weekend. But Mr. Obama carved a broad exception for "a clear national security or law enforcement need," the officials said on Saturday, a loophole that is likely to allow the N.S.A. to continue to exploit security flaws both to crack encryption on the Internet and to design cyberweapons. The White House has never publicly detailed Mr. Obama's decision, which he made in January as he began a three-month review of recommendations by a presidential advisory committee on what to do in response to recent disclosures about the National Security Agency. But elements of the decision became evident on Friday, when the White House denied that it had any prior knowledge of the Heartbleed bug, a newly known hole in Internet security that sent Americans scrambling last week to change their online passwords. The White House statement said that when such flaws are discovered, there is now a "bias" in the government to share that knowledge with computer and software manufacturers so a remedy can be created and distributed to industry and consumers.

NSA hacking the networks of leading companies to break encryption

John Naughton, March 8, 2015, The Guardian, Don't trust your phone, don't trust your laptop - this is the reality that Snowden has shown us;

Edward Snowden's astute revelations show that no electronic communications device - from hard disks to sim cards - is trustworthy,
<http://www.theguardian.com/commentisfree/2015/mar/08/edward-snowden-trust-phone-laptop-sim-cards> DOA: 3-20-15

But a few recent revelations suggest that we may now be getting down to bedrock. Two concern the consummate hacking capabilities of the NSA and its overseas franchises. The first - which came not from Snowden but from Kaspersky, a computer security firm - showed that for at least 14 years a unit in the NSA had succeeded in infecting the firmware that controls hard disk drives with malicious software that is able to persist even through reformatting of the disks. Firmware is computer code embedded in a read-only silicon chip. It's what transforms a disk from a paperweight into a storage device. The hack is significant: the Kaspersky researchers who uncovered this said its ability to subvert hard-drive firmware

"surpasses anything else" they had ever seen. Being able to compromise firmware gives an attacker total control of the system in a way that is stealthy and lasting, even through software updates. Which means that the unsuspecting victim can never get rid of it. If you think this has nothing to do with you, **the compromised drives were manufactured by most of the leading companies in the disk-drive business, including Western Digital, Seagate, Toshiba, IBM, Micron and Samsung.** Check your laptop specifications to see which one of these companies made the drive. **The second revelation**, last month, **came from a GCHQ presentation provided by Snowden and reported in online publication the Intercept. Documents showed that a joint NSA/GCHQ team had hacked into the internal computer network of Gemalto, the world's largest manufacturer of sim cards, stealing, in the process, encryption keys used to protect the privacy of mobile communications internationally.**

NSA hacking for surveillance undermines network security, leaving the US vulnerable to cyber attack

National Journal, April 29, 2014, [http://www.nationaljournal.com/daily/the-nsa-isn't-just-spying-on-us-it's-also-undermining-internet-security-20140429](http://www.nationaljournal.com/daily/the-nsa-isn-t-just-spying-on-us-it-s-also-undermining-internet-security-20140429) DOA: 9-1-14

Bolstering the nation's defenses against hackers has been one of the Obama administration's top goals. **Officials have warned for years that a sophisticated cyberattack could cripple critical infrastructure or allow thieves to make off with the financial information of millions of Americans.** President Obama pushed Congress to enact cybersecurity legislation, and when it didn't, he issued his own executive order in 2013. "The cyber threat to our nation is one of the most serious economic and national security challenges we face," Obama wrote in a 2012 op-ed in Wall Street Journal. **But critics argue that the National Security Agency has actually undermined cybersecurity and made the United States more vulnerable to hackers.**

At its core, the problem is the NSA's dual mission. On one hand, the agency is tasked with securing U.S. networks and information. On the other hand, the agency must gather intelligence on foreign threats to national security. Collecting intelligence often means hacking encrypted communications. That's nothing new for the NSA; the agency traces its roots back to code-breakers deciphering Nazi messages during World War II. **So in many ways, strong Internet security actually makes the NSA's job harder.** "This is an administration that is a vigorous defender of surveillance," said Christopher Soghoian, the head technologist for the American Civil Liberties Union. **"Surveillance at the scale they want requires insecurity."** **The leaks from Edward Snowden have revealed a variety of efforts by the NSA to weaken cybersecurity and hack into networks.** Critics say those programs, while helping NSA spying, have made U.S. networks less secure. According to the leaked documents, **the NSA inserted a so-called back door into at least one encryption standard that was developed by the National Institute of Standards and Technology. The NSA could use that back door to spy on suspected terrorists, but the vulnerability was also available to any other hacker who discovered it.**

NIST, a Commerce Department agency, sets scientific and technical standards that are widely used by both the government and the private sector. The agency has said it would never "deliberately weaken a cryptographic standard," but it remains unclear whether the agency was aware of the back door or whether the NSA tricked NIST into adopting the compromised

standard. NIST is required by law to consult with the NSA for its technical expertise on cybersecurity. **The revelation that NSA somehow got NIST to build a back door into an encryption standard has seriously damaged NIST's reputation with security experts.** “NIST is operating with a trust deficit right now,” Soghoian said. “Anything that NIST has touched is now tainted.” **It's a particularly bad time for NIST to have lost the support of the cybersecurity community. In his executive order,** Obama tasked NIST with drafting the cybersecurity guidelines for critical infrastructure such as power plants and phone companies. Because it’s an executive order instead of a law, the cybersecurity standards are entirely voluntary, and the U.S. government will have to convince the private sector to comply. **The Snowden leaks weren't the first to indicate that the NSA is involved in exploiting commercial security.** According to a 2012 New York Times report, the NSA developed a worm, dubbed “Stuxnet,” to cripple Iranian nuclear centrifuges. But the worm, which exploited four previously unknown flaws in Microsoft Windows, escaped the Iranian nuclear plant and quickly began damaging computers around the world. The NSA and Israeli officials have also been tied to “Flame,” a virus that impersonated a Microsoft update to spy on Iranian computers. Vanee Vines, an NSA spokeswoman, said the U.S. government “is as concerned as the public is with the security of these products.” “The United States pursues its intelligence mission with care to ensure that innocent users of those same technologies are not affected,” she said. According to Vines, the NSA relies on the same encryption standards it recommends to the public to protect its own classified networks. “We do not make recommendations that we cannot stand behind for protecting national security systems and data,” she said. “The activity of NSA in setting standards has made the Internet a far safer place to communicate and do business.” But due to concern over the NSA damaging Internet security, the president’s review group on surveillance issues recommended that the U.S. government promise not to “in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption.” **Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible,** the group wrote in its report, which was released in December. “For the entire system to work, encryption software itself must be trustworthy.” In response to the report, the administration adopted a new policy on whether the NSA can exploit “zero-days”—vulnerabilities that haven’t been discovered by anyone else yet. According to the White House, there is a “bias” toward publicly disclosing flaws in security unless “there is a clear national security or law enforcement need.” In a blog post Monday, Michael Daniel, the White House’s cybersecurity coordinator, said that disclosing security flaws “usually makes sense.” “Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest,” he said. But Daniel added that, in some cases, disclosing a vulnerability means that the U.S. would “forego an opportunity to collect crucial intelligence that could thwart a terrorist attack, stop the theft of our nation’s intellectual property, or even discover more dangerous vulnerabilities.” He said that the government weighs a variety of factors, such as the risk of leaving the vulnerability un-patched, the likelihood that anyone else would discover it, and how important the potential intelligence is. **But privacy advocates and many business groups are still uncomfortable with the U.S. keeping security flaws secret. And many don't trust that the NSA will only exploit the vulnerabilities with the most potential for intelligence and least opportunity for other hackers.** **The surveillance bureaucracy really doesn't have a lot of self-imposed limits.** **They want to get everything,** said Ed Black, the CEO of the Computer & Communications Industry Association, which represents companies including Google, Microsoft, Yahoo, and Sprint. “Now I think people dealing with that bureaucracy have to understand they can’t take

anything for granted." Most computer networks are run by private companies, and the government must work closely with the private sector to improve cybersecurity. But companies have become reluctant to share security information with the U.S. government, fearing the NSA could use any information to hack into their systems.

NSA has been working on the Bullrun program to crack encryption

David Sanger, April 12, 2014, Obama lets N.S.A. exploit online security flaws, officials say, <http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html> DOA: 3-21-15

At the center of that technology are the kinds of hidden gaps in the Internet - almost always created by mistake or oversight - that Heartbleed created. There is no evidence that the N.S.A. had any role in creating Heartbleed, or even that it made use of it. When the White House denied prior knowledge of Heartbleed on Friday afternoon, it appeared to be the first time that the N.S.A. had ever said whether a particular flaw in the Internet was - or was not - in the secret library it keeps at Fort Meade, Md., the headquarters of the agency and Cyber Command. But documents released by Edward J. Snowden, the former N.S.A. contractor, make it clear that two years before Heartbleed became known, the N.S.A. was looking at ways to accomplish exactly what the flaw did by accident. A program code-named Bullrun was part of an effort to crack or circumvent encryption on the web.

NSA weakening encryption standards

Teri Robinson, SC Magazine, July 2014, OTI report exposes economic costs of NSA spying, <http://www.scmagazine.com/oti-report-exposes-economic-costs-of-nsa-spying/article/363660/> DOA: 3-21-15

And, the study noted, by weakening key **encryption** standards, allegedly inserting **surveillance** backdoors into "widely used hardware and software products," being slow to report software security vulnerabilities and participating in a "variety of offensive hacking operations," the NSA has roundly damaged internet security. To mitigate the economic and foreign policy damage caused by NSA surveillance activities, OTI made a number of recommendations, including "strengthening privacy protections for both Americans and non-Americans" and "providing for increased transparency around government surveillance, both from the government and companies." The report also noted that the U.S. should take steps to restore trust in cryptography standards through the National Institute of Standards and Technology. The U.S. government must not "undermine cybersecurity" by putting surveillance backdoors into tech products and should commit to eliminating vulnerabilities rather than stockpiling them.

Government can crack encryption now

Bloomberg, October 2, 2014, Apple's encryption will slow not stop snooping by cops and spies, <http://www.bloomberg.com/news/articles/2014-10-02/apple-s-encryption-will-slow-not-stop-cops-and-spies> DOA: 3-20-15

Those assertions "are wildly exaggerated" because police can still obtain evidence through traditional court warrants while revelations about government spying show the National Security Agency (NSA) can break or bypass encryption for terrorism investigations, said Jonathan Turley, a constitutional-law professor at The George Washington University Law School. "Citizens should not assume that these encryption devices will necessarily prevent government from intercepting communications," Turley said in a phone interview. "If history is any guide, the government will find a way to penetrate these devices."

NSA working to weaken encryption

Der Spiegel, December 28, 2014, Inside the NSA's War on Internet Security, <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html> DOA: 12-28-14

But how do the Five-Eyes agencies manage to break all these encryption standards and systems? The short answer is: They use every means available. One method is consciously weakening the cryptographic standards that are used to implement the respective systems. Documents seen by SPIEGEL show that NSA agents travel to the meetings of the Internet Engineering Task Force (IETF), an organization that develops such standards, to gather information but presumably also to influence the discussions there. "New session policy extensions may improve our ability to passively target two sided communications," says a brief write-up of an IETF meeting in San Diego on an NSA-internal Wiki. This process of weakening encryption standards has been going on for some time. A classification guide, a document that explains how to classify certain types of secret information, labels "the fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable" as Top Secret. Cryptographic systems actively weakened this way or faulty to begin with are then exploited using supercomputers. The NSA maintains a system called Longhaul, an "end-to-end attack orchestration and key recovery service for Data Network Cipher and Data Network Session Cipher traffic." Basically, Longhaul is the place where the NSA looks for ways to break encryption. According to an NSA document, it uses facilities at the Tordella Supercomputer Building at Fort Meade, Maryland, and Oak Ridge Data Center in Oak Ridge, Tennessee. It can pass decrypted data to systems such as Turmoil -- a part of the secret network the NSA operates throughout the world, used to siphon off data. The cover term for the development of these capabilities is Valentsurf. A similar program called Gallantwave is meant

to "break tunnel and session ciphers." In other cases, the spies use their infrastructure to steal cryptographic keys from the configuration files found on Internet routers. A repository called Discoroute contains "router configuration data from passive and active collection" one document states. Active here means hacking or otherwise infiltrating computers, passive refers to collecting data flowing through the Internet with secret NSA-operated computers. An important part of the Five Eyes' efforts to break encryption on the Internet is the gathering of vast amounts of data. For example, they collect so-called SSL handshakes -- that is, the first exchanges between two computers beginning an SSL connection. A combination of metadata about the connections and metadata from the encryption protocols then help to break the keys which in turn allow reading or recording the now decrypted traffic. If all else fails, the NSA and its allies resort to brute force: They hack their target's computers or Internet routers to get to the secret encryption -- or they intercept computers on the way to their targets, open them and insert spy gear before they even reach their destination, a process they call interdiction.

International Modeling

Surveillance backdoors weaken security and are a terrible model for other governments

John Shinal, March 17, 2015, USA Today, At SXSW, unlikely allies in privacy-law fight,
<http://www.pressreader.com/usa/usa-today-international-edition/20150318/281762742738887/TextView DOA: 3-21-15>

Those concerns were heightened in January, after Obama, alongside U.K. Prime Minister David Cameron, said law enforcement and intelligence agencies should not be locked out of encrypted messages. The president's remarks came after Apple, Google and other tech giants -- stung by criticism of their cooperation with the FBI and NSA -- built stronger **encryption** technology into their latest smartphone software. The problem with backdoors -- that is, a way for governments to use surveillance -- is that they weaken encryption technology. "Any attempt to weaken encryption via a backdoor will make it easier for bad actors to get in," says David Campbell, chief security officer of SendGrid, a Boulder, Colo.-based security software start-up. "It's a huge mistake." It also sets a bad precedent for other governments. "Our government has asked companies to give them a backdoor," Farenthold says. "But what if China and other countries ask for it?" also? Earlier this year, China did exactly that when they drafted a new anti-terror law asking for its own backdoor -- a move Obama later criticized.

Cyber Security Advantage Links

Ron Wyden, December 18, 2014, Wyden, D-Ore., is a member of the Senate Intelligence Committee, Best defense against massive data theft, With hackers running rampant, why would we poke holes in data security?

<http://www.latimes.com/opinion/op-ed/la-oe-1215-wyden-backdoor-for-cell-phones-20141215-story.html> DOA: 3-21-15

Hardly a week goes by without a new report of some massive data theft that has put financial information, trade secrets or government records into the hands of computer hackers. The best defense against these attacks is clear: strong data encryption and more secure technology systems. The leaders of U.S. intelligence agencies hold a different view. Most prominently, James Comey, the FBI director, is lobbying Congress to require that electronics manufacturers create intentional security holes - so-called back doors - that would enable the government to access data on every American's cellphone and computer, even if it is protected by strong encryption. **Unfortunately, there are no magic keys that can be used only by good guys for legitimate reasons. There is only strong security or weak security.** Americans are demanding strong security for their personal data. Comey and others are suggesting that security features shouldn't be too strong, because this could interfere with surveillance conducted for law enforcement or intelligence purposes. The problem with this logic is that **building a back door into every cellphone, tablet, or laptop means deliberately creating weaknesses that hackers and foreign governments can exploit. Mandating back doors also removes the incentive for companies to develop more secure products at the time people need them most;** if you're building a wall with a hole in it, how much are you going to invest in locks and barbed wire? What these officials are proposing would be bad for personal data security and bad for business and must be opposed by Congress.

Recent security issues related to weak encryption demonstrate that backdoors weaken cyber security

Craig Timberg, March 4, 2015, Washington Post, 'FREAK' flaw leaves a gaping security hole, http://www.stltoday.com/business/local/the-freak-aw-leaves-a-gaping-security-hole/article_228db9de-7ebc-51b4-bada-8d1f30f4b147.html DOA: 5-3-15

Technology companies are scrambling to fix a major security flaw that for more than a decade left users of Apple and Google devices vulnerable to hacking when they visited millions of supposedly secure Web sites, including Whitehouse.gov, NSA.gov and FBI.gov. **The flaw resulted from a former U.S. government policy that forbade the export of strong encryption and required that weaker "export grade" products be shipped to customers in other countries,** say the researchers who discovered the problem. **These restrictions were lifted in the late 1990s, but the weaker encryption got baked into widely used software that proliferated around the world and back into the United States, apparently unnoticed until this year.** Researchers discovered in recent weeks that they could force browsers to use the weaker encryption and then crack it over the course of just a few hours. Once cracked, hackers

could steal passwords and other personal information and potentially launch a broader attack on the Web sites themselves by taking over elements on a page, such as a Facebook "Like" button. The problem illuminates the danger of unintended security consequences at a time when top U.S. officials, frustrated by increasingly strong forms of encryption on smartphones, have called for technology companies to provide "doors" into systems to protect the ability of law enforcement and intelligence agencies to conduct surveillance. Matthew D. Green, a Johns Hopkins cryptographer who helped investigate the encryption flaw, said any requirement to weaken security adds complexity that hackers can exploit. "You're going to add gasoline onto a fire," he said. "When we say this is going to make things weaker, we're saying this for a reason." Christopher Soghoian, principal technologist for the ACLU, said: "You cannot have a secure and an insecure mode at the same time. . . . What we've seen is that those flaws will ultimately impact all users." The existence of the problem with export-grade encryption amazed the researchers, who have dubbed the flaw "FREAK" for Factoring attack on RSA-EXPORT Keys. The export-grade encryption had 512 bits, the maximum allowed under U.S. restrictions designed to limit trade in military technologies in the 1990s, during an era often called "The Crypto Wars" because of pitched political battles over deploying cryptographic algorithms that even advanced government computers had trouble cracking. But 512-bit cryptography has been considered unacceptably weak for more than a decade. Even experts thought it had disappeared.

Encryption cracking undermines Internet security

Karin Lillington, January 22, 2015, Irish Times, World Without Data Encryption unimaginable, <http://www.highbeam.com/doc/1P2-37591772.html> DOA: 2-21-15

If the national legislatures of the United Kingdom and United States decide their leaders are right, and laws are passed to cripple encryption and permit other forms of mass surveillance, the world - especially the business world - will become a very strange, more vulnerable and difficult-to-regulate place. UK prime minister David Cameron's suggestion last week that all digital encryption in Britain be maimed by supplying back doors for security organisations, and President Barack Obama's dovetailing proposals for new cybersecurity laws, suggest national politics remain disconnected from the realities of technology, the internet, business and, for that matter, security. Liberal Democrats accused Cameron of being "technologically illiterate" for proposing new online data surveillance legislation to ensure law enforcement would have access to all encrypted data. Cameron said such legislation would guarantee there would be "no means of communication" that "we cannot read". But encryption becomes meaningless when there's a master skeleton key that can unlock it, allowing back-door access to the data. That master key is a substantial, persistent, crippling risk. What if the key is leaked? What if it is hacked? If such a key exists it will immediately be a hacker target.

Private companies adopting encryption to protect privacy

Teri Robinson, March 2015, SC Magazine, Greenwald says Snowden invoked changes toward privacy, <http://www.scmagazine.com/companies-and-private-citizens-making-changes-in-privacy-post-snowden/article/401938/> DOA: 3-21-15

Although data security and privacy legislation hasn't evolved yet, "there have been extreme changes" in privacy and security itself in the wake of the Edward Snowden documents , Glen Greenwald, the journalist who worked with Snowden to release information on the NSA mass surveillance program, told attendees at the International Association of Privacy Professionals (IAPP) Privacy Summit in Washington Thursday. In fact, Greenwald said prospective laws are "the least interesting" part of the equation, noting that Snowden's revelations helped raise awareness among individuals that their privacy was being compromised by government. And, he noted that some companies, such as Apple and Google, are pushing back against government intrusion/incursion by advocating for encryption - encryption, said Greenwald, "is a barrier to U.S. government spying - and showing less willingness to collaborate with government to share information on their customers with government agencies. That pushback has prompted "vituperative" comments by government and law enforcement that he said are "usually reserved for journalists and activists," implying that those companies are "friends of the terrorists" or are "aiders and abettors of terrorists." Demonizing them, he said, is an attempt to push them back into the more collaborative relationship technology companies have had with government in the past. Many companies actively worked with the NSA, offering "what the law required them to do but also beyond" those requirements. Earlier relationships with the NSA were beneficial, or at least came at no cost, to those companies. But now that kind of cooperation can cost them in terms of reputation - and business.

Breaking Encryption Undermines Cyber Security

PC World, 10, 1, 13, <http://www.pcworld.com/article/2051240/nsa-encryptiondefeating-efforts-will-backfire-privacy-advocates-say.html> NSA encryption-defeating efforts will backfire, privacy advocates say Grant Gross

The U.S. National Security Agency's efforts to defeat encryption will backfire by eroding trust in U.S.-based Internet services and in the agency's own efforts to aid U.S. companies with cybersecurity, a group of privacy advocates said Tuesday.

Many companies will see the NSA's dual roles of code breaking and helping U.S. companies with cybersecurity as clashing, following news reports of the agency's efforts to defeat online encryption, said Kevin Bankston, director of the Free Expression Project at the Center for Democracy and Technology.

The NSA has defeated encryption through a variety of means, including through reported backdoors in online services and covert compromises in encryption standards, according to news reports last month. Those reports followed revelations in June by former NSA contractor Edward Snowden about massive data-collection programs at the agency. The NSA says the data collection efforts, which include monitoring U.S. phones and overseas Internet communications, are necessary to counter the threat of terrorism.

For U.S. technology companies, it is "terribly debilitating and undermining to have the rest of world thinking there have been backdoors built into their systems to help the U.S. government," said Alan Davidson, a visiting scholar at the Massachusetts Institute of Technology and former public policy director at Google.

The NSA's encryption-defeating efforts will also hurt the agency, Davidson said at an Information Technology and Innovation Foundation discussion.

Many U.S. companies have asked the NSA for cybersecurity assistance in recent years, but "you'd be crazy to ask for that kind of help now," Davidson said. "You want to have the best mathematicians and security experts in the world to help you secure your systems. But when it's the same people who ... want to compromise the security of your system, that's probably going to dissuade you a bit."

The NSA's efforts will prompt other governments to require that their citizens' data be stored within their borders and will lead to efforts to route Internet traffic around the U.S., Bankston said. The NSA's efforts will lead to compromised intelligence-gathering capabilities in the long run as other countries seek to circumvent U.S. services and networks, he said.

"They could very easily kill the goose that laid the golden egg here," he said. "[The NSA has] been placed in a privileged position here because so much data is stored in the U.S., so much data transits the U.S. However, to the extent that it is not clear that we have strong legal standards governing the access to data ... we're going to see that data go away."

The NSA's encryption-defeating efforts will also lower trust in security standards developed through the U.S. National Institute of Standards and Technology (NIST) because of the reports that the NIST helped the NSA tamper with encryption standards, panelists at the encryption forum said.

A NIST spokesman wasn't available for comment Tuesday because of a partial government shutdown, but the agency has denied that it helped build backdoors into encryption standards.

Coytly weakening encryption standards would be "cheating in the worst way," Bankston said.

An NSA spokeswoman defended the agency's work on security standards.

"NSA is responsible for setting the security standards for systems carrying the nation's most sensitive and classified information," she said in an email. "We use the cryptography and standards that we recommend, and we recommend the cryptography and standards that we use. We do not make recommendations that we cannot stand behind for protecting national security systems and data. The activity of NSA in setting standards has made the Internet a safer place to communicate and do business."

The 2002 Federal Information Security Management Act (FISMA) requires the NIST to work with the NSA on cybersecurity standards, but little is known about how the two agencies have cooperated, said Amie Stepanovich, director of the Domestic Surveillance Project at the Electronic Privacy Information Center (EPIC). Stepanovich called on lawmakers to require more transparency in the relationship between the two agencies.

Grant Gross covers technology and telecom policy in the U.S. government for The IDG News Service.

Economy Advantage

Internet surveillance costs US industry billions

Teri Robinson, SC Magazine, July 2014, OTI report exposes economic costs of NSA spying,
<http://www.scmagazine.com/oti-report-exposes-economic-costs-of-nsa-spying/article/363660/>
DOA: 3-21-15

A report from New America OTI found that the NSA surveillance program has had a chilling effect on U.S. commerce and foreign policy. In the 13 months since Edward Snowden leaked details revealing the extent of National Security Agency (NSA) spying, American companies are paying an economic price here and abroad for the vast, and questionable, surveillance program, according to a report from the New American Open Technology Institute (OTI). Despite the outrage expressed at Snowden's revelations, the national discourse has not moved passed a debate the tradeoffs between national security and individual privacy despite, as OTI's "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Security" revealed, "the NSA's actions have already begun to, and will continue to, cause significant damage to the interests of the United States and the global Internet community." As one article of proof, the study cited an April 2014 Harris Poll in which "26 percent of respondents indicated that they are now doing less online shopping and banking since learning the extent of government surveillance programs." Noting that three other significant studies, the President's Review Group on Intelligence and Communications Technologies, the Privacy and Civil Liberties Oversight Board, and the New America Foundation's International Security Program, focus on the national security/privacy conundrum, the OTI study seeks to "quantify and categorize the costs of the NSA surveillance programs." The organization divides those costs into four main groups - direct economic costs to U.S. businesses, potential costs to U.S. businesses and to the openness of the internet, costs to U.S. foreign policy and those to cybersecurity. "The economic cost issues are not just a PR problem that will blow over," Katharine Kendrick, policy associate at the Center for Business and Human Rights at NYU Stern School of Business, told SCMagazine.com in a Wednesday interview. In an earlier statement, Kendrick had commended the report for highlighting "the real costs of NSA surveillance to American businesses," making clear that "NSA practices have caused real damages to the U.S. tech industry, and have fueled other governments to pursue policies that are bad for both U.S. businesses and for human rights." In Wednesday's interview, Kendrick, who focuses on free expression and privacy challenges facing tech companies, noted that NSA spying and implications that U.S. companies had been somehow complicit by filling data requests and offering up products that were tainted with backdoors and vulnerabilities that made surveillance easier had "caused a fundamental breach of trust in an industry where trust is a value proposition." Regaining trust will likely "take a long time," she said. In fact, U.S. companies have seen both declining sales overseas as well as lost business opportunities, the report said, noting that foreign companies are using the scandal to hawk products that they claim "protect users from NSA spying," thereby gaining a competitive advantage over their American counterparts. The cloud computing industry could take a tremendous hit, losing billions of dollars in the next five years. Both U.S. businesses and the nation's economy will likely suffer in the long term as foreign

governments impose data localization requirements or stronger data protection regulations.
"These proposals could also force changes to the architecture of the global network itself, threatening free expression and privacy if they are implemented," the report said.

Internet surveillance means cloud providers go overseas in order to promise data protection

Teri Robinson, March 2015, SC Magazine, Greenwald says Snowden invoked changes toward privacy, <http://www.scmagazine.com/companies-and-private-citizens-making-changes-in-privacy-post-snowden/article/401938/> DOA: 3-21-15

Many companies actively worked with the NSA, offering "what the law required them to do but also beyond" those requirements. Earlier relationships with the NSA were beneficial, or at least came at no cost, to those companies. But now that kind of cooperation can cost them in terms of reputation - and business. "Companies are petrified that they will lose a whole generation" who get wooed by companies from other countries like Brazil that assure them that their data won't be shared with government. That was a sentiment echoed later by a panelist in the session "Search Warrants vs. Privacy Laws: Can They Live Together?" who used the example of cloud users flocking to non-U.S. companies because data would be outside the reach of the U.S. government. Noting that the NSA's motto is "Collect It All," Greenwald urged the audience to take steps to secure the internet so it doesn't become a "tool" for monitoring, coercion and surveillance.

Encryption essential to the security of business data

Karin Lillington, January 22, 2015, Irish Times, World Without Data Encryption unimaginable, <http://www.highbeam.com/doc/1P2-37591772.html> DOA: 2-21-15

Even as Cameron implied encryption made society more vulnerable because terrorists use it to encode communications, **a leaked 2009 report from the US National Intelligence Council** (which answers directly to the head of intelligence in the US) undermined his "security equals surveillance" bombast. The report, again from Snowden, **stated unequivocally that encryption is essential to business and consumer security, offering the "best defence" for private data.** Encryption is no longer some fancy exotic feature. **It's as mundane as can be, an embedded feature in business services and applications. Most day-to-day business operations, from ordinary communications using a Gmail account to an online purchase from a website, the automated backing up of corporate data or the processing of credit card transactions, involve the routine use of encryption.**

Weakening encryption for US businesses will force business and capital overseas

Karlin Lillington, January 22, 2015, Irish Times, World Without Data Encryption unimaginable, <http://www.highbeam.com/doc/1P2-37591772.html> DOA: 2-21-15

We are in a world where cryptocurrencies such as bitcoin, created using the same basic idea as encryption for data communications, can be invented anonymously and become internationally significant. It's idiotic to believe that new encryption products won't likewise be created for communications, even as economies deprived of adequate mainstream encryption will suffer and grow even more vulnerable to hacker attacks, cyberterrorism and espionage. One imagines a potential intellectual and business capital shift to other, wiser nations. How would large multinationals react, with their international data and cloud centres? What would be the response of, say, US-based banks forced to use weakened encryption? It is an almost unimaginable scenario.

Companies relying on encryption to prevent the loss of billions of dollars in business

Omar El Akkad, January 19, 2015 Technology firms are caught between the need for better encryption against hackers and politicians' calls for surveillance measures, Globe & Mail, <http://penny2.theglobeandmail.com/servlet/ArticleNews/story/gam/20150119/RBIBSOFTWAREENCRYPTION> DOA: 3-21-15

Encryption is, at its most basic level, a means of keeping information secret using very large numbers. Just as a 15-digit PIN is harder to guess than a four-digit PIN, high-grade encryption algorithms that manipulate larger numbers are usually harder to break. As such, all things being equal, encryption is not only a fairly effective means of keeping data private, its effectiveness can also be mathematically measured. But ever since the Edward Snowden leaks revealed widespread claims of authorized and unauthorized government surveillance of many of the world's most popular digital services and social networks, the technology giants responsible for those services have taken great pains to improve their encryption standards. (The motivation for doing so is, primarily, financial - companies such as Google, Microsoft and Apple stand to lose billions if enterprise customers such as banks and other large corporations no longer trust their systems to keep sensitive information private.)

Surveillance undermines the ability of companies to sell their products abroad

Ron Wyden, December 18, 2014, Wyden, D-Ore., is a member of the Senate Intelligence Committee, Best defense against massive data theft, With hackers running rampant, why would we poke holes in data security?

<http://www.latimes.com/opinion/op-ed/la-oe-1215-wyden-backdoor-for-cell-phones-20141215-story.html> DOA: 3-21-15

In Silicon Valley several weeks ago I convened a roundtable of executives from America's most innovative tech companies. They made it clear that widespread availability of data encryption technology is what consumers are demanding. Most Americans accept that there are times their government needs to rely on clandestine methods of intelligence gathering to protect national security and ensure public safety. But they also expect government agencies and officials to operate within the boundaries of the law, and they now know how egregiously intelligence agencies abused their trust. This breach of trust is also hurting U.S. technology companies' bottom line, particularly when trying to sell services and devices in foreign markets. The president's own surveillance review group noted that concern about U.S. surveillance policies "can directly reduce the market share of U.S. companies." One industry estimate suggests that lost market share will cost just the U.S. cloud computing sector \$21 billion to \$35 billion over the next three years.

Encryption cracking undermines US Internet companies

David Sanger, April 12, 2014, Obama lets N.S.A. exploit online security flaws, officials say, <http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html> DOA: 3-21-15

One recommendation urged the N.S.A. to get out of the business of weakening commercial encryption systems or trying to build in "back doors" that would make it far easier for the agency to crack the communications of America's adversaries. Tempting as it was to create easy ways to break codes - the reason the N.S.A. was established by President Harry S. Truman 62 years ago - the committee concluded that the practice would undercut trust in American software and hardware products. In recent months, Silicon Valley companies have urged the United States to abandon such practices, while Germany and Brazil, among other nations, have said they are considering shunning American-made equipment and software.

Internet surveillance is encouraging European companies to move their data off of US servers

Kate O'Flaherty, September 2014, SC Magazine, How safe is cloud - really?,
<http://www.scmagazine.com/how-safe-is-cloud--really/article/366352/>
DOA: 3-25-15

Revelations of government surveillance are fueling a paranoia that isn't going to subside. Kate O'Flaherty asks whether firms should be afraid of adopting cloud? Cloud technology has improved dramatically but its security implications are once again under the spotlight. Is cloud allowing firms to keep their data safer, or exposing them to greater risk? Recent revelations from National Security Agency (NSA) whistleblower Edward Snowden made companies aware that communications - such as those passing through cloud technology - could be subject to government surveillance. This is breeding paranoia and spurring many European firms to demand that their data storage be removed from servers hosted on U.S. soil. These fears are supported by a recent report which concludes that rising levels of government surveillance is leading firms away from cloud computing. According to the report, the presence of automated hacking tools means that even a small number of improperly secured resources are certain to give hackers free reign on the network - and access to customers' private data - within minutes of an incursion. There does not seem to be a fix-all solution - although some experts suggest the type of cloud used makes a difference. After all, a private cloud is likely to be more secure than a public one. On top of this, countries within the European Union (EU) are considering following the example of the French and adopting national clouds in the struggle to ensure data is protected. Even with such measures in place, resisting government surveillance is futile, experts say. Whether private, national or public clouds are used, data will still be available to government spies - and criminals - if they really want it. Currently, most cloud service providers are U.S.-based, which is leading some to roll out European-wide data centers, says Alvaro Hoyos, director, risk and compliance at San Francisco-based OneLogin, which provides single sign-on and identity management for cloud-based applications.

Businesses can't sell products that have a back door to the NSA

Center for Democracy & Technology, November 10, 2014, Issue Brief: a "Backdoor to Encryption for Government Surveillance," <https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/> DOA: 3-15-15

Consumers outside of the US may be much less inclined to purchase American tech products that facilitate government surveillance. Consider, for example, the difficulty US companies would have selling smartphones or network servers in the EU that are built to enable easy access for the NSA. As a technical matter, it is difficult and expensive to both build a backdoor security vulnerability and then defend that vulnerability against unauthorized use. This burden would be heaviest on small businesses and innovators of new communications services, which may create a disincentive to encrypt their products and reduce the overall security of users.

Privacy Advantage

Breaking encryption threatens medical privacy

Health Care Renewal, September 6, 2013

N.S.A. Able to Foil Basic Safeguards of Privacy on Web, or, If You Contracted V.D. From That Sexy Prostitute At That Vegas Conference, You Better Not Tell Your Doctor About It

LENGTH: 853 words

There's already a major issue with privacy and protection of medical records in electronic form.

Now this from the New York Times:

N.S.A. Able to Foil Basic Safeguards of Privacy on Web By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE September 5, 2013

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show. But don't worry, your electronic medical records are secure, and will NEVER be used for political purposes by your adversaries...

Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own 'back door' in all encryption, it set out to accomplish the same goal by stealth. The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated. At least we may have gotten faster PC's as a side result of the research that supported these efforts.

... the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.

Some of the agency's most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer[4], or SSL; virtual private networks[5], or VPNs; and the protection used on fourth-generation, or 4G, smartphones. Many Americans, often without realizing it, rely on such protection every time they send an e-mail, buy something online, consult with colleagues via their company's computer network, or use a phone or a tablet on a 4G

network. Might as well just send them a copy of all your communications to spare them the effort...

...Ladar Levison, the founder of Lavabit, wrote a public letter[6] to his disappointed customers, offering an ominous warning. 'Without Congressional action or a strong judicial precedent,' he wrote, 'I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.' Hey, how about let's ALL have our medical records stored by health IT companies providing ASP (Application service provider, [http://en.wikipedia.org/wiki/Application_service_provider\[7\]](http://en.wikipedia.org/wiki/Application_service_provider[7])) offsite EHR hosting services to hospitals and clinics...

From the site "techdirt.com":

NSA back door encryption hacking violates privacy

New York Times Editorial Board, 9-21, 13, "Close the NSA's Back Doors,"
http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=1&

In 2006, a federal agency, the National Institute of Standards and Technology, helped build an international encryption system to help countries and industries fend off computer hacking and theft. Unbeknown to the many users of the system, a different government arm, the National Security Agency, secretly inserted a "back door" into the system that allowed federal spies to crack open any data that was encoded using its technology.

Documents leaked by Edward Snowden, the former N.S.A. contractor, make clear that the agency has never met an encryption system that it has not tried to penetrate. And it frequently tries to take the easy way out. Because modern cryptography can be so hard to break, even using the brute force of the agency's powerful supercomputers, the agency prefers to collaborate with big software companies and cipher authors, getting hidden access built right into their systems.

The New York Times, The Guardian and ProPublica recently reported that the agency now has access to the codes that protect commerce and banking systems, trade secrets and medical records, and everyone's e-mail and Internet chat messages, including virtual private networks. In some cases, the agency pressured companies to give it access; as The Guardian reported earlier this year, Microsoft provided access to Hotmail, Outlook.com, SkyDrive and Skype. According to some of the Snowden documents given to Der Spiegel, the N.S.A. also has access to the encryption protecting data on iPhones, Android and BlackBerry phones.

These back doors and special access routes are a terrible idea, another example of the intelligence community's overreach. Companies and individuals are increasingly putting their most confidential data on cloud storage services, and need to rely on assurances their data will be secure. Knowing that encryption has been deliberately weakened will undermine confidence in these systems and interfere with commerce.

The back doors also strip away the expectations of privacy that individuals, businesses and governments have in ordinary communications. If back doors are built into systems by the

N.S.A., who is to say that other countries' spy agencies — or hackers, pirates and terrorists — won't discover and exploit them?

The government can get a warrant and break into the communications or data of any individual or company suspected of breaking the law. But crippling everyone's ability to use encryption is going too far, just as the N.S.A. has exceeded its boundaries in collecting everyone's phone records rather than limiting its focus to actual suspects.

Representative Rush Holt, Democrat of New Jersey, has introduced a bill that would, among other provisions, bar the government from requiring software makers to insert built-in ways to bypass encryption. It deserves full Congressional support. In the meantime, several Internet companies, including Google and Facebook, are building encryption systems that will be much more difficult for the N.S.A. to penetrate, forced to assure their customers that they are not a secret partner with the dark side of their own government.

Frontlines to Cybersecurity Contention

FT: No Real Threat

Escalates to nuclear war

Fritz, Bond University IR masters, 2009

(Jason, “Hacking Nuclear Command and Control”, July,
http://www.icnnd.org/latest/research/Jason_Fritz_Hacking_NC2.pdf, ldg)

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists' capabilities, strategies, and tactics. If access to command and control centres is obtained, terrorists could fake or actually cause one nuclear-armed state to attack another, thus provoking a nuclear response from another nuclear power.

This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves. This would also act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a relatively low cost. Continuing difficulties in developing computer tracking technologies which could trace the identity of intruders, and difficulties in establishing an internationally agreed upon legal framework to guide responses to computer network operations, point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is particularly relevant to reducing the hair trigger posture of existing nuclear arsenals. All computers which are connected to the internet are susceptible to infiltration and remote control. Computers which operate on a closed network may also be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, and maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. Information found on the internet may also reveal how to access these closed networks directly. Efforts by militaries to place increasing reliance on computer networks, including experimental technology such as autonomous systems, and their desire to have multiple launch options, such as nuclear triad capability, enables multiple entry points for terrorists. For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task.

There is evidence to suggest multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines. Additionally, the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications through computer network operations in an attempt to engage the system. Should a warhead be launched, damage could be further enhanced through additional computer network operations. By using proxies, multi-layered attacks could be engineered. Terrorists could remotely commandeer computers in China and use them to launch a US nuclear attack against Russia. Thus Russia would believe it was under attack from the US and the US would believe China was responsible. Further, emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted, thereby hindering the disaster relief effort and maximizing destruction. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses.

For example, a nuclear strike between India and Pakistan could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened and be forced to respond quickly. Terrorists could also knock out communications between these states so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response. These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials. A sophisticated and all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.

Impact Extension

It's on par with nuclear war – existential threat
DSB '12

Defense Science Board, a Federal Advisory Committee established to provide independent advice to the Secretary of Defense, "TASK FORCE REPORT:

Resilient Military Systems and the Advanced Cyber Threat," October 10, 2012.
<http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

The benefits to an attacker using cyber exploits are potentially spectacular. Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space. U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed. Military Commanders may rapidly lose trust in the information and ability to control U.S. systems and forces. Once lost, that trust is very difficult to regain.

The impact of a destructive cyber attack on the civilian population would be even greater with no electricity, money, communications, TV, radio, or fuel (electrically pumped). In a short time, food and medicine distribution systems would be ineffective, transportation would fail or become so chaotic as to be useless. Law enforcement, medical staff, and emergency personnel capabilities could be expected to be barely functional in the short term and dysfunctional over sustained periods. If the attack's effects were reversible, damage could be limited to an impact equivalent to a power outage lasting a few days. If an attack's effects cause physical damage to control systems, pumps, engines, generators, controllers, etc., the unavailability of parts and manufacturing capacity could mean months to years are required to rebuild and reestablish basic infrastructure operation.

The DoD should expect cyber attacks to be part of all conflicts in the future, and should not expect competitors to play by our version of the rules, but instead apply their rules (e.g. using surrogates for exploitation and offense operations, sharing IP with local industries for economic gain, etc.).

Based upon the societal dependence on these systems, and the interdependence of the various services and capabilities, the Task Force believes that the integrated impact of a cyber attack has the potential of existential consequence. While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same.

FT: Deterrence

Cyber-attacks hollow out US deterrence capabilities, encourages aggression and risks nuclear first use

Colby '13

Elbridge, is a principal analyst at CNA, where he focuses on strategic issues and advises a number of U.S. Government entities. He previously served with the Department of Defense on the New START treaty negotiation and ratification effort and as an expert advisor with the Congressional Strategic Posture Commission, “Cyberwar and the Nuclear Option,” June 26, 2013. <http://strategicstudyindia.blogspot.com/2013/06/cyberwar-and-nuclear-option.html>

Thus **a major cyber attack's effect** on our conventional forces **could mean that**, without our nuclear forces in the equilibrium, **the United States might well find itself with no serious riposte to a massive cyber assault, leaving us exposed to coercion or worse.** Thus, while the Task Force wisely advocated for having more discriminate cyber and other non-nuclear options to provide steps on the escalatory ladder, it rightly argued that at the top of that ladder resides the U.S. nuclear deterrent—the ultimate reminder that, even if a major cyber attack could emasculate our conventional forces, our resilient nuclear forces would still pose a devastating threat that would make such an assault patently foolhardy. (The Task Force also rightly advocated ensuring the absolute effectiveness of our nuclear forces even under highly sophisticated cyber assault.) Now these kinds of scenarios might seem fantastically remote—and thankfully they are highly unlikely. But **worst cases can happen**, and what else are our most powerful military forces for, if not for warding off the worst cases? **More likely**, however, **is the danger that adversaries would derive coercive leverage if both we and they know that they have the upper hand on the escalatory ladder.** Advantages at the top of the escalatory ladder can **cast a dark shadow**. For instance, during the 1950s, the United States used its huge advantages at the level of nuclear warfare to try to coerce Maoist China, with at least some success. So, if China or Russia knows that we would never consider using nuclear weapons in response to even a massive cyber attack, then that gives them a strong incentive to try to exploit that advantage—even implicitly—by using cyber as a way to deter and even coerce the United States and our allies. Low-level versions of this problem are apparent today. But what if the United States and China squared off over one of the territorial maritime disputes in the Western Pacific or South China Sea? Or if the United States and Russia faced off over instability in a NATO Baltic state? **The United States does not want to find itself in a situation in which it has no good options to respond to** escalating **cyber attacks**. Perhaps **even worse, it would not want to find itself in a situation in which it felt itself forced into actually considering nuclear options** when it had loudly declared that it would not.

FT: No Capability

**Cyberwarfare threat is real—smaller states/non-state entities—spillover—
serious intrusions are occurring—cyber>traditional weps**

Brecht, former Information Technician in the military, 15

Daniel, holds a graduate Certificate in Information Assurance and a Master of Science in Information Technology, "Cyber Warfare and Cyber Weapons, a Real and Growing Threat", Jan 15 2015, Infosec Institute, resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/

Is a Cyber World War a Concern? A 2013 report by Director of National Intelligence James R. Clapper explained that the possibility of a major cyber attack to US critical infrastructures causing a long-term and widespread disruption of services by major players like Russia and China is remote. However, smaller scale attacks by smaller states or non-state entities seem to be a concern. According to the report, "less advanced but highly motivated actors could access some poorly protected US networks that control core functions, such as power generation, during the next two years, although their ability to leverage that access to cause high-impact, systemic disruptions will probably be limited. At the same time, there is a risk that unsophisticated attacks would have significant outcomes due to unexpected system configurations and mistakes, or that vulnerability at one node might spill over and contaminate other parts of a networked system." This may not come as a surprise to anyone, but any telecommunications infrastructure attack could cause enough harm to generate fear. Every government or corporation entire infrastructure, let alone the public at large, may be at stake. Can digital attacks really have tangible effects? Absolutely. An oil pipeline in Turkey was cyber attacked and exploded in 2008. The pipeline was super-pressurized and alarms were shut off. By hacking security cameras, attackers (allegedly Russian) were able to hide the blast from the control room that, unaware, was unable to respond promptly. Another attack to a German steel company demonstrated how, by simply infiltrating the information systems running the plant, hackers could cause major damage. Although not a single Internet successful attack has been recognized as directed by a foreign terror organization against the United States homeland, there have been instances of intrusions intended to inflict significant harm on the American government or state agency, as well as US businesses. Last November, there was an intrusion into the networks of the Department of the State that led to the unclassified email system shutdown. Carol Morello, the diplomatic correspondent for The Washington Post who covered the affair, noted the activity was related to hacking of White House computers reported a month prior, and to security breaches that occurred at both the U.S. Postal Service and the National Weather Service. Those incidents pointed to Russian hackers as prime suspects; the perpetrators were believed to be working directly for the Russian government. Sony Pictures Entertainment (SPE) is another recent case; its networks were infected in a November 2014 incident. According to the FBI, the occurrence resembled past cyber efforts by North Korea. What makes a cyber warfare attack appealing? Mainly the fact that it can come at little or no cost for the perpetrator. An attacker with great technical capabilities can create disruption by using a single computer wherever he or she is located. While the use of conventional weapons requires expensive manufacturing and physical travel to target locations, cyber attacks can be conducted from anywhere. Traditional weapons have a cost that might be prohibitive for many and are hard to transport (or deliver) in secrecy. In other cases, attacks might require the sacrifice of the offenders. Cyber attacks are quick, can be equally destructive and can definitely be inexpensive to execute. According to Amy Chang, research associate at the Center for a New American Security, "Cyber warfare is a great alternative to conventional weapons. [...] It is cheaper for and far more accessible to these small nation-states. It allows these countries to pull off attacks without as much risk of getting caught and without the repercussions when they are."

Terrorists are preparing for cyber attacks now

Brennan 12 (Lt Colonel John – US Army, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” 15 March 2012, Civilian Research Project; U.S. Army War College)

As Al-Qa’ida and its affiliates and adherents have evolved into much more technically savvy terrorist organizations, their ability to threaten to U. S. National Security has likewise increased. The divergence between American national strategies, laws, and policies that govern counterterrorism (CT) operations within cyberspace has hampered the efforts of U. S. CT professionals to keep pace with the transformation of transnational terrorist organizations into more cyber-enabled threats.

Counterterrorism is defined as, “Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.”² Due to terrorists’ heavy reliance on cyberspace, it is an operational environment which CT professionals must simultaneously dominate, and effectively deny to these shadowy groups in order to defeat them. CT cyber strategies, law, and policies provide the framework through which CT cyber professionals execute their assigned operations.

Of considerable concern is the fact that current U. S. CT cyber policies are not necessarily completely sourced in domestic or international law, and they inhibit American CT professionals from efficiently implementing the very strategies which they are charged to execute. These restrictive and hierarchical CT cyber policies clearly hinder the ability of strategic and operational-level military commanders who are deployed in support of Overseas Contingency Operations (OCO) to manipulate cyberspace to their greatest advantage.

In 2010 General David Petraeus, then Commander of United States Central Command (USCENTCOM) accurately described the degree to which al-Qa’ida was operating with impunity in cyberspace to finance, command, and recruit its forces.³ The tactical and operational commanders subordinate to General Petraeus in Iraq and Afghanistan often lamented that they were permitted to drop two-thousand pound bombs on terrorists’ homes, but were forced to request from USCENTCOM Headquarters, or even the Secretary of Defense, the approval to attack or manipulate terrorists’ computer networks.⁴ This dichotomous situation flies in the face of logic and is caused by a trifurcated divergence between: what is expected of military CT professionals in order kill or capture terrorists; what is permissible under current CT cyber law; and the current policies that actually govern offensive CT operations in cyberspace.

This work will analyze the current threat posed by international terrorist organizations from within cyberspace, as well as the inconsistencies between current national security, CT and cyber strategies, and the laws, and policies that permit CT professionals to disrupt and degrade international terrorist organizations through the use of the internet. The results of this analysis reveal that current cyber-related counterterrorism policies constrain military CT professionals, and that before CT cyber strategies can be effectively implemented, they must be in holistic alignment with cyber policies and existing statutes. Furthermore, this work proffers several recommendations concerning adjustments to current CT cyber policies that are intended to better enable more efficient CT operations, and ultimately prevent future attacks on America and its interests.

The Nature of the Cyber-terror Threat

There is conclusive and irrefutable evidence that terrorist organizations such as al-Qa’ida in Iraq (AQI) not only recruit, propagandize, coordinate attacks, and finance their activities, but these terror organizations are actively seeking the means to initiate casualty-producing kinetic events using the worldwide web as well.⁵ Groups such as the Muslim Hackers Club have developed their own software and tutorials in order to sabotage not only U. S. computer networks, but to also seek to cause the physical destruction of key American infrastructure.⁶ ADM Michael Mullen, then Chairman of the Joint Chiefs of Staff described cyber terrorism as one of two existential threats to U. S. national security, the other being the Russian nuclear threat.⁷ Additionally, the intelligence community (IC) writ large considers cyber attacks as the most prominent, long-term threat to the country.⁸ Deputy Secretary of Defense William J. Lynn III similarly suggests that terrorists are seeking to effectively weaponize cyberspace in order to achieve kinetic effects against key U. S. infrastructure.⁹

Speed matters in stopping potentially calamitous events, and it is of seminal importance as al-Qa’ida and its ilk continue to develop more efficient and effective methods of attack.¹⁰ Current trends indicate that terrorist organizations such as Lashkar e-Tayyibah (LeT) and al-Qa’ida in Iraq (AQI) are investing heavily in the education of select members in the fields of computer and electrical engineering.¹¹ Ayman al-

Zawahiri counseled deceased AQI leader Abu Musab al Zarqawi that half of the battle for Islam should be waged on the internet and he constantly stressed to Zarqawi the importance of digital information operations.¹²

In order to pay for their operations, terrorist groups have begun to resort to various forms of computer-assisted robbery and identity theft. Cybercrime has become so important to financing their operations, that it now surpasses drug trafficking as a source of income to fund their operations.¹³ During their investigation into the 2002 Bali bombing by Jemaah Islamiyah, the Indonesian police discovered that the attack was financed through computer credit card fraud.¹⁴

More disturbing than terror financing, is the implementation of a worldwide recruiting drive, launched by al-Qa'ida in order to co-opt computer and electrical engineers who already possess advanced degrees from elite universities. Before their demise, Al-Qa'ida in the Arabian Peninsula (AQAP) leaders Anwar al Awlaki and Inspire Magazine editor-in-chief Samir Kahn were posting high-tech want ads in their jihadi circular on the internet in order to elicit acts of terror by homegrown western Muslims. The two also posted numerous want-ads to recruit individuals who possessed high-tech degrees.¹⁵ As we shall learn, the lack of an effective U. S. CT Cyber policy prevented the timely interdiction and/or manipulation of the data on this website--action that could have been used to not only thwart AQAP's cyber efforts, but could have been used to create physical vulnerabilities within the organization as well.

The plots that could be hatched by heavily recruited techno-savvy terrorists are especially horrifying. Imagine if you will, the mayhem that could be unleashed by a terrorist, who using the internet, pilots multiple unmanned aircraft armed with explosive, chemical, or biological payloads. A hint of this frightening scenario came to pass when FBI foiled a plot by Rezwan Ferdaus, a young Bangladeshi-American physicist, who was arrested while in the process of developing the means to fly remote-controlled aircraft packed with explosives into the U. S. Capitol and the Pentagon.(Valencia, Milton J. and Ballou, Brian R. 2011, A1) Another terrifying possibility consists of dozens, if not hundreds of improvised explosive devices igniting simultaneously through the instantaneity of the internet. The process of perfecting this method of terrorist attack was proven to be well on its way to fruition, as was evident after the capture of numerous Al-Qa'ida in Iraq (AQI) improvised explosive device (IED) cell members. These individuals were detained while in the possession of hundreds of digital tone multi-frequency (DTMF) boards that were purported to be used to simultaneously initiate multiple IEDs to destroy U. S. and Iraqi security forces.¹⁶

Today these potential threats may seem far-fetched to some, but so did the concept of crashing jet airliners into the World Trade Center and the Pentagon prior to September 11th, 2001. These and other cyber-enabled terror plots are unfortunately far from fiction, as their perpetrators were caught in the acts of planning or executing them. The cyber terror threats which emanate from the various international terrorist organizations around the globe are of a seminal concern to U. S. national decision-makers. Though significant, the task of countering these terrorists' threats within cyberspace is anything but insurmountable, provided that those who are charged with exposing and attacking these networks are given the latitude to act effectively. The concerns of national leaders and their desires to exploit terrorist organizations in cyberspace are clearly evident in the content of numerous past, and current national security strategy documents.

FT: No Blackout

Attacks collapse the grid—critical infrastructure is vulnerable Savenjie 14

Davide and Ethan Howland, senior editors at Industry Dive, "Could terrorists really black out the power grid?", Utility Dive, March 24 2014, www.utilitydive.com/news/could-terrorists-really-black-out-the-power-grid/241192/

The possibility of a terrorist attack knocking out the power grid makes for a good headline, but could it really happen? The U.S. Federal Energy Regulatory Commission (FERC) says yes. If terrorists are ever able to knock out nine of the nation's 55,000 substations, the U.S. power grid could suffer coast-to-coast blackouts lasting 18 months or more, according to leaked excerpts from a FERC report. There are 30 substations in the U.S. that play a critical role in the nation's grid operations, the report said. If any nine of them were taken offline, there could be widespread blackouts for weeks — or far longer. Just because a crippling grid attack is possible, doesn't mean it's going to happen. But terrorist attacks on the power grid don't just make for good headlines — they're already happening. Is the grid vulnerable to terrorist attacks? It's no surprise to see headlines warning that the grid is susceptible to attack. But why all the concern now? Well, it doesn't help that a Pacific Gas & Electric substation that feeds Silicon Valley was shot by snipers last year. And it's not the only such incident. A man tried to take down the power grid in central Arkansas by bringing down several power lines (with a stolen tractor and a passing train) and setting a substation on fire, causing \$2 million worth of damage. These attacks show the grid is vulnerable to terrorism, a finding confirmed by a previously classified report sponsored by the U.S. Department of Homeland Security. Leaked portions of the FERC report paint a dark picture. "Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," a summary of the report reads. Perhaps most disturbingly, the California substation attack, in which snipers destroyed 17 transformers, "demonstrates that it does not require sophistication to do significant damage to the U.S. grid," according to FERC. And it's not just physical attacks. Despite the recent focus on physical security, some say cyberattacks present an even greater threat to the grid. A "sophisticated, targeted cyberattack" could knock out large portions of the U.S. power grid for 9 to 18 months, cybersecurity consultant Joe Weiss told Utility Dive. Such an attack would be "irrecoverable," he said. More than a decade after 9/11, experts believe the U.S. has failed to adequately safeguard critical infrastructure, including grid operations, from cyberattacks. "We've been led down the path to believe that: one, these systems are secure; and two, other countries don't have the capability to effectively attack the U.S. electric grid," Weiss said. "Both of those assumptions are wrong." Why the grid is 'inherently vulnerable' The U.S. electrical grid was not designed with today's complexities in mind — let alone the ability to withstand terrorist attacks. "The power grid is inherently vulnerable because it is spread across hundreds of miles, and many key facilities are unguarded," the report prepared for Homeland Security found. "Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time." Another big reason the grid is vulnerable is that it takes a long time to replace equipment — such as large boilers, turbines and transformers — underpinning the nation's critical infrastructure. It could take months or even years to replace such equipment, according to estimates. And yet this is all old news. Policymakers, security experts and the utility industry have known about the grid security issue for the last 30 years. Amory Lovins, chairman of the Rocky Mountain Institute, wrote in his 1982 book Brittle Power that "a few people could probably black out most of the country." The book surprised people when it came out — citing frequent instances of grid terrorism throughout the 1970s, such as transformer shootings and substation bombings — but the same debate over grid security continues today.

Cascade effect

Plumer 14

Brad, senior editor at Vox.com, where he oversees the site's science, energy, and environmental coverage, "It's way too easy to cause a massive blackout in the US", April 14 2014, Vox, www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability

Back in 2012, the National Research Council worried that a well-coordinated attack on the grid "could deny large regions of the country access to bulk system power for weeks or even months. ... If such large extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold." How would that work? It's worth walking through the mechanics of how a truly massive blackout — like the 2003 Northeast blackout that left 50 million people without power — can happen. REALLY BIG BLACKOUTS ARE OFTEN CAUSED BY CASCADING FAILURES IN THE GRID Power grids are, by their nature, extremely complex. It's hard to store electricity for any extended period. That means that the output from power plants has to be equal to the use of electricity at all times. Otherwise, power lines can get overloaded or generators underloaded, causing damage to the equipment. Usually, the grid has protective devices that switch off a piece of equipment if there's a problem. So if, say, a sagging power line hits a tree — causing it to overheat — that line will get disconnected. The problem is that all the other lines now have to carry excess current. If they start overheating and have to switch off, you can get ... cascading failures. So power grid operators have to constantly monitor the system to make sure that power generation and power use are matched up and that a single fault can't cause the entire grid to fail. They're usually very good at this. But it's a difficult task — and if, the grid is already running at capacity or a major piece of equipment falters, it can be hard to prevent "cascading failures." The National Research Council was worried about an attack causing this sort of cascading effect.

EXT- Grid Impact

Collapse of the power grid causes extinction IBT 11

International Business Times, Solar Flare Could Unleash Nuclear Holocaust Across Planet Earth, Forcing Hundreds of Nuclear Power Plants Into Total Meltdowns,
<http://au.ibtimes.com/articles/213249/20110914/solar-flare-could-unleash-nuclear-holocaust-across-planet-earth-forcing-hundreds-of-nuclear-power-pl.htm>

What happens when there's no electricity? **Imagine a world without electricity. Even for just a week. Imagine New York City with no electricity, or Los Angeles, or Sao Paulo. Within 72 hours, most cities around the world will devolve into total chaos, complete with looting, violent crime, and runaway fires.** But that's not even the bad news. Even if all the major cities of the world burned to the ground for some other reason, humanity could still recover because it has the farmlands: the soils, the seeds, and the potential to recover, right? And yet the real crisis here stems from the realization that **once there is no power grid, all the nuclear power plants of the world suddenly go into "emergency mode" and are forced to rely on their on-site emergency power backups** to circulate coolants and prevent nuclear meltdowns from occurring. And yet, as we've already established, these facilities typically have only a few hours of battery power available, followed by perhaps a few days worth of diesel fuel to run their generators (or propane, in some cases). Did I also mention that half the people who work at nuclear power facilities have no idea what they're doing in the first place? Most of the veterans who really know the facilities inside and out have been forced into retirement due to reaching their **lifetime limits** of on-the-job radiation exposure, so most of the workers at nuclear facilities right now are **newbies** who really have no clue what they're doing. **There are 440 nuclear power plants operating across 30 countries around the world today.** There are an additional 250 so-called "research reactors" in existence, making a total of **roughly 700 nuclear reactors to be dealt with** (<http://www.world-nuclear.org/info/i...>). Now imagine the scenario: You've got a massive solar flare that knocks out the world power grid and destroys the majority of the power grid transformers, thrusting the world into darkness. Cities collapse into chaos and rioting, martial law is quickly declared (but it hardly matters), and every nation in the world is on full emergency. But that doesn't solve the really big problem, which is that you've got **700 nuclear reactors that can't feed power into the grid** (because all the transformers are blown up) **and yet simultaneously have to be fed a steady stream of emergency fuels to run the generators the keep the coolant pumps functioning**. How long does the coolant need to circulate in these facilities to cool the nuclear fuel? **Months.** This is also the lesson of Fukushima: You can't cool nuclear fuel in mere hours or days. It takes **months** to bring these nuclear facilities to a state of cold shutdown. And that means **in order to avoid a multitude of Fukushima-style meltdowns from occurring around the world, you need to truck diesel fuel, generator parts and nuclear plant workers to every nuclear facility on the planet, ON TIME, every time, without fail, for months on end.** Now remember, **this must be done in the middle of the total chaos** breakdown of modern civilization, **where there is no power**, where law enforcement and emergency services are totally overrun, where people are starving because food deliveries have been disrupted, and when looting and violent crime runs rampant in the streets of every major city in the world. Somehow, despite all this, you have to run these diesel fuel caravans to the nuclear power plants and keep the pumps running. Except there's a problem in all this, even if you assume you can somehow work a logistical miracle and actually deliver the diesel fuel to the backup generators on time (which you probably can't). The problem is this: Where do you get diesel fuel? Why refineries will be shut down, too from petroleum refineries. Most people don't realize it, but petroleum refineries run on electricity. Without the power grid, the refineries don't produce a drop of diesel. With no diesel, there are no generators keeping the coolant running in the nuclear power facilities. But wait, you say: Maybe we could just acquire diesel from all the gas stations in the world. Pump it out of the ground, load it into trucks and use that to power the generators, right? Except there are other problems here: How do you pump all that fuel without electricity? How do you acquire all the tires and spare parts needed to keep trucks running if there's no electricity to keep the supply businesses running? How do you maintain a truck delivery infrastructure when the electrical infrastructure is totally wiped out? Some countries might be able to pull it off with some degree of success. With military escorts and the total government control over all fuel supplies, a few nations will be able to keep a few nuclear power facilities from melting down. But

here's the real issue: There are 700 nuclear power facilities in the world, remember? Let's suppose that in the aftermath of a massive solar flare, the nations of the world are somehow able to control half of those facilities and nurse them into cold shutdown status. That still leaves roughly 350 nuclear facilities at risk. Now let's suppose half of those are somehow luckily offline and not even functioning when the solar flare hits, so they need no special attention. This is a very optimistic assumption, but that still leaves 175 nuclear power plants where all attempts fail. Let's be outrageously optimistic and suppose that a third of those somehow don't go into a total meltdown by some miracle of God, or some bizarre twist in the laws of physics. So we're still left with **115 nuclear power plants** that "go Chernobyl." Fukushima was one power plant. **Imagine the devastation of 100+ nuclear power plants, all going into meltdown all at once across the planet.** It's not the loss of electricity that's the real problem; it's the **global tidal wave of invisible radiation** that blankets the planet, permeates the topsoil, irradiates everything that breathes and delivers the final crushing blow to human civilization as we know it today. Because if you have **100 simultaneous global nuclear meltdowns**, **the tidal wave of radiation will make farming nearly impossible for years. That means no food production for several years in a row.** And that, in turn, **means a near-total collapse of the human population on our planet.** How many people can survive an entire year with no food from the farms? Not one in a hundred people. Even beyond that, how many people can essentially **live underground** and be safe enough from the radiation that they can have viable children and repopulate the planet? It's a very, very small fraction of the total population.

FT: Backups

Backups don't solve meltdowns.

AP 11 (Associated Press 3-29, Nuclear power plants in U.S. vulnerable to power outages, study shows,

http://www.pennlive.com/midstate/index.ssf/2011/03/nuclear_power_plants_in_us_vul.html)

Long before the nuclear emergency in Japan, U.S. regulators knew that a power failure lasting for days at an American nuclear plant, whatever the cause, could lead to a radioactive leak. Even so, they have required the nation's 104 nuclear reactors only to develop plans for dealing with much shorter blackouts on the assumption that power would be restored quickly. ¶ In one simulation presented by the Nuclear Regulatory Commission in 2009, it would take less than a day for radiation to escape from a reactor at a Pennsylvania nuclear power plant after an earthquake, flood or fire knocked out all electrical power and there was no way to keep the reactors cool after backup battery power ran out. ¶ That plant, the Peach Bottom Atomic Power Station outside Lancaster, has reactors of the same older make and model as those releasing radiation at Japan's Fukushima Dai-ichi plant, which is using other means to try to cool the reactors. ¶ And like Fukushima Dai-ichi, the Peach Bottom plant has enough battery power on site to power emergency cooling systems for eight hours. In Japan, that wasn't enough time for power to be restored. ¶ The risk of a blackout leading to core damage, while extremely remote, exists at all U.S. nuclear power plants, and some are more susceptible than others, according to an Associated Press investigation. While regulators say they have confidence that measures adopted in the U.S. will prevent or significantly delay a core from melting and threatening a radioactive release, the events in Japan raise questions about whether U.S. power plants are as prepared as they could and should be.

FT: Not Likely

Attacks coming—not a question of if but when—building resilience key Weise 14

Elizabeth, works in USA Today's San Francisco bureau, "Experts: Major cyberattack will hit in next 11 years", Oct 29 2014, USA Today, www.usatoday.com/story/tech/2014/10/29/pew-survey-cyber-attack/18114719/

SAN FRANCISCO – Almost two-third of technology experts expect a "major" cyber attack somewhere in the world that will cause significant loss of life or property losses in the tens of billions of dollars by 2025. A survey released Wednesday by the Pew Research Center found that many of analysts expect disruption of online systems like banking, energy and health care to become a pillar of warfare and terrorism. The survey asked over 1,600 technology experts whether a major attack that would cause "widespread harm to a nation's security and capacity to defend itself" would be launched within the next 11 years. Sixty-one percent said yes. "The probability of a major cyber attack is not 'if' but 'when,'" Oliver Crepin-Leblond, Global Information Highway, United Kingdom It's already beginning to happen, several of the researchers noted. One recent example given was an attack on Apple's iCloud data storage system earlier this month, which some security experts believe was linked to the Chinese government. Another was the July attack on JPMorgan. Some in the White House wonder if it was orchestrated by the Putin regime in Russia in retaliation for U.S. support of Ukraine, the New York Times reported. As critical infrastructure moves online, cyber attacks could take out financial systems, the power grid and health systems, wreaking as much damage as bombs, the experts said. There's already been "a Pearl Harbor event," said Jason Pontin, editor of the MIT Technology Review. He cited the 2009 Stuxnet computer worm that disabled Iranian nuclear plant centrifuges. Many in the defense world believe the attack was launched by the United States and Israel. Cyberware just plain makes sense. Attacking the power grid or other industrial control systems is asymmetrical and deniable and devilishly effective, said Stewart Baker, a partner at Steptoe & Johnson, a Washington D.C. law firm. Futurist Jamais Cascio thinks cyber attacks will become part of military engagements. "Cyber is a force-multiplier," he said. "We'll likely see a major attack that has a cyber component, but less likely to see a major cyber-attack only. Part of the problem is that security tends to be an add-on. Building resiliency into systems is crucial, said futurist David Brin.

We don't need a “perfect storm” scenario—a single blackout increases the likelihood of the next failure

Ascher 12

Brock, Communications Specialist at Iowa State University, "Quantifying Cascading Failure", Aug 17 2012, Iowa State University College of Engineering, news.engineering.iastate.edu/2012/08/17/quantifying-cascading-failure/

"People always say 'It was the perfect storm.'" Dobson says. "But these large blackouts happen because of the cascading effect. You're never going to get 20 different independent failures to happen at the same time because that's vanishingly unlikely. But if the first couple events make the next events more likely, then those events happen and make the next ones more likely – then you get those rare events happening. This is the typical way that large complicated systems have catastrophic failures, and it is not really a perfect storm."

Cascading failure is difficult to analyze because of the huge number of unanticipated variables. In other words, researchers don't know what they don't know. In addition, the dependence of individual failures on previous failures and their effect on subsequent failures creates an incredibly complex system of dependent variables. Large blackouts involve the failure of many interconnected variables, each of which affect how variables down the line interact with each other. "Imagine you're very, very tightly scheduled on a certain day," Dobson says. "Then, things start getting delayed in the morning and things get worse and worse throughout the day. Because your first appointment was delayed, It's more likely that the next one will be delayed. Pretty soon you start missing appointments altogether in the afternoon. That's a very small example of cascading failure." There are a few common attributes, like critical loading, that researchers can look for when studying cases of cascading failure. A power grid's critical loading can be defined as a point somewhere between a very low load and a very high load where the risk of a blackout increases sharply. If the amount of electricity flowing through the system is higher than the power grid critical load, the likelihood of a blackout spikes. The power grid's critical load acts as a reference point for cascading failure; stay below it and the system will likely be fine. Go above it, and the risk of a blackout is more severe. "If a transmission line carrying its usual load fails, other lines can pick up the slack without much trouble," he says. "But if the power grid as a whole is carrying a load that is above its critical loading, its burden has a much greater effect on the other lines. That's something we look for."

FT: Resilient

Their defense doesn't assume the scenario of a nuclear meltdown with a grid blackout—makes containment impossible

Stein 12

Matthew, Matthew Stein is a design engineer, green builder and author of two bestselling books, "When Disaster Strikes: A Comprehensive Guide to Emergency Planning and Crisis Survival" (Chelsea Green 2011), and "When Technology Fails: A Manual for Self-Reliance, Sustainability, and Surviving the Long Emergency" (Chelsea Green 2008). Stein is a graduate of the Massachusetts Institute of Technology (MIT), where he majored in mechanical engineering. Stein has appeared on numerous radio and television programs and is a repeat guest on Fox News, Lionel, Coast-to-Coast AM and the Thom Hartmann Show, "Four Hundred Chernobyls: Solar Flares, Electromagnetic Pulses and Nuclear Armageddon", Truthout, truth-out.org/news/item/7301-400-chernobyls-solar-flares-electromagnetic-pulses-and-nuclear-armageddon

What do extended grid blackouts have to do with potential nuclear catastrophes? Nuclear power plants are designed to disconnect automatically from the grid in the event of a local power failure or major grid anomaly; once disconnected, they begin the process of shutting down the reactor's core. In the event of the loss of coolant flow to an active nuclear reactor's core, the reactor will start to melt down and fail catastrophically within a matter of a few hours, at most. In an extreme GMD, nearly every reactor in the world could be affected. It was a short-term cooling-system failure that caused the partial reactor core meltdown in March 1979 at Three Mile Island, Pennsylvania. Similarly, according to Japanese authorities, it was not direct damage from Japan's 9.0 magnitude Tohoku Earthquake on March 11, 2011, that caused the Fukushima Daiichi nuclear reactor disaster, but the loss of electric power to the reactor's cooling system pumps when the reactor's backup batteries and diesel generators were wiped out by the ensuing tidal waves. In the hours and days after the tidal waves shuttered the cooling systems, the cores of reactors number 1, 2 and 3 were in full meltdown and released hydrogen gas, fueling explosions which breached several reactor containment vessels and blew the roof off the building housing reactor number 4's spent-fuel storage pond. Of even greater danger and concern than the reactor cores themselves are the spent fuel rods stored in on-site cooling ponds. Lacking a permanent spent nuclear fuel storage facility, so-called "temporary" nuclear fuel containment ponds are features common to nearly all nuclear reactor facilities. They typically contain the accumulated spent fuel from ten or more decommissioned reactor cores. Due to lack of a permanent repository, most of these fuel containment ponds are greatly overloaded and tightly packed beyond original design. They are generally surrounded by common light industrial buildings with concrete walls and corrugated steel roofs. Unlike the active reactor cores, which are encased inside massive "containment vessels" with thick walls of concrete and steel, the buildings surrounding spent fuel rod storage ponds would do practically nothing to contain radioactive contaminants in the event of prolonged cooling system failures. Since spent fuel ponds typically hold far greater quantities of highly radioactive material than the active nuclear reactors locked inside reinforced containment vessels, they clearly present far greater potential for the catastrophic spread of highly radioactive contaminants over huge swaths of land, polluting the environment for multiple generations. A study by the Nuclear Regulatory Commission (NRC) determined that the "boil down time" for spent fuel rod containment ponds runs from between 4 and 22 days after loss of cooling system power before degenerating into a Fukushima-like situation, depending upon the type of nuclear reactor and how recently its latest batch of fuel rods had been decommissioned.^[9] Reactor fuel rods have a protective zirconium cladding, which, if superheated while exposed to air, will burn with intense, self-generating heat, much like a

magnesium fire, releasing highly radioactive aerosols and smoke. According to nuclear whistleblower and former senior vice president for Nuclear Engineering Services Arnie Gundersen, once a zirconium fire has started, due to its extreme temperatures and high reactivity, contact with water will result in the water dissociating into hydrogen and oxygen gases, which will almost certainly lead to violent explosions. Gundersen says that once a zirconium fuel rod fire has started, the worst thing you could do is to try to quench the fire with water streams, which would cause violent explosions. Gundersen believes the massive explosion that blew the roof off the spent fuel pond at Fukushima was caused by zirconium-induced hydrogen dissociation.^[10] Had it not been for heroic efforts on the part of Japan's nuclear workers to replenish waters in the spent fuel pool at Fukushima, those spent fuel rods would have melted down and ignited their zirconium cladding, which most likely would have released far more radioactive contamination than what came from the three reactor core meltdowns. Japanese officials have estimated that Fukushima Daiichi has already released just over half as much total radioactive contamination as was released by Chernobyl into the local environment, but other sources estimate it could be significantly more than at Chernobyl. In the event of an extreme GMD-induced long-term grid collapse covering much of the globe, if just half of the world's spent fuel ponds were to boil off their water and become radioactive, zirconium-fed infernos, the ensuing contamination could far exceed the cumulative effect of 400 Chernobyls.

Grid vulnerable—lots of different groups

Gertz 14

Bill, a national security columnist for The Washington Times and senior editor at The Washington Free Beacon, "Inside the Ring: U.S. power grid defenseless from physical and cyber attacks", April 16 2014, The Washington Times,
www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/?page=all

The U.S. electrical power grid is vulnerable to cyber and physical attacks that could cause devastating disruptions throughout the country, federal and industry officials told Congress recently. Gerry Cauley, president of the North American Electric Reliability Corp., said that several — if not all — other critical U.S. infrastructures depend on electricity, and that he is “deeply concerned” about attacks, extreme weather and equipment failures causing power outages. “I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures,” Mr. Cauley told the Senate Energy and Natural Resources Committee last Thursday. Mr. Cauley said the April 2013 attack on a California electrical power substation by unidentified gunmen did not result in power outages, but highlighted the vulnerability of the country's three-sector power grid. The incident at the Metcalf substation in Northern California “demonstrates that attacks are possible and have the potential to cause significant damage to assets and disrupt customer service,” he said. Cheryl A. LaFleur, acting chairman of the Federal Energy Regulatory Commission who testified at the Senate hearing, said the Metcalf attack led federal authorities to conduct a 13-city campaign to warn utilities about the need for better security. Ms. LaFleur said cyber threats to electrical infrastructure are “fast-changing,” as she called for better information-sharing about threats between government and industry. Sue Kelly, head of the American Public Power Association of more than 2,000 U.S. electric utilities, testified about the growing danger of cyberattacks against the power grid. “The threat of cyberattack is relatively new compared to long-known physical threats, but an attack with operational

consequences could occur and cause disruptions in the flow of power if malicious actors are able to hack into the data and control systems used to operate our electric generation and transmission infrastructure,” Ms. Kelly said. To date, security measures have prevented a successful cyberattack on the bulk electric system, she said. An Energy Department-sponsored study published last fall said the U.S. power grid is vulnerable to catastrophic disruption by nation states like China and North Korea, terrorist groups like al Qaeda, and non-state criminals. The 269-page study “Electric Sector Failure Scenarios and Impact Analyses” was published in September by the National Electric Sector Cybersecurity Organization Resource, a non-government group of industry and security specialists. A malicious software cyberattack on the power grid’s Distributed Energy Resource Management System (DERMS), which manages requests and commands for the power system, would damage transformers that are costly and difficult to replace. Cyberattacks against computers that distribute electrical power over wide areas could be jammed or disrupted through wireless signals. And cyber attackers could cause widespread power outages or cascading power failures by gaining access to distribution systems and equipment via remote hacking. “After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations,” the report said. “A blackout of varying degree and potential equipment damage ensues.” According to the report, nation state threats to the grid include China, North Korea and Cuba. Among the cyber terrorist threats listed: al Qaeda and the Afghan Taliban, the Pakistani group Lashkar-e-Taibi, and the Palestinian group Hamas. Domestic threats include “lone wolf” extremists, ecoterrorists among Earth First and Greenpeace, U.S. separatist groups, and militias and hate groups, the report said.

FT: Cant solve cyberterrorism

NSA hacking means cyber-criminals become more capable of exploiting vulnerabilities—we must end our offensive strategy in order to garner international cooperation and end the zero-day race

Brewster, reporter @ The Guardian, 14

Tom, "The NSA Is Screwing Up The Fight Against Cybercrime", March 7 2014, Business Insider, www.businessinsider.com/nsa-screwing-up-fight-against-cybercrime-2014-3

Criminals learning from NSA Intelligence agency hacking techniques will also be adopted by criminals, according to security luminaries speaking with The Guardian. This has been seen in other nations in recent history. “The spear-phishing tricks we saw the Chinese secret police using against the Dalai Lama in 2008 were being used by Russian crooks to steal money from US companies by 2010. We predicted as much in … 2009,” said Ross Anderson, professor of security engineering at the University of Cambridge. “A lot more people have become aware of what can be done.” Cryptography expert and author Bruce Schneier said some of the techniques the NSA used to hack routers are starting to be seen in criminal cases, amongst other attack types. Indeed, from compromises of much used but vulnerable mobile applications, to spying on people through their web cams, dark web dealers were already using the same methods as the NSA. “Today’s secret NSA programs are tomorrow’s PHD theses and the next day’s hacker tools,” he added. “The US has done an enormous amount of damage here. There is a basic level of trust that has been lost… There is a lot of international mistrust right now because the US was supposed to be a trusted keeper of everything, but it turned out they were subverting it with every chance they got. And the NSA keeps saying it’s not as bad as you think, but who the hell believes that?” The zero-day race Purposeful backdoors in security products - another revelation from leaked security agency documents - benefit all hackers. If firms have allowed for weaknesses in their product sets, they don’t just open up holes for agents to exploit, but criminals too. Organized crime groups are pumping money into hunting for such vulnerabilities, placing the everyday user at ever greater risk. Those crooks and the NSA are racing to uncover and use zero-day flaws - previously-unknown, unpatched weaknesses in software and hardware. After governments buy, discover or use these vulnerabilities, they often filter down into the wider criminal community, says Jason Steer, director of technology strategy at FireEye. “We know that governments purchase undisclosed zero-day vulnerabilities, and the providers of such zero-days such as Vupen openly acknowledge that government are big buyers of their research in text on their website,” Steer said. “All exploits have an inevitable lifecycle - from highly targeted usage to APT [advanced persistent threat] usage, then to broader cyber criminals and finally hacktivists. “Once an exploit is used in the wild, its effectiveness will drop as researchers in both the black hat and white hat communities discover it and learn about it. Once its effectiveness is weakened, any zero-day is picked up by the broader attacker community as this gives them an opportunity to monetize their window for a time, until the targeted software or hardware fixes the vulnerability - it’s quite simply a race.” Government malware = criminal malware^[1]. But the NSA isn’t the only official body that is spurring on digital crime, whether willingly or unwittingly. In using offensive digital tools against one another, governments have brought about a degradation of co-operation on dealing with cybercrime, according to RSA chief Art Coviello. “The only ones deriving advantage from governments trying to gain advantage over one another on the internet are the criminals. Our lack of immediate, consistent and sustained cooperation, globally, gives them the equivalent of safe havens,” Coviello said during his keynote. And the introduction of government-owned malware on global networks only gives criminals yet more tools to play with. “The genie is out the bottle on the use of cyber weaponry and unlike nuclear weapons, cyber weapons are easily

propagated and can be turned on the developer,” Coviello added. Anderson has concerns around organized criminals taking advantage. “If governments keep on giving millions of people access to this stuff, it’s only a matter of time before serious organized crime gets in there.” It’s long been believed governments across the world are paying cyber criminals to help them attack foreign entities too. While this has never been detailed, Coviello and numerous others in the security industry have claimed knowledge of it happening. This has all combined to create a chaotic, dangerous environment, where attack numbers continue to rise and aggressive, sophisticated techniques have been given a sense of legitimacy, whether the targets are governmental data or individuals’ money. “Paraphrasing a famous quote, those who seek military advantage riding the back of the tiger will end up inside,” Coviello said during his keynote. Many are now calling for the NSA and other government bodies contributing to the rise in digital crime to get off that tiger.

FT: No US Leadership

The US can make up for past cyber-hypocrisy with leadership now

Weigant 13 Chris, is a political commentator, author, and blogger, "We Need a Geneva Convention on Cyber Warfare," http://www.huffingtonpost.com/chris-weigant/we-need-a-geneva-convention_b_4171853.html

Preventing any or all of this by means of **international diplomacy** might at first glance **seem to be a fool's errand**. **But it's certainly worth a try**, considering what could be avoided if it were successful. **Hammering out exactly what will and will not be allowed in cyberwarfare will be a tough task -- made even more tough by the knowledge that any such agreement would almost certainly have to be updated** (at a minimum) every decade or so, to keep up with new technological developments.

America has lost a lot of its moral standing in the world, since 9/11. This is not a partisan problem, either. Both Republicans and Democrats alike have given their consent to practices which we used to consider not only illegal, but downright abhorrent and inhumane. This includes waterboarding and all the other Orwellian-named "enhanced interrogation techniques" (which we used to consider ourselves morally above using), to dropping bombs from remotely-controlled airplanes to assassinate people we consider fair targets (how would we feel if people in Peoria were being assassinated in this fashion?).

But while this might leave the U.S. open to cries of "hypocrisy" from other countries, leading the effort to define allowable cyberwarfare techniques **would go a long way towards regaining some of that moral standing**. **America could make the case: "OK, look, we may have crossed a few lines in our war on terror, but a lot of this stuff is brand-new, so we just had the opportunity before other countries** were faced with similar choices -- **and now that we've had time to consider, we think there ought to be some rules to cover futuristic battlefields, both real and virtual."**

America should be the one to call for another Geneva Convention in the cyberwar realm. "Let's lay down some rules" we could say to the rest of the world, and then we could all start creating a few definitions and banning certain tactics (like, for instance, a cyber attack on hospital management software -- which could grind hospitals' capacity to deal with emergencies to an absolute standstill). **American politicians -- after secrets are revealed by leakers**, of course -- **always say "we welcome this conversation,"** from President Obama on down. But this conversation needs to include the whole world.

The whole effort could be doomed to failure, of course -- **but this is always true of diplomacy**. It could take a century to actually have any effect, as just the dates of the chemical weapons bans of 1899 and 1997 prove. But that doesn't mean that banning chemical weapons wasn't a worthwhile thing to attempt. We could indeed have to see a future cyber disaster of "World War I mustard gas" proportions before the nations of the world even begin to take such a thing seriously. In fact, it is very easy to be pessimistic about the chances for success.

But again, that doesn't mean it isn't worth the attempt. **The "brave new world" of computer warfare** -- in all its frightening aspects -- **desperately needs** some **rules and limits**. Communications spying and drone attacks are only the precursors for what could be eventually deployed against the United States. **If we don't take the lead now** in calling for some definition of what is humanely allowable even by countries at war with each other, **we may seriously regret not doing so later.**

EXT-Solves Cybersecurity

Trust between the government and the private sector is key to ensure cybersecurity

Kelly, reporter @ USA Today, 15

Erin, "Tech companies leery of sharing cyber threats with feds", April 2 2015,
www.usatoday.com/story/news/politics/2015/04/02/phyllis-schneck-cybersecurity-technology-summit/70838226/

WASHINGTON — U.S. tech companies still don't trust the federal government enough to share information about cyber threats, the top cybersecurity official at the Department of Homeland Security said Thursday. "My top priority is building that trust," said Phyllis Schneck, the department's deputy under secretary for cybersecurity and communications for the National Protection and Programs Directorate. Privacy concerns have grown in the wake of the 2013 revelations by former National Security Agency contractor Edward Snowden that the agency was collecting phone and other data on millions of Americans not suspected of any crime, often with the help of tech companies. The tech industry is now seeking to convince customers that their personal data will be protected from government surveillance as well as from hackers. But companies have yet to overcome the backlash they faced for complying with government orders to turn over emails, photos and other data. "It's very hard for companies to be optically aligned with the U.S. government," Schneck said at a Cybersecurity Technology Summit hosted by the Washington, D.C. chapter of the Armed Forces Communications and Electronics Association. "But there has never been a more important time to build that trust." Companies will become more trusting when the federal government can begin "showing value" to them by providing effective information to battle cyber criminals while still protecting Americans' privacy and civil liberties, Schneck said. Both the Obama administration and Congress are pushing for more information-sharing between the business community and the federal government so that the private and public sectors can help one another detect and thwart cyber criminals. President Obama announced an executive order in February to create a process for information-sharing. Last month, both the Senate and House intelligence committees passed bills that would give companies protection from lawsuits when they share cyber threat information with the government. William Evanina, head of national counterintelligence for the U.S. government, said the government is working to be able to provide companies with information beyond just who is hacking them. "We want to put context on what they (the hackers) are doing," he said. "What's the intent of the person who is doing it? Who else is being hit the same way?" That information will help the government and private companies do a better job of figuring out how to thwart cyber criminals, Evanina said. He said many hackers laugh at how easy it is to get victims to click on a link that allows the criminals to get around a company's cybersecurity system.

FT: Trust Now

Rebuilding trust between the government and the private sector is necessary to create cybersecurity

Kumar, enterprise IT investor at General Catalyst Partners, 15

Deepak Jeevan, "Crossing the Cybersecurity Trust Chasm", March 29 2015, Tech Crunch, techcrunch.com/2015/03/29/crossing-the-cybersecurity-trust-chasm/#.lxjyep:iRNX

Kudos to the President for visiting Silicon Valley last month and drawing the attention of the nation to a new world of continuous cyber attacks. The executive order signed by the President addresses the critical piece that is needed to help companies protect themselves in the future – by sharing cyber threat information between different private sector companies, and between the government and the private sector. But we need to cross the cybersecurity trust chasm to make sharing really work. Today, this trust has been broken in the system due to incessant hacking of employee/customer confidential data stored in private sector enterprises. Multiple allegations of excessive snooping against the private sector and the government have only complicated matters. We need to (re)build trust: between the government and the public; between a company and its employees; between a company and its customers; between different private sector companies; and finally between the government and the private sector. The traditional cybersecurity debate has been portrayed as a security vs. privacy dialog. Trust has largely been ignored. But, trust and only trust can bring together the repelling poles of security & privacy.

EXT: Econ Imp

Perception of global economic decline triggers lashout and global war--- economic institutions won't check

Harold James 14, Professor of history at Princeton University's Woodrow Wilson School who specializes in European economic history, 7/2/14, "Debate: Is 2014, like 1914, a prelude to world war?", <http://www.theglobeandmail.com/globe-debate/read-and-vote-is-2014-like-1914-a-prelude-to-world-war/article19325504/>

As we get closer to the centenary of Gavrilo Princip's act of terrorism in Sarajevo, there is an ever more vivid fear: **it could happen again.** The approach of **the hundredth anniversary of 1914 has put a spotlight on the fragility of the world's** political and **economic security systems.**

At the beginning of 2013, Luxembourg's Prime Minister Jean-Claude Juncker was widely ridiculed for evoking the shades of 1913. By now he is looking like a prophet. By 2014, as **the security situation in the South China Sea deteriorated**, Japanese Prime Minister Shinzo Abe cast China as the equivalent to Kaiser Wilhelm's Germany; and the **fighting in Ukraine and in Iraq is a sharp reminder of the dangers of escalation.**

Lessons of 1914 are about more than simply the dangers of national and sectarian animosities. **The main story of today as then is the precariousness of financial globalization,** and the consequences that political leaders draw from it.

In the influential view of Norman Angell in his 1910 book The Great Illusion, **the interdependency of the increasingly complex global economy made war impossible. But a quite opposite conclusion was possible and equally plausible – and proved to be the case.** Given the extent of **fragility, a clever twist to the control levers might make war easily winnable by the economic hegemon.**

In the wake of an epochal financial crisis that almost brought a complete global collapse, in 1907, several countries started to think of finance as primarily an instrument of raw power, one that could and should be turned to national advantage.

The 1907 panic emanated from the United States but affected the rest of the world and demonstrated the fragility of the whole international financial order. The aftermath of the 1907 crash drove the then hegemonic power – Great Britain – to reflect on how it could use its financial power.

Between 1905 and 1908, the British Admiralty evolved the broad outlines of a plan for financial and economic warfare that would wreck the financial system of its major European rival, Germany, and destroy its fighting capacity.

Britain used its extensive networks to gather information about opponents. London banks financed most of the world's trade. Lloyds provided insurance for the shipping not just of Britain, but of the world. Financial networks provided the information that allowed the British government to find the sensitive strategic vulnerabilities of the opposing alliance.

What pre-1914 Britain did anticipated the private-public partnership that today links technology giants such as Google, Apple or Verizon to U.S. intelligence gathering. Since last year, the Edward Snowden leaks about the NSA have shed a light on the way that global networks are used as a source of intelligence and power.

For Britain's rivals, the financial panic of 1907 showed the necessity of mobilizing financial powers themselves. The United States realized that it needed a central bank analogous to the Bank of England. American financiers thought that New York needed to develop its own commercial trading system that could handle bills of exchange in the same way as the London market.

Some of **the dynamics of the pre-1914 financial world are now re-emerging.** Then an **economically declining power, Britain, wanted to use finance as a weapon** against its larger and faster growing competitors, Germany and the United States. **Now America is** in turn **obsessed by being overtaken by China** – according to some calculations, set to become the world's largest economy in 2014.

In the aftermath of the 2008 financial crisis, financial institutions appear both as dangerous weapons of mass destruction, but also as potential instruments for the application of national power.

In managing the 2008 crisis, the dependence of foreign banks on U.S. dollar funding constituted a major weakness, and required the provision of large swap lines by the Federal Reserve. The United States provided that support to some countries, but not others, on the basis of an explicitly political logic, as Eswar Prasad demonstrates in his new book on the “Dollar Trap.”

Geo-politics is intruding into banking practice elsewhere. Before the Ukraine crisis, Russian banks were trying to acquire assets in Central and Eastern Europe. European and U.S. banks are playing a much reduced role in Asian trade finance. Chinese banks are being pushed to expand their role in global commerce. After the financial crisis, China started to build up the renminbi as a major international currency. Russia and China have just proposed to create a new credit rating agency to avoid what they regard as the political bias of the existing (American-based) agencies.

The next stage in this logic is to think about how financial power can be directed to national advantage in the case of a diplomatic tussle. Sanctions are a routine (and not terribly successful) part of the pressure applied to rogue states such as Iran and North Korea. But financial pressure can be much more powerfully applied to countries that are deeply embedded in the world economy.

The test is in the Western imposition of sanctions after the Russian annexation of Crimea. President Vladimir Putin’s calculation in response is that the European Union and the United States cannot possibly be serious about the financial war. It would turn into a boomerang: Russia would be less affected than the more developed and complex financial markets of Europe and America.

The threat of systemic disruption generates a new sort of uncertainty, one that mirrors the decisive feature of the crisis of the summer of 1914. At that time, no one could really know whether clashes would escalate or not. That feature contrasts remarkably with almost the entirety of the Cold War, especially since the 1960s, when **the strategic doctrine of Mutually Assured Destruction left no doubt that any superpower conflict would inevitably escalate.**

The idea of network disruption relies on the ability to achieve advantage by surprise, and to win at no or low cost. But it is inevitably a gamble, and raises prospect that others might, but also might not be able to, mount the same sort of operation. Just as in 1914, **there is an enhanced temptation to roll the dice, even though the game may be fatal.**

Cooperation

Global Cooperation

NSA restrictions create credibility for more effective counter-terrorism and cybersecurity programs

Goldsmith 13

Jack Goldsmith, a contributing editor, teaches at Harvard Law School and is a member of the Hoover Institution Task Force on National Security and Law, 10-10-13, We Need an Invasive NSA, The New Republic, <http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>

There are two reasons to think that these predictions are wrong and that the government, with extensive assistance from the NSA, will one day intimately monitor private networks.[¶] The first is that the cybersecurity threat is more pervasive and severe than the terrorism threat and is somewhat easier to see. If the Times' website goes down a few more times and for longer periods, and if the next penetration of its computer systems causes large intellectual property losses or a compromise in its reporting, even the editorial page would rethink the proper balance of privacy and security. The point generalizes: As cyber-theft and cyber-attacks continue to spread (and they will), and especially when they result in a catastrophic disaster (like a banking compromise that destroys market confidence, or a successful attack on an electrical grid), the public will demand government action to remedy the problem and will adjust its tolerance for intrusive government measures.[¶] At that point, the nation's willingness to adopt some version of Alexander's vision will depend on the possibility of credible restraints on the NSA's activities and credible ways for the public to monitor, debate, and approve what the NSA is doing over time.[¶] Which leads to the second reason why skeptics about enhanced government involvement in the network might be wrong. The public mistrusts the NSA not just because of what it does, but also because of its extraordinary secrecy. To obtain the credibility it needs to secure permission from the American people to protect our networks, the NSA and the intelligence community must fundamentally recalibrate their attitude toward disclosure and scrutiny. There are signs that this is happening—and that, despite the undoubtedly damage he inflicted on our national security in other respects, we have Edward Snowden to thank.[¶] "Before the unauthorized disclosures, we were always conservative about discussing specifics of our collection programs, based on the truism that the more adversaries know about what we're doing, the more they can avoid our surveillance," testified Director of National Intelligence James Clapper last month. "But the disclosures, for better or worse, have lowered the threshold for discussing these matters in public."[¶] In the last few weeks, the NSA has done the unthinkable in releasing dozens of documents that implicitly confirm general elements of its collection capabilities. These revelations are bewildering to most people in the intelligence community and no doubt hurt some elements of collection. But they are justified by the countervailing need for public debate about, and public confidence in, NSA activities that had run ahead of what the public expected. And they suggest that secrecy about collection capacities is one value, but not the only or even the most important one. They also show that not all revelations of NSA capabilities are equally harmful. Disclosure that it sweeps up metadata is less damaging to its mission than disclosure of the fine-grained details about how it collects and analyzes that metadata.[¶] It is unclear whether the government's new attitude toward secrecy is merely a somewhat panicked reaction to Snowden, or if it's also part of a larger rethinking about the need for greater tactical openness to secure strategic political legitimacy. Let us hope, for the sake of our cybersecurity, that it is the latter.

NSA surveillance undermines US-EU intelligence cooperation.

Kristin Archick, 12/1/2014. Specialist in European Affairs @ Congressional Research Service. "U.S.-EU Cooperation Against Terrorism," CRS Report, <https://www.fas.org/sgp/crs/row/RS22030.pdf>.

The September 11, 2001, terrorist attacks on the United States and the subsequent revelation of Al Qaeda cells in Europe gave new momentum to European Union (EU) initiatives to combat terrorism and improve police, judicial, and intelligence cooperation among its member states. Other deadly incidents in Europe, such as the Madrid and London bombings in 2004 and 2005 respectively, injected further urgency into strengthening EU counterterrorism capabilities and reducing barriers among national law enforcement authorities so that information could be meaningfully shared and suspects apprehended expeditiously. Among other steps, the EU has established a common definition of terrorism and a common list of terrorist groups, an EU arrest warrant, enhanced tools to stem terrorist financing, and new measures to strengthen external EU border controls and improve transport security. Over the years, the EU has also encouraged member states to devote resources to countering radicalization and terrorist recruitment, issues that have been receiving renewed attention in light of growing European concerns about the possible threats posed by European fighters returning from the conflicts in Syria and Iraq. Promoting law enforcement and intelligence cooperation with the United States has been another top EU priority since 2001. Washington has largely welcomed enhanced counterterrorism cooperation with the EU, which has led to a new dynamic in U.S.-EU relations by fostering dialogue on law enforcement and homeland security issues previously reserved for bilateral discussions. Contacts between U.S. and EU officials on police, judicial, and border control policy matters have increased substantially and a number of new U.S.-EU agreements have also been reached; these include information-sharing arrangements between the United States and EU police and judicial bodies, two U.S.-EU treaties on extradition and mutual legal assistance, and accords on container security and airline passenger data. In addition, the United States and the EU have been working together to curb terrorist financing and to strengthen transport security. Nevertheless, some challenges persist in fostering closer U.S.-EU cooperation in these fields. Among the most prominent and long-standing are data privacy and data protection issues. The negotiation of several U.S.-EU information-sharing agreements, from those related to tracking terrorist financial data to sharing airline passenger information, has been complicated by EU concerns about whether the United States could guarantee a sufficient level of protection for European citizens' personal data. EU worries about U.S. data protection safeguards and practices have been further heightened by the unauthorized disclosures since June 2013 of U.S. National Security Agency (NSA) surveillance programs and subsequent allegations of U.S. collection activities in Europe (including reports that U.S. intelligence agencies have monitored EU diplomatic offices and German Chancellor Angela Merkel's mobile phone). Other issues that have led to periodic tensions include detainee policies, differences in the U.S. and EU terrorist designation lists, and balancing measures to improve border controls and border security with the need to facilitate legitimate transatlantic travel and commerce. Congressional decisions related to intelligence-gathering reforms, data privacy, border controls, and transport security may affect how future U.S.-EU counterterrorism cooperation evolves. In addition, given the European Parliament's growing influence in many of these policy areas, Members of Congress may be able to help shape the Parliament's views and responses through ongoing contacts and the existing Transatlantic Legislators' Dialogue (TLD). This report examines the evolution of U.S.-EU counterterrorism cooperation and the ongoing challenges that may be of interest in the 113 th Congress.

Intelligence sharing is key to effective operations --- diplomacy key to maintain those coalitions.

Anna-Katherine Staser **McGill and David H. Gray**, Summer 2012. School of Graduate and Continuing Studies in Diplomacy Norwich University; and Campbell University. "Challenges to International Counterterrorism Intelligence Sharing," Global Security Studies, 3.3, <http://globalsecuritystudies.com/McGill%20Intel%20Share.pdf>.

It is clear that diplomacy will continue to be a key component in US counterterrorism coalition building. Intelligence sharing, as a by-product of these efforts, will likely improve for as long as trust is maintained or improved and compromises are made in the greater interest of combating the shared threat of terrorism. However, the US is also likely to face continuing foreseeable challenges from the ever expanding breadth of its international allies, its increasing dependence on its counterterrorism coalitions, and unpredictable setbacks to international trust like WikiLeaks. There are ways, however, to allay the impact of these challenges if not overcome

them all together. With regards to traditional allies the United States must continue to negotiate a close working relationship with its NATO, EU, and 5 EYES partners. Great strides have been made but future disagreements on policy, tactics, and strategy for the war on terrorism are inevitable. The best way to prepare for such future issues is to continue to foster a positive collaborative relationship with these nations so that mutual trust will prevent arguments from threatening the survival of the alliance. This means that the US must carefully manage its international position. It cannot exploit legal loopholes like exporting suspects to other nations for questionable interrogations; it cannot bully its friends nor act unilaterally against their wishes; and it must hold itself to high moral standards befitting a liberal democracy. For new and non-traditional allies, Reveron states that “the long-term challenge for policymakers will be to convert these short-term tactical relationships into meaningful alliances while protecting against counterintelligence threats” (467). Traditional alliances have to start somewhere and over time these new relationships can turn in to tried and tested cooperation. In order to further develop these relationships the US should attempt to iron out policy differences in other arenas rather than turn a blind eye to them and continue providing technical and material support to their development of effective intelligence programs. The US should not however hold CT cooperation supreme over other critical issues such as nuclear and conventional arms proliferation and human rights violations. Nations like Iran and Syria may be helpful in the short term and for limited purposes but this does not negate their less desirable practices. Finally, the US will also need to look inward to prevent more classified information leaks. The US needs to be more critical in the issuance of security clearances, employ digital monitoring of who is downloading information and in what amount to prevent mass dumps, and give greater importance to curtailing the “insider threat” of US citizens leaking information overall. Improving intelligence security will help to mitigate the blowback from WikiLeaks and will go a long way to advancing US credibility and trust building. The careful maintenance and development of counterterrorism intelligence sharing is no doubt critical to the success of national and international-level CT operations. As this paper has demonstrated, many of the solutions to challenges facing CT intelligence sharing will require long-term solutions requiring patience, compromise, and vigilance. It will no doubt be a difficult task but intelligence is the first line of defense against terrorism. As such, it is imperative that the United States do all that it can strengthen this defense.

EU intelligence cooperation is key to effective prevention of terrorism but NSA surveillance deters cooperation.

George X. Protopapas, December 2014. Analyst at the Research Institute for European and American Studies (RIEAS) and member of International Institute for Middle-East and Balkan Studies. “European Union’s Intelligence Cooperation: A Failed Imagination?” Journal of Mediterranean and Balkan Intelligence, 4,2, http://www.academia.edu/10996393/European_Union_s_Intelligence_Cooperation_A_Failed_Imagination.

In addition, Snowden’s case provoked confrontation among the euro Atlantic partners as the National Security Agency (NSA) spying revelations broke the ties of trust between USA and EU Member- States. For example, the German parliament decided the establishment of a special Bundestag committee in order to investigate the global spying activities of the American National Security Agency (NSA) and European counterparts such as the GCHQ in the UK. Furthermore, the committee will likely examine if the German intelligence agencies were either aware of, or complicit in, the gathering of people’s data.¹⁸ The threat of the spread of Islamic extremism in the European continent desperately demands a close cooperation of the intelligence communities of USA, the European Union and the European states. The European Islamist extremists, who fight in the war of Syria against the president Bashar Assad pose a very dangerous threat, when they return in their European hometowns. The intelligence cooperation and sharing between USA and the European allies increase the possibilities for an effective identification and the prevention of terrorist, terrorism attacks and the organized crime’s illegal activities. In addition, the links between Islamic terrorist cells and organized crime groups pose

a more combined threat to European security, as the terrorists and criminals has a boarder field of cooperation (illegal trade weapons, smuggling, human trafficking, drugs, extortion, adductions for money etc.)

Surveillance by the National Security Agency is undermining intelligence cooperation with allies as the U.S. fights the growing threat of Islamic extremists.

The June 2013 revelations of NSA spying by contractor Edward Snowden are having repercussions, particularly in Germany, even as many allies come to appreciate the need to keep closer tabs on potential terrorists in the wake of deadly attacks in Europe and North America.

Reports in the German media that the NSA asked the German intelligence service BND to spy on Siemens, a German company suspected of dealing with Russia, as well as other European companies and politicians, have rattled the government of Chancellor Angela Merkel, which is already dealing with demands from a parliamentary investigation into Snowden's allegations.

The BND last week reportedly stopped sharing Internet surveillance data with the NSA, the latest fallout from the scandal.

Efforts to smooth out the bumps caused by Snowden have contributed to some of the fallout, as European parliaments become more assertive at overseeing their own intelligence agencies, which often are full partners in the NSA's activities.

European Cooperation

NSA overreach hurts US-EU terror cooperation

Mix 15 (Derek E. , Analyst in European Affairs “The United States and Europe: Current Issues,” <https://www.fas.org/sgp/crs/row/RS22163.pdf> , February 3)

In 2013, press reports began surfacing about U.S. National Security Agency (NSA) surveillance programs in the United States and Europe created tensions in the transatlantic relationship. Among other allegations, the reports asserted that objects of U.S. spying included the EU offices in Washington, DC and the cell phone of German Chancellor Angela Merkel. The information was based on leaked, classified documents obtained from Edward Snowden, a former NSA contractor; and focused on operations allegedly conducted by the NSA and the UK’s Government Communications Headquarters (the UK’s signals intelligence agency). The reports raised serious concerns on both sides of the Atlantic about the extent of U.S. surveillance operations, the degree of involvement by European intelligence services, and the appropriate balance between promoting security and upholding privacy rights and civil liberties. Some observers worry that the allegations have resulted in lasting damage to transatlantic trust, negatively affecting U.S.-European political, security, and economic ties. Many European leaders, EU officials, and European citizens were deeply dismayed by the reports and concerned that such operations could violate European privacy rights and civil liberties and compromise the security of European citizens’ personal data. Criticism has been most pronounced in Germany, where disclosed NSA activities appear to have been broad in scope and the issue of government surveillance of private citizens evokes particularly strong feelings due to the legacy of domestic spying by the Nazi and East German regimes. Many analysts point out that the fallout from the reports could have implications for U.S.- European cooperation on counterterrorism and data privacy by complicating negotiations about renewal of the SWIFT and passenger name record (PNR) agreements (in 2015 and 2019, respectively), as well as the proposed Data Privacy and Protection Agreement. In the European Parliament, the reports exacerbated long-standing objections to the SWIFT and PNR agreements and intensified MEPs’ concerns about U.S. data protection safeguards and access to European citizens’ personal data. In the aftermath of the reports, the European Parliament called for 17 suspension of the U.S.-EU Safe Harbor agreement that allows commercial data exchanges, and there have been suggestions that the purported U.S. surveillance activities may have a wider effect on economic relations, including with regard to negotiations on the proposed TTIP.

Europe specifically hates surveillance of information held by US companies-the aff solves their concerns

Moyer 13 (Edward, Edward Moyer is an associate editor at CNET News and a many-year veteran of the writing and editing world “Eye on surveillance: France's PRISM, EU's concerns,” Eye on surveillance: France's PRISM, EU's concerns July 4)

Valls isn't the only European concerned about the U.S. National Security Agency: The European Parliament has adopted a joint, cross-party resolution to begin investigations into widespread NSA surveillance of the citizens of member states. As Zack Whittaker at CNET sister site ZDNet reports, the vote calls on the U.S. "to suspend and review any laws and surveillance programs that 'violate the fundamental right of EU citizens to privacy and data protection,' as well as Europe's 'sovereignty and jurisdiction'." The resolution also gives the European Commission the go-ahead to suspend data-sharing laws between Europe and the U.S., should the commission decide[d] to. The resolution says the

EC should "give consideration to all the instruments at their disposal in discussions and negotiations with the U.S...including the possible suspension of the passenger name record (PNR) and terrorist finance tracking program (TFTP) agreements." If the PNR were put on ice, flights between the U.S. and Europe could conceivably be grounded. The vote also notes "concern" over PRISM surveillance programs involving EU countries including Germany, the Netherlands, Poland, and Sweden. And it gives the European Parliament's Civil Liberties, Justice and Home Affairs committee the greenlight to start gathering evidence from U.S. and EU sources on how surveillance activities might violate EU citizens' rights to privacy and data protection. The committee plans to deliver its conclusions by the end of the year. In other Europe-related news, the Guardian cited a German government spokesman in reporting that "a working group of high-level U.S. and German intelligence experts will begin 'an immediate and intense discussion' over the issues of data protection and intelligence collection" to address mounting European concerns that are "threatening to overshadow trade negotiations and damage Silicon Valley exports." Those talks could begin as soon as Monday. Also, EC Vice President Neelie Kroes said in a statement after the meeting of the European Cloud Partnership Board that though "cloud computing helps us benefit from the data revolution and is a gift to our economy," questions surrounding surveillance efforts are a problem. "If European cloud customers cannot trust the United States government or their assurances [regarding surveillance efforts], then maybe they won't trust U.S. cloud providers either. That is my guess. And if I am right then there are multibillion euro consequences for American companies." "We need trust," Kroes said. "In some cases, of course, it may be legitimate for authorities to access, to some degree, information held online; child protection and terrorism are good examples. Such access must be based on transparent rule of law, and is the exception to the rule." Is all this world-shaking cloak-and-dagger business beginning to sound like fodder for a Hollywood-style film? Well, a group of Hong Kong-based indie filmmakers have already been there, done that -- sort of. The Wall Street Journal's Speakeasy blog recently noted the posting to YouTube of the 5-minute short "Verax," which imagines what might have happened as U.S. and Chinese intelligence officers raced to find PRISM leaker Edward Snowden as he hid out in Hong Kong. Co-creator Marcus Tsui described the effort to Speakeasy as "a snapshot in time," as residents of the city speculated about the fate of Snowden, who was eventually allowed to leave the city because a U.S. extradition request did not fully comply with Hong Kong law. Snowden has reportedly filed for political asylum in 20 countries but is still apparently holed up in the transit section of Russia's Sheremetyevo airport. And Mashable reported today that members of Iceland's Pirate Party introduced a bill that would give Snowden Icelandic citizenship, should he end up in that country. The film's title, "Verax" ("truth teller" in Latin), refers to the code-name Snowden used when dealing with The Washington Post, to which, along with the U.K.'s Guardian, he leaked top-secret documents regarding NSA spying programs. Here's the film. We imagine someone will make a feature length movie about the Snowden saga one of these days.

Regulation of domestic surveillance is sufficient to solve- it's key to compliance with international agreements

PROFITT 13 (BRIAN , Brian Proffitt is a technology expert specializing in enterprise, cloud computing and big data with 23 years of journalism and publishing experience. He is the author of 24 books on mobile technology and personal computing and an adjunct instructor at top-ranked Mendoza College of Business at the University of Notre Dame. Breathing is a hobby. "PRISM Fallout: U.S. Internet Companies Stained By Intelligence Actions

Is the cloud about to be geo-fenced into Balkanized collections of data thanks to PRISM? ,"
<http://readwrite.com/2013/07/03/prism-fallout-us-internet-companies-stained-by-intelligence-actions>, JUL 3)

It was bound to happen sooner or later: faced with mounting global criticism on its use of Internet data to monitor international denizens for intelligence reasons, the U.S. is now starting right up there with China as safest places to store data on the Web. If trust in U.S. web and data services continues to erode, the future of global cloud computing will be a much different place than what is currently envisioned. The AP is reporting today that German Interior Minister Hans-Peter Friedrich is warning anyone on the Internet to avoid using U.S.-based services such as those from Facebook, Google or Microsoft. ... Friedrich told reporters in Berlin on Wednesday that "whoever fears their communication is being intercepted in any way should use services that don't go through American servers." Germany is only one of several nations that are particularly angered by revelations that the U.S. apparently is engaging in wide-scale intelligence gathering using data collected directly from private Internet firms via the so-called PRISM project. If the allegations implied by the leaked PRISM documents are true, then PRISM would seriously jeopardize business relations between the U.S. and other countries. The European Union may be the first

relationship to get damaged. See also: PRISM Fallout: In Cloud We Don't Trust? In order to comply with strict E.U. data laws, which essentially prevent data being stored outside an E.U. member nation's borders, the E.U. and the U.S. have established a Safe Harbor agreement that enables data to be stored in U.S.-based cloud services so long as the U.S. service providers self-regulate themselves to maintain strict standards of privacy protections. Recent assertions show that U.S. intelligence services may actually have on-site equipment on PRISM participants' property, despite repeated denials from those services, which also include Yahoo, PalTalk, AOL, Skype, YouTube and Apple. If the information from the leaked PRISM documents is true, this is a serious breach of their Safe Harbor agreement. Even if PRISM turns out to be fictitious, just the hint that something like PRISM could exist could evaporate a large amount of trust and business for U.S. cloud vendors—even ones not named in the PRISM documents. Friedrich's comments today are a sharp reminder of just how fast the relationship between E.U. and U.S. companies could deteriorate Bound by law not to discuss what they are doing to help intelligence services, the named PRISM companies and services are facing a P.R. nightmare, where all they can do is deny and hope the problem goes away. International policy makers are growing increasingly angered at what they see as U.S. arrogance. (Yesterday's search of Bolivian President Evo Morales's plane by Austrian authorities in Vienna for Edward Snowden, the self-identified leaker of the PRISM documents, probably does not help that perception.) We may very well be heading for a new geo-fenced world of data isolationism, where the storage of data across international borders will not be so commonplace as it is today. If that becomes the case, how will the Internet landscape work then? Will apps that sell on an international scale be forced to maintain separate Balkanized data collections for each nation served? Or will any Internet-based company now be forced to lock down their data in direct defiance of state-sanctioned data collection operations? Neither choice seems palatable, but to regain the trust and business of a global audience, the U.S. may have to take such drastic measures. What's your picture of a post-PRISM Internet future?

The perception of restoring oversight is key to solve European concerns

Lister 13 (Tim, CNN, 10-25-2013, "Europe falls out of love with Obama over NSA spying claims," CNN, <http://www.cnn.com/2013/10/24/world/europe/europe-us-surveillance/>)

On July 24, 2008, then-presidential candidate Barack Obama addressed tens of thousands of Germans on the avenue that leads from the Brandenburg Gate in Berlin. In a pointed reference to the outgoing administration of President George W. Bush, he promised a new era of "allies who will listen to each other, who will learn from each other, who will, above all, trust each other." One German present among the hugely enthusiastic crowd said the occasion reminded him of Berlin's famous "Love Parade." No U.S. politician since John F. Kennedy had so captured Europeans' imagination. Five years on, in the words of the song, it's a case of "After the Love Has Gone." The U.S. ambassador in Berlin has been summoned to the foreign ministry over reports in Der Spiegel that the U.S. National Security Administration (NSA) monitored Chancellor Angela Merkel's official cellphone. His counterpart in Paris received a similar summons earlier this week after revelations in Le Monde. Merkel says Europe's trust must be repaired after U.S. spying claims Both Der Spiegel and Le Monde used documents provided by former NSA contractor Edward Snowden. U.S. denies report it spied on Merkel. One of Chancellor Merkel's closest allies, Defense Minister Thomas de Maiziere told broadcaster ARD there would be consequences. "We can't simply turn the page," he warned. Der Spiegel reported Thursday that Thomas Oppermann, who leads the parliamentary committee that scrutinizes Germany's intelligence services, complained that "the NSA's monitoring activities have gotten completely out of hand, and take place beyond all democratic controls." In an article for the forthcoming edition of Foreign Affairs magazine, Henry Farrell and Martha Finnemore argue that it's the disclosure of such practices rather than their existence that is damaging. "When these deeds turn out to clash with the government's public rhetoric, as they so often do, it becomes harder for U.S. allies to overlook Washington's covert behavior and easier for U.S. adversaries to justify their own," they

write. "The U.S. government, its friends, and its foes can no longer plausibly deny the dark side of U.S. foreign policy and will have to address it head-on," they argue. Among the Twitterati, #merkelphone has gained some traction, with the famous Obama motif "Yes We Can" finding a new interpretation. And the European media has begun to debate whether the revelations provided by Edward Snowden to The Guardian and other newspapers will do to Obama's image on the continent what the Iraq war did to that of President George W. Bush. Hyperbole perhaps, but the Obama administration is on the defensive, caught between fuller disclosure of just what the NSA has been up to and the need to protect intelligence-gathering methods. The president himself received what German officials describe as an angry call from Merkel Wednesday demanding assurances that there is no American eavesdropping on her conversations. The language out of the White House has been less than forthright, with spokesman Jay Carney saying that "the president assured the chancellor that the United States is not monitoring, and will not monitor, the communications of the chancellor." His careful avoidance of the past tense has heightened suspicions in Europe that only the Snowden disclosures have forced a change of practice. Even pro-U.S. newspapers like the Frankfurter Allgemeine Zeitung are in full throttle, writing that: "The government in Washington has apparently not yet understood the level of damage that continues to be caused by the activities of American intelligence agencies in Europe." Le Monde reported that the NSA collected details of millions of phone calls made in France, and described it indignantly as "intrusion, on a vast scale, both into the private space of French citizens as well as into the secrets of major national firms." French Prime Minister Jean-Marc Ayrault commented it was "incredible that an allied country like the United States at this point goes as far as spying on private communications that have no strategic justification, no justification on the basis of national defense." The U.S. Director of National Intelligence insisted in a curt statement that "the allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false." But President Obama called his French counterpart, Hollande, and the White House subsequently acknowledged the allegations had raised legitimate questions for our friends and allies. "The fall-out may be more than rhetorical." Germany's opposition Social Democrats are asking whether the European Union can -- or should -- agree a free trade deal with the U.S. in the current atmosphere. Negotiations on the Transatlantic Trade and Investment Partnership were already in a fragile state and will not be helped by claims in Le Monde that large French corporations such as telecom company Alcatel-Lucent have been targeted by the NSA. The European parliament has always been prickly about data-sharing with the U.S., and for years held up the U.S. Treasury's efforts to use the SWIFT interbank apparatus to keep tabs on terrorists' financial flows. The parliament this week passed a non-binding resolution calling for the agreement that was eventually reached to be suspended. And a parliamentary committee has agreed tough measures that would forbid U.S. companies providing data services in Europe to transfer the information to the U.S. without obtaining permission. The legislation must be agreed with member states, but for those hoping to get the provision deleted the wind is blowing in the wrong direction. Not unlike the WikiLeaks disclosures, reports based on the Snowden documents have caused embarrassment and friction around the world. President Dilma Rousseff of Brazil cancelled a visit to the United States after it was alleged that the NSA had intercepted her messages as well as communications from the state oil company, Petrobras, now one of the biggest players in the oil industry. Spiegel reported the U.S. had also accessed emails to and from former Mexican President Felipe Calderón while he was still in office. Obama, in his address to the U.N. General Assembly last month, tried to head off the gathering storm - saying: "We've begun to review the way that we gather intelligence, so that we properly balance the legitimate security concerns of our citizens and allies with the privacy concerns that all people share." U.S. spy chief says reports of NSA logging French phone calls are false. And there is a hint in the U.S. response this week that, to borrow from Hamlet: "The lady doth protest too much." The NSA itself has made the point that "the United States gathers foreign intelligence of the type gathered by all nations." The UK and France are among governments that run their own expansive technical programs. Der Spiegel reported -- again based on Snowden's disclosures -- that the British equivalent of the NSA was involved in a cyber-attack against Belgium's state-run telecommunications company, Belgacom. The company would only say that "the intruder had massive resources, sophisticated means and a steadfast intent to break into our network." The Europeans have been very grateful to share the benefits of the NSA's immense data-gathering abilities in counter-terrorism and other fields. U.S. diplomatic cables disclosed by WikiLeaks show Germany was enthusiastic in 2009 and 2010 for closer links with the NSA to develop what is known as a High Resolution Optical System (HiROS) -- a highly advanced "constellation" of reconnaissance satellites. One cable from the U.S. Embassy in Berlin said: "Germany anticipates that their emergence as a world leader in overhead reconnaissance will generate interest from the USG and envisions an expansion of the

intelligence relationship." The 9/11 attacks changed espionage beyond recognition, leading to massive investment in the U.S. in "technical means" -- the flagship of which is the enormous NSA data center being completed in Bluffdale, Utah. Its computing power, according to the specialist online publication [govtech.com](#) is "equivalent to the capacity of 62 billion iPhone 5s." But 9/11 also shifted the balance between intelligence-gathering and civil liberties, with the U.S. federal government acquiring new powers in the fight against terrorism -- some sanctioned by Congress but others ill-defined. The technology that allows such enormous data-harvesting cannot be put back in the box, but the limits to its use pose an equally huge challenge. Ultimately, the Europeans need to collaborate with the U.S. on intelligence-gathering, to deal with international terrorism, cyber threats and organized crime. But the Snowden allegations, whether reported accurately or not, have changed the public perception and mood in Europe, obliging leaders like Merkel to take a tougher stand. At least there has been plenty of room for black humor amid the diplomatic back-and-forth. "Earnest question: What do European leaders talk about that's worth spying on?" asked Politico's Blake Hounshell on Twitter, while New York Times London bureau chief Steve Erlanger quipped: "I'm not sure I'd want to listen in to Silvio Berlusconi's cellphone."

NSA surveillance hurts EU-US cooperation

Ball 13 (James, special projects editor, The Guardian. 10/25.

www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls)

The National Security Agency monitored the phone conversations of 35 world leaders after being given the numbers by an official in another US government department, according to a classified document provided by whistleblower Edward Snowden. The confidential memo reveals that the NSA encourages senior officials in its "customer" departments, such the White House, State and the Pentagon, to share their "Rolodexes" so the agency can add the phone numbers of leading foreign politicians to their surveillance systems. The document notes that one unnamed US official handed over 200 numbers, including those of the 35 world leaders, none of whom is named. These were immediately "tasked" for monitoring by the NSA. The revelation is set to add to mounting diplomatic tensions between the US and its allies, after the German chancellor Angela Merkel on Wednesday accused the US of tapping her mobile phone. After Merkel's allegations became public, White House press secretary Jay Carney issued a statement that said the US "is not monitoring and will not monitor" the German chancellor's communications. But that failed to quell the row, as officials in Berlin quickly pointed out that the US did not deny monitoring the phone in the past. Arriving in Brussels for an EU summit Merkel accused the US of a breach of trust. "We need to have trust in our allies and partners, and this must now be established once again. I repeat that spying among friends is not at all acceptable against anyone, and that goes for every citizen in Germany." The NSA memo obtained by the Guardian suggests that such surveillance was not isolated, as the agency routinely monitors the phone numbers of world leaders – and even asks for the assistance of other US officials to do so. The memo, dated October 2006 and which was issued to staff in the agency's Signals Intelligence Directorate (SID), was titled "Customers Can Help SID Obtain Targetable Phone Numbers". It begins by setting out an example of how US officials who mixed with world leaders and politicians could help agency surveillance. In one recent case," the memo notes, "a US official provided NSA with 200 phone numbers to 35 world leaders ... Despite the fact that the majority is probably available via open source, the PCs [intelligence production centers] have noted 43 previously unknown phone numbers. These numbers plus several others have been tasked." The document continues by saying the new phone numbers had helped the agency discover still more new contact details to add to their monitoring. "These numbers have provided lead information to other numbers that have subsequently been tasked." But the memo acknowledges that eavesdropping on the numbers had produced "little reportable intelligence". In the wake of the Merkel row, the US is facing growing international criticism that any intelligence benefit from spying on friendly governments is far

outweighed by the potential diplomatic damage. The memo then asks analysts to think about any customers they currently serve who might similarly be happy to turn over details of their contacts. "This success leads S2 [signals intelligence] to wonder if there are NSA liaisons whose supported customers may be willing to share their 'Rolodexes' or phone lists with NSA as potential sources of intelligence," it states. "S2 welcomes such information!" The document suggests that sometimes these offers come unsolicited, with US "customers" spontaneously offering the agency access to their overseas networks. "From time to time, SID is offered access to the personal contact databases of US officials," it states. "Such 'Rolodexes' may contain contact information for foreign political or military leaders, to include direct line, fax, residence and cellular numbers." The Guardian approached the Obama administration for comment on the latest document. Officials declined to respond directly to the new material, instead referring to comments delivered by Carney at Thursday's daily briefing. Carney told reporters: "The [NSA] revelations have clearly caused tension in our relationships with some countries, and we are dealing with that through diplomatic channels. "These are very important relations both economically and for our security, and we will work to maintain the closest possible ties."" The public accusation of spying on Merkel adds to mounting political tensions in Europe about the scope of US surveillance on the governments of its allies, after a cascade of backlashes and apologetic phone calls with leaders across the continent over the course of the week. Asked on Wednesday evening if the NSA had in the past tracked the German chancellor's communications, Caitlin Hayden, the White House's National Security Council spokeswoman, said: "The United States is not monitoring and will not monitor the communications of Chancellor Merkel. Beyond that, I'm not in a position to comment publicly on every specific alleged intelligence activity." At the daily briefing on Thursday, Carney again refused to answer repeated questions about whether the US had spied on Merkel's calls in the past. The NSA memo seen by the Guardian was written halfway through George W Bush's second term, when Condoleezza Rice was secretary of state and Donald Rumsfeld was in his final months as defence secretary. Merkel, who, according to Reuters, suspected the surveillance after finding her mobile phone number written on a US document, is said to have called for US surveillance to be placed on a new legal footing during a phone call to President Obama. "The [German] federal government, as a close ally and partner of the US, expects in the future a clear contractual basis for the activity of the services and their co-operation," she told the president. The leader of Germany's Green party, Katrin Göring-Eckhart, called the alleged spying an "unprecedented breach of trust between the two countries. Earlier in the week, Obama called the French president François Hollande in response to reports in Le Monde that the NSA accessed more than 70m phone records of French citizens in a single 30-day period, while earlier reports in Der Spiegel uncovered NSA activity against the offices and communications of senior officials of the European Union. The European Commission, the executive body of the EU, this week backed proposals that could require US tech companies to seek permission before handing over EU citizens' data to US intelligence agencies, while the European parliament voted in favour of suspending a transatlantic bank data sharing agreement after Der Spiegel revealed the agency was monitoring the international bank transfer system Swift.

NSA overreach undermines counter-terror operations- international cooperation is key

Riechmann 13 (Deb, journalist for the Associated Press. "NSA Spying Threatens U.S. Foreign Policy Efforts" www.huffingtonpost.com/2013/10/26/nsa-spying-foreign-policy_n_4166076.html)

Secretary of State John Kerry went to Europe to talk about Mideast peace, Syria and Iran. What he got was an earful of outrage over U.S. snooping abroad. President Barack Obama has defended America's surveillance dragnet to leaders of Russia, Mexico, Brazil, France and Germany, but the international anger over the disclosures shows no signs of abating in the short run. Longer term, the revelations by former National Security Agency contractor Edward Snowden about NSA tactics that allegedly include tapping the cellphones of as many as 35 world leaders threaten to undermine U.S. foreign policy in a range of areas. This vacuum-cleaner approach to data collection has rattled allies. "The magnitude of the eavesdropping is what shocked us," former French Foreign Minister Bernard Kouchner said in a radio interview. "Let's be honest, we eavesdrop too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous." So where in the world isn't the NSA? That's one big question

raised by the disclosures. Whether the tapping of allies is a step too far might be moot. The British ambassador to Lebanon, Tom Fletcher, tweeted this past week: "I work on assumption that 6+ countries tap my phone. Increasingly rare that diplomats say anything sensitive on calls." Diplomatic relations are built on trust. If America's credibility is in question, the U.S. will find it harder to maintain alliances, influence world opinion and maybe even close trade deals. Spying among allies is not new. Madeleine Albright, secretary of state during the Clinton administration, recalled being at the United Nations and having the French ambassador ask her why she said something in a private conversation apparently intercepted by the French. The French government protested revelations this past week that the NSA had collected 70.3 million French-based telephone and electronic message records in a 30-day period. Albright says Snowden's disclosures have hurt U.S. policymakers. "A lot of the things that have come out, I think are specifically damaging because they are negotiating positions and a variety of ways that we have to go about business," Albright said at a conference hosted by the Center for American Progress in Washington. "I think it has made life very difficult for Secretary Kerry. ... There has to be a set of private talks that, in fact, precede negotiations and I think it makes it very, very hard." The spy flap could give the Europeans leverage in talks with the U.S. on a free trade agreement, which would join together nearly half of the global economy. "If we go to the negotiations and we have the feeling those people with whom we negotiate know everything that we want to deal with in advance, how can we trust each other?" asked Martin Schulz, president of the European Parliament. Claude Moniquet, a former French counterintelligence officer and now director of Brussels-based European Strategic Intelligence and Security Center, said the controversy came at a good time for Europe "to have a lever, a means of pressure ... in these negotiations." To Henry Farrell and Martha Finnemore at George Washington University, damage from the NSA disclosures could "undermine Washington's ability to act hypocritically and get away with it." The danger in the disclosures "lies not in the new information that they reveal but in the documented confirmation they provide of what the United States is actually doing and why," they wrote in Foreign Affairs. "When these deeds turn out to clash with the government's public rhetoric, as they so often do, it becomes harder for U.S. allies to overlook Washington's covert behavior and easier for U.S. adversaries to justify their own." They claim the disclosures forced Washington to abandon its "naming-and-shaming campaign against Chinese hacking." The revelations could undercut Washington's effort to fight terrorism, says Kiron Skinner, director of the Center for International Relations and Politics at Carnegie Mellon University. The broad nature of NSA surveillance goes against the Obama administration's claim that much of U.S. espionage is carried out to combat terrorism, she said. "If Washington undermines its own leadership or that of its allies, the collective ability of the West to combat terrorism will be compromised," Skinner said. "Allied leaders will have no incentive to put their own militaries at risk if they cannot trust U.S. leadership." The administration asserts that the U.S. is amassing intelligence of the type gathered by all nations and that it's necessary to protect the U.S. and its allies against security threats. Kerry discussed the NSA affair in Europe with French and Italian officials this past week. Most governments have not retaliated, but some countries are pushing back. Germany and France are demanding that the administration agree by year's end to new rules that could mean an end to reported American eavesdropping on foreign leaders, companies and innocent citizens. Brazilian President Dilma Rousseff canceled her official state visit to the White House. She ordered measures aimed at greater Brazilian online independence and security after learning that the NSA intercepted her communications, hacked into the state-owned Petrobras oil company's network and spied on Brazilians. Brazil says it is working with other countries to draft a U.N. General Assembly resolution that would guarantee people's privacy in electronic communications. A European Parliament committee approved rules that would strengthen online privacy and outlaw the kind of data transfers the U.S. is using for its spying program. European lawmakers have called for the suspension of an agreement that grants U.S. authorities access to bank data needed for terrorism-related investigations. "We need trust among allies and partners," said German Chancellor Angela Merkel, whose cellphone was allegedly tapped by the NSA. "Such trust now has to be built anew."

U.S. – E.U. cooperation key for counter-terrorism

Mix 15 (Derek E. , Analyst in European Affairs “The United States and Europe: Current Issues,” <https://www.fas.org/sgp/crs/row/RS22163.pdf> , February 3)

The United States and European countries have been cooperating in efforts to counter the Islamic State and seek a political solution to the conflict in Syria. Recent estimates suggest that upward of 3,000 European citizens have traveled to Syria and Iraq to join groups involved in the conflict, and the potential threat posed by returning “foreign fighters” has become a central concern. U.S.-EU counterterrorism cooperation has been strong since 9/11, although differences regarding data privacy have posed some key information-sharing challenges. The United States and Europe remain central actors in negotiations seeking to reach an agreement that ensures that Iran’s nuclear program can be used solely for peaceful purposes. While an extensive array of U.S. and EU sanctions have worked to isolate and pressure Iran, the final outcome of talks remains uncertain. • The United States and EU share broad objectives with regard to resolving the Israeli-Palestinian conflict. Increased European support for recognizing Palestinian statehood, however, has diverged from the approach taken by the United States and strained Europe’s relationship with Israel. • The United States and the EU have the largest trade and investment relationship in the world. The two sides have been negotiating a free trade agreement, the Transatlantic Trade and Investment Partnership (TTIP) aimed at boosting jobs and growth on both sides, but obstacles could make it difficult to conclude a deal by the end of 2015. While the conditions that fueled the Eurozone crisis from 2010-2012 appear to have stabilized, there is considerable doubt that underlying economic problems in Europe have been fully resolved. • Allegations of U.S. spying and surveillance programs in Europe have caused a sharp backlash and damaged transatlantic trust. Although tensions appear to have proven manageable and U.S. intelligence cooperation with European governments continues, data privacy concerns could complicate future talks on U.S.-EU information-sharing agreements. The United States takes over the chairmanship of the Arctic Council in May 2015. The Arctic is increasingly viewed as a region of potential economic and geopolitical importance. As the United States and Europe face a changing geopolitical environment, some observers assert that the global influence of the Euro-Atlantic partnership is in decline. In addition, the Obama Administration’s announced intention of “re-balancing” U.S. foreign policy toward Asia has caused some anxiety among Europeans. Overall, however, most analysts maintain that the United States and Europe are likely to remain one another’s closest partner, and that U.S.-European cooperation is likely to remain the foundation of international action on a wide range of critical issues.

US-EU cooperation is key to stopping terror

Mix, 2015 (Derek E. , Analyst in European Affairs “The United States and Europe: Current Issues,” <https://www.fas.org/sgp/crs/row/RS22163.pdf> , February 3)

Overall, in the years since the 9/11 attacks, transatlantic cooperation on counterterrorism has been strong. U.S. and European officials from the cabinet level down maintain regular dialogues on issues related to homeland security and counterterrorism. In 2010, new U.S.-EU treaties on extradition and mutual legal assistance entered into force. The United States and the EU have also reached agreements on container security and sharing airline passenger data as part of their efforts to strengthen aviation, transport, and border security. In addition, the United States and the EU actively work together to track and counter the financing of terrorism, in forums such as the Financial Action Task Force and through information sharing deals such as the U.S.-EU “SWIFT agreement,” which allows U.S. authorities access to financial data held by a Belgium-based consortium of international banks as part of the U.S. Treasury Department’s Terrorist Finance Tracking Program (TFTP). While the EU has been increasing its relevance in this area, bilateral intelligence sharing and law enforcement cooperation between the United States and individual European countries also remains key to disrupting terrorist plots and apprehending those involved. Although overall counterterrorism cooperation is strong, areas of tension exist. European policy makers have had significant concerns over the adequacy of data privacy safeguards in a number of U.S.-EU information-sharing arrangements. The EU considers data privacy a basic right and has strict regulations protecting personal data. During the past several years, objections raised in the European Parliament complicated and delayed the adoption of the most recent version of the SWIFT deal and the

agreement on sharing airline passenger name record (PNR) data. The United States and the EU have been negotiating a framework Data Privacy and Protection Agreement (DPPA) since 2011. Over the past decade, the United States and the EU have largely aligned their lists of entities designated as terrorist organizations. In July 2013, the EU added Hezbollah's military wing to its terrorist list, a move welcomed as a positive step by U.S. officials. Successive U.S. Administrations and many Members of Congress have long urged the EU to include Hezbollah on its common terrorist list. Critics contend, however, that listing only Hezbollah's military wing is insufficient because Hezbollah is still allowed to fundraise in Europe and there is no meaningful distinction between Hezbollah's political and military wings. In December 2014, the General Court of the European Union ruled that Hamas should be removed from the EU's common list of designated terrorist organizations on procedural grounds related to the decision-making process used in adding the group to the list over a decade ago. The EU External Action Service responded that the ruling was not a political or substantive decision made by EU governments, and that restrictive measures against Hamas will remain in place as an appeal process goes forward. The United States and Israel both urged the EU to maintain its sanctions against Hamas.

Emerging Powers Cooperation

NSA overreach hurts cooperation with emerging powers- that's key to global security efforts

Lewis , Director of CSIS, 15 (James, Director And Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies, Senate Foreign Relations Subcommittee on East Asia, the Pacific and International Cybersecurity Policy Hearing: [1], March 14. "Cybersecurity: Setting The Rules For Responsible Global Cyber Behavior.", proquest, http://www.foreign.senate.gov/imo/media/doc/051415_REVISED_Lewis_Testimony.pdf)

Dealing with these countries also requires a broad diplomatic strategy to win support from key allies and from emerging new powers, like Brazil, India and others. These new powers from a middle ground between western democracies and authoritarian regimes, and the policies these countries choose to pursue will determine the future of the internet and cybersecurity. Most of the new powers support fundamental human rights, and in particular freedom of speech and free access to information. This puts them at odds with the authoritarian view of cyberspace, but they also believe that national sovereignty and government must play a larger role in internet matters, and they were troubled by the NSA revelations, factors that work against U.S. influence. To win the global support, the U.S. needs persuasive arguments on privacy, internet governance, and the use of force in cyberspace. We do not now have these persuasive arguments and some of what we say now about the internet is seen as duplicitous. The NSA leaks of the last two years, whose selective release is used intentionally to damage the U.S., have not helped us. Cybersecurity is a military and intelligence contest with dangerous opponents. There are significant trade issues. The internet has immense political effect that threatens authoritarian regimes and has led them to mount significant challenges to market and democratic ideals and the international institutions created to support them. The focal point of this challenge is to reduce U.S. influence, not just over the internet but also in trade, security, and finance. We face a determined effort to dismantle American leadership in international affairs.

Cooperation with emerging powers is key to counter-terror efforts

Jones 11 (Bruce, director and senior fellow at the NYU Center on Int'l Cooperation and Senior fellow at the Brookings Institution. "Beyond Blocs: The West, Rising Powers, and Interest-Based International Cooperation. October.

www.stanleyfoundation.org/publications/pab/jonespab1011b.pdf

The first pattern worth observing here is the sustained intensive cooperation since 9/11 between the United States, Russia, India, China, and myriad other states on combating Al Qaeda and other forms of terrorism. At times, this cooperation took the ugly form of a "you kill your terrorists and we'll kill ours" compact. The fissure in this sphere was not between the United States and the emerging powers; far from it. Instead, the public split was between the United States and Europe over the question of the application of international legal and human rights standards in the counterterrorist endeavor. This is not to say that the United States and the emerging powers agreed or agree on all things terrorist. Indeed, the political/ideological dispute over whether Palestinian nonstate actors are engaged in terrorism or resistance continues unabated at the United Nations—but that issue divides the United States as much from Europe as it does from the emerging powers. Operationally, though, intelligence sharing and political backing for counterterrorist moves has been remarkably steady between the United States, Russia, and the emerging powers. This is unsurprising. Terrorism poses simultaneous both to sovereign security as well as to the very infrastructural networks on which globalization depends, and the United States and the emerging powers share profound interests in protecting both.

India Cooperation

Domestic surveillance hurts US-Indian cooperation

Burke 13 (Jason, south Asia correspondent, The Guardian. 9/25.

www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission)

The US National Security Agency may have accessed computers within the Indian embassy in Washington and mission at the United Nations in New York as part of a huge clandestine effort to mine electronic data held by its south Asian ally. Documents released by the US whistleblower Edward Snowden also reveal the extent and aggressive nature of other NSA datamining exercises targeting India as recently as March of this year. The latest revelations – published in the Hindu newspaper – came as Manmohan Singh, the Indian prime minister, flew to Europe on his way to the US, where he will meet President Barack Obama. The NSA operation targeting India used two datamining tools, Boundless Informant and Prism, a system allowing the agency easy access to the personal information of non-US nationals from the databases of some of the world's biggest tech companies, including Apple, Google, Microsoft and Yahoo. In June, the Guardian acquired and published top-secret documents about Boundless Informant describing how in March 2013 the NSA, alongside its effort to capture data within the US, also collected 97bn pieces of intelligence from computer networks worldwide. The largest amount of intelligence was gathered from Iran, with more than 14bn reports in that period, followed by 13.5bn from Pakistan. Jordan, one of America's closest Arab allies, came third with 12.7bn, Egypt fourth with 7.6bn and India fifth with 6.3bn. Though relations between India and the US were strained for many decades, they have improved considerably in recent years. President George Bush saw India as a potential counterweight to China and backed a controversial civil nuclear agreement with Delhi. Obama received a rapturous welcome when he visited in 2010, though concrete results of the warmer relationship have been less obvious. According to one document obtained by the Hindu, the US agency used the Prism programme to gather information on India's domestic politics and the country's strategic and commercial interests, specifically categories designated as nuclear, space and politics. A further NSA document obtained by the Hindu suggests the agency selected the office of India's mission at the UN in New York and the country's Washington embassy as "location targets" where records of Internet traffic, emails, telephone and office conversations – and even official documents stored digitally – could potentially be accessed after programs had been clandestinely inserted into computers. In March 2013, the NSA collected 6.3bn pieces of information from internet networks in India and 6.2bn pieces of information from the country's telephone networks during the same period, the Hindu said. After the Guardian reported in June that Pm program allowed the NSA "to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders", both US and Indian officials claimed no content was being taken from the country's networks and that the programs were intended to aid "counter-terrorism". Syed Akbaruddin, an external affairs ministry spokesperson, said on Wednesday there was no further comment following the latest revelations. Siddharth Varadajaran, editor of the Hindu, said the Indian government's "remarkably tepid and even apologetic response to the initial set of disclosures" made the story a "priority for Indians". A home ministry official told the newspaper the government had been "rattled" to discover the extent of the the programme's interest in India. "It's not just violation of our sovereignty, it's a complete intrusion into our decision-making process," the official said. Professor Gopalapuram Parthasarathy, a former senior diplomat, said no one should be surprised by the Hindu's story.

"Everybody spies on everyone else. Some just have better gadgets. If we had their facilities, I'm sure we would do it too. The US-Indian relationship is good and stable and if they feel India merits so much attention then good for us," he told the Guardian. Others have been less phlegmatic. Gurudas Dasgupta, a leader of the Indian Communist party, asked the government to raise the issue with Obama. Anja Kovacs of the Delhi-based Internet Democracy Project said the articles showed that such datamining was not about any broader "struggle to protect society as a whole through something like fighting terrorism, but about control". The Hindu argued that "the targeting of India's politics and space programme by the NSA busts the myth of close strategic partnership between India and US", pointing out that the other countries targeted in the same way as India "are generally seen as adversarial" by Washington.

Improved US-Indian security cooperation is key to fighting terrorism

Panda 14 (Ankit, 10/2. Ankit Panda is a foreign affairs analyst, writer, and editor with expertise in international relations, political economy, international security, and crisis diplomacy. He has been an editor at The Diplomat since 2013. thediplomat.com/2014/10/10-takeaways-on-us-india-security-cooperation/)

7. The statement understandably has a broad focus on countering terror groups in South Asia and elsewhere. The statement mentions the Islamic State, Al Qaeda, Lashkar-e-Taiba, the Haqqani Network, Jaish-e-Mohammed, and the D-Company. The statement was relatively specific on areas of U.S.-India cooperation on counter-terrorism, highlighting the “dismantling of safe havens for terrorist and criminal networks, to disrupt all financial and tactical support for networks.” Furthermore, the statement identifies areas for growth in bilateral cooperation on criminal law enforcement, military information exchange, and legal cooperation — all areas where considerable lacunae exist in Indo-U.S. security ties. In the context of cooperation in these areas, the statement mentions interdicting terrorist activities in cyberspace — an area of concern for both countries.

China Cooperation

Surveillance overreach hurts US-Chinese tech cooperation

Song 13 (Sophie, Sophie is a graduate of Northwestern University. She covers the emerging markets in Southeast Asia, with a particular interest in foreign investment in the region. “Growing Chinese Animosity Following PRISM Revelations Could Threaten Tech Firms’ Prospects In World’s No. 2 Economy,” <http://www.ibtimes.com/growing-chinese-animosity-following-prism-revelations-could-threaten-tech-firms-prospects-worlds-no>, July 19)

Edward Snowden’s revelations about the U.S. government’s PRISM surveillance program have triggered a backlash against American technology firms that threatens their growth in the world’s second-largest economy. Following Snowden’s exposure of PRISM Chinese authorities and the public have become increasingly worried about exposure to U.S. technology and equipment, according to a note published on Thursday by the Rhodium Group (RHG), a New York-based advisory firm that frequently provides business insights related to China. When the leak of PRISM hit Chinese media in early June, two major storylines emerged. The first accused the U.S. of operating under double standards – the U.S. government was monitoring other nations, companies and individuals, while accusing China and Chinese companies like Huawei Technology Co Ltd (SHE:002502) and ZTE Corporation (SHE:000063) of aiding the Chinese government in conducting espionage, as PRISM proved. The other headline, far more threatening to U.S. and other foreign businesses, according to RHG, is what the state-run media termed a “de-Cisco campaign.” The state-backed China Economic Weekly ran a cover story calling eight U.S. companies – Cisco Systems, Inc. (NASDAQ:CSCO), International Business Machines Corp. (NYSE:IBM), Google Inc. (NASDAQ:GOOG), QUALCOMM (NASDAQ:QCOM), Intel Corporation (NASDAQ:INTC), Apple Inc. (NASDAQ:AAPL), Oracle Corporation (NYSE:ORCL) and Microsoft Corporation (NASDAQ:MSFT) – the eight “guardian warriors” that had “seamlessly penetrated” Chinese society. The weekly newspaper called Cisco “the most horrible”, given its over 50 percent market share in China’s information infrastructure in financial, military, government and transportation sectors. In the past, comparative advantage in IT innovation has made U.S. equipment suppliers’ products more popular than those of Chinese suppliers, but if recent rhetoric is any indication that popularity may end in the near future. The Chinese government has already spent massive sums developing its own supercomputers and satellite navigation systems, and now Chinese officials seem to think Chinese companies like Huawei and ZTE, the very companies that have been repeatedly suspected of espionage in the west, are mature enough to replace Cisco, Microsoft and IBM. This could be bad news for both sides. China is a fast-growing market and a large contributor to these tech companies’ overall revenue. If the campaign against American companies gains traction these firms could see their market share dwindle. Last year, following the House report warning Huawei may pose a security risk, Unicom, China’s leading telecom operator, replaced Cisco routers in one of its backbone networks, citing security concerns. Other similar replacements may happen in the future. The effects could even trickle down to other U.S. firms, in particular those firms in supplying the tech giants. Cisco’s equipment and network is too widespread in China to be eliminated completely in the short term, if ever. Any policy like the de-Cisco campaign would almost certainly damage China’s economic and security interests, by radicalizing foreign trading partners who may be less willing to engage positively with China across a wider portfolio of interests, according to RHG’s research note. Now most of the back and forth remains rhetoric, but Beibei Bao, a New York-based China analyst at Rhodium Group and the author of the report, believes the situation will likely escalate. China will not drop the issue without further investigation, and as such, the fates of American firms under suspicion in uncertain at best. “The situation for the American technology firms in China is not very clear right now.” Bao said. We don’t think Huawei and other Chinese firms can replace the technology 100 percent, but when the issue concerns national security, China is unlikely to back down.”

Cooperation necessary between US – China to stop terrorism

deLeon and Jiemian 14 (Rudy - Secretary of Defense for Clinton’s administration, and Yang – Professor, ph.D in political science ,“U.S.-China Relations Toward a New Model of Major Power Relationship,” <https://www.americanprogress.org/wp-content/uploads/2014/02/ChinaReport-Full.pdf> ,February)

Officials and experts in both countries need a more effective dialogue with their citizens on the importance of the U.S.-China relationship and what newmodel relations exercise is designed to prevent and achieve. There are many positive stories of workaday Sino-American cooperation that do not make the mainstream press and are therefore not known to the public —and in some cases to key political leaders, particularly at the local level. For example, the American and Chinese Coast Guards cooperate frequently and effectively on an operational level, but that kind of operational cooperation is not as likely to attract media attention as bilateral flare-ups on sensitive issues. As one Chinese participant in our dialogues pointed out, we should seek to increase the attention paid to the positive attributes of the relationship that can shift the focus from “crisis management” to “opportunity management.” There are many areas of cooperation that could be expanded, including counterpiracy efforts; U.N. peacekeeping operations, or UNPKO; joint humanitarian, disaster-relief, and search-and-rescue exercises; multilateral military exercises or exercises hosted by third countries; professional military educational exchanges; maritime law enforcement; fisheries protection; taking steps to counter nuclear proliferation; and international terrorism. To build up a NMMPR is also in the common interests of regional and global order in transition. Both China and the United States are two key players with systematic influence on the international order in transition. A constructive bilateral relationship is the foundation of effective cooperation on both regional and global levels. On the one hand, if these two countries are able to work together, they can play a leading role in global and regional governance through coordinated policies on climate change, economic and financial governance, energy security, anti-global poverty and sustainable development, nonproliferation and international counterterrorism, and other global and regional challenges. On the other hand, neither bilateral confrontation nor G-2 would be welcomed by the international community as other members will either have to choose the side or worry about their respective national interests that would be jeopardized. For the collective interests of international community, a stable and healthy China-U.S. relationship based upon mutual respect and win-win cooperation could contribute to peace, security, and prosperity around the world.

Restoring confidence in protection of domestically held data is critical to Chinese perceptions

SHAHANI, 2014 (AARTI ,Aarti Shahani is a Tech Reporter on NPR's Business Desk, where she covers breaking news, and does investigative and enterprise reporting.“A Year After Snowden, U.S. Tech Losing Trust Overseas,”<http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas>, June 5)

This week marks the one-year anniversary of the Snowden revelations. Whatever you may think about Edward Snowden’s the man — is he a traitor or a hero? — one fact is indisputable. His leaks shook the world technology industry to its core. And the reverberations keep on coming. Take Cisco. The Silicon Valley giant is now at risk of losing its once-stellar reputation with foreign customers — at the exact same moment it needs to grow abroad. Security Worries For The Cloud Cisco is one of the companies that connect us to the cloud, by making routers and switches. About half of its business is abroad, and every year Cisco throws an event for its customers. The latest one was a concert by rock legend Lenny Kravitz. He performed at AT&T Park in San Francisco and, between the crowd’s cheers, he complained about the weather. "It's cold here. I live in the Bahamas." Many in the audience came from much farther away. In fact, 25,000 high-powered executives from around the world flew into town. To keep growing, Cisco needs the trust of these foreign customers. The Snowden revelations don’t help. Take one man I randomly bump into, Elly Resende from Brazil. He is responsible for the technology for staging the 2016 Olympic Games in Rio. He’s the kind of guy who dives headfirst into the newest gadgets and gear. "I'm like a freak with ... I like technology a lot," he says. But this past year, he hit the brakes on a hot trend: cloud computing. That’s when you put data online, in servers that can be outside your own country. Mike Janke is the chief executive officer of Silent Circle, a company that sells privacy devices and apps. ALL TECH CONSIDERED A Privacy Capitalist Wins Big After Snowden Cisco provides cloud services and was putting them on display prominently at the conference. Resende is a client who is skeptical. While he likes the convenience of accessing data from anywhere, he’s worried about security — especially with data that is valuable to the competition, like athletes’ training results. "This is a concern especially after the Snowden thing," he says. "How do you guarantee that your data is accessed only by you? Who else has the same access to the information that you produce, you think you control?" Plenty Of Questions From Customers Cisco hears such concerns all over the world. "I think it's been pretty universal outside of the U.S.," says Christopher Young, Cisco senior vice president of security. "So you can go to Latin America, you can go to Europe, to Asia, and there's many examples of customers asking those questions." The very first

Snowden revelation — which was about the National Security Agency spying on phone calls — did not rock the high-tech industry. But the news bomb that came one day later, about a program called PRISM, did. The U.S. was tapping directly into the central servers of nine leading Internet companies including Microsoft, Yahoo, Google, Facebook and Apple. The journalist who broke the Snowden story, Glenn Greenwald, published a picture of a Cisco router allegedly intercepted in the mail, taken out of the box and tampered with by the NSA.ⁱ The journalist who broke the Snowden story, Glenn Greenwald, published a picture of a Cisco router allegedly intercepted in the mail, taken out of the box and tampered with by the NSA. No Place to Hide / Metropolitan Books Suddenly cloud computing could be a platform for mass surveillance. American tech companies could be working hand-in-hand with their government, and foreign clients would not get the memo. Young says the revelations have shaken customer confidence: "People say, 'Hey, we've known Cisco for a long time. We know we trust you guys. But given what's going on, how much can we really trust you?'" The answer is a moving target because the revelations keep on coming. Recently Cisco got caught in the cross hairs. The journalist who broke the Snowden story, Glenn Greenwald, published a picture of a Cisco router allegedly intercepted in the mail, taken out of the box and tampered with by the NSA. Another progressive journalist, Amy Goodman, asked Greenwald about it on her show Democracy Now: "So they get the Cisco router — with the knowledge or without the knowledge of Cisco?" Greenwald responded, "It's unclear." "More Shoes To Drop?" Cisco says it was not aware of its routers being hacked. And CEO John Chambers wrote an open letter to President Obama, telling him that the actions, if true, "undermine confidence in our industry." Chambers also urged standards of conduct that meet national security objectives without jeopardizing business interests. It's not every day that an industry in hypergrowth loses trust with its customers in a big way. Andrew Bartels, with Forrester Research, studies cloud computing. "At this point, we don't know which direction it's going to take," he says. "Is everything out? Or [are] there still more shoes to drop?" By his estimate, a sector that hardly existed five years ago will be worth \$191 billion by 2020. But that big number, he says, hides the rates at which different countries are moving to the cloud, and new resistance to that move. "You found in Europe, Germany in particular, companies putting those plans on the shelf because of the privacy issues." Bartels says. According to a study by German high-tech association Bitkom, cloud use grew just 3 percent in 2013, compared with a 9 percent increase in 2012. When Brazilian President Dilma Rousseff found out her emails were monitored by the NSA, she called for an end to the unquestioned use of U.S.-based servers. Bartels says, "That in turn has cascaded through the Brazilian government, which does still own a certain large portion of the economy." And businesses are realizing that cloud computing exposes them to new levels of domestic spying, Bartels says. "In markets like China's or like Russia, I think the issue here is concerns in the private sector about giving business information to the government," he says. In this messy landscape, Cisco is losing ground. In its last quarterly earnings call, the company reported that orders from emerging countries fell 7 percent — down 27 percent in Brazil alone, 8 percent in China and 28 percent in Russia. The company and its Silicon Valley competitors are now retooling services, trying to rebuild trust — or offer more secure products.

Tech Companies Cooperation

Cooperation between Government surveillance and the private industry is key to breaking down terrorism- the plan is key to restoring trust necessary to effective surveillance

Michaels, J.D. 08 (Don Michaels: J.d. from Yale, Prof at UCLA Law School “All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror” California Law Review: Vol. 96, No. 4 (Aug., 2008), pp. 901-966, <http://www.jstor.org/stable/20441037> (pg. 901))

Unable to target or repel terrorists using conventional military tactics and munitions alone, the United States is acutely aware that today's pivotal battlefield is an informational one. Teams of U.S. intelligence agents, acting as eavesdroppers, infiltrators, interrogators, and data-miners, must race against the clock to anticipate terrorists' actions, frustrate their missions, and dismantle their infrastructure.' Because the U.S. government does not know the who, what, where, and when of the next terrorist strike, but recognizes that the plot might be hatched on domestic soil, its first step must be to cast a wide net to gather all sorts of data points, any one of which might be the clue that leads intelligence agents to prevent another September 11-like catastrophe.³ In this regard, there is no better ally than the private sector. Its comparative advantage over the government in acquiring vast amounts of potentially useful data is a function both of industry's unparalleled access to the American public's intimate affairs-access given by all those who rely on businesses to facilitate their personal, social, and economic transactions-and of regulatory asymmetries insofar as private organizations can at times obtain and share information more easily and under fewer legal restrictions than the government can when it collects similar information on its own.

Cooperation with private companies allows access to a wider data set which prevents terror

Michaels, J.D. 08 (Don Michaels: J.d. from Yale, Prof at UCLA Law School “All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror” California Law Review: Vol. 96, No. 4 (Aug., 2008), pp. 901-966, <http://www.jstor.org/stable/20441037> (pg. 908))

Technological advances and the concomitant universal reliance on such innovations to communicate and to conduct personal and business transactions electronically have generated an unprecedented number of data points about individuals who use email, surf the web, speak via telephone, wire money, bank, travel commercially, and transact business via the Internet.¹⁸ All of the information about particular electronic transactions (and all of the background details people supply to subscribe to shopping or frequent-traveler membership clubs or to gain access to websites' content) is possessed in large measure by private firms involved in commerce, finance, and telecommunications.¹⁹ With high-powered computers and increasingly sophisticated software,²⁰ analysts can mine these stores of data and detect particularly significant patterns of behavior, including activities ostensibly indicative of terrorist planning. People simply do not interface with the government in the same ways or with the same frequency as they do with the

private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources.²

Cooperation solves-Private data regulations are less restricted, leading to an increase in available data

Michaels, J. D, 08 (Don Michaels: J.d. from Yale, Prof at UCLA Law School “All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror” California Law Review: Vol. 96, No. 4 (Aug., 2008), pp. 901-966, <http://www.jstor.org/stable/20441037> (pg. 908-909))

Coupled with the private sector's attractiveness as a convenient repository of information is its legal allure, notably in instances when private data gathering is subject to less stringent regulation than what the government faces. That is, federal law-enforcement and intelligence-gathering offices (along with, for example, health and labor departments) are at times comparatively hamstrung in their direct ability to collect and catalog private, personal information about U.S. persons.²³ The reasons for this asymmetry include legislative happenstance, consumer convenience, and the assumption that private businesses can do less "harm" with personal information than the government can. But if the government can convince private businesses to share their data collections, it can make an end-run around the more stringent restrictions limiting its ability to access information directly.

Private Sector cooperation is key to prevent terror

Wiktorowicz and Amanullah 15 (Quintan Wiktorowicz is a PhD from Cornell. He served as senior adviser for technology at the Department of State from 2011-2014, “How tech can fight extremism” Published: Feb 17, 2015, <http://www.cnn.com/2015/02/16/opinion/wiktorowicz-tech-fighting-extremism/>)

Violent extremists like the self-proclaimed Islamic State of Iraq and Syria, or ISIS, have become increasingly sophisticated at creating dense, global networks of support online, networks that are helping these groups run virtual circles around governments and communities. And it is activities like these that have raised a disturbing prospect, one that has serious implications for fighting extremism: We could lose the information war. It's with this troubling reality in mind that the Obama administration will this week hold a Summit on Countering Violent Extremism, where it will underscore the importance of technology companies in the fight against terrorist recruitment. This is critical. As Robert Hannigan, director of Britain's Government Communications Headquarters (the National Security Agency's sister organization), emphasized, technology companies' services "have become the command-and-control networks of choice for terrorists." ISIS, in particular, has proven virulent in using technology to radicalize. It has mobilized armies of online followers to engage audiences in ways that take advantage of the decentralized and open nature of the Internet, leveraging online tools such as Twitter, Facebook, Ask.fm, Kik, SoundCloud and Instagram, to name just a few. Indeed, in a single day this past summer, ISIS supporters sent out some 40,000 tweets, and supporters often repetitively tweet specific hashtags at particular times of day to maximize message trending. ISIS also has strategically run hashtag campaigns to tap into trending topics on Twitter, such as the World Cup and Ebola, which have nothing to do with violent extremism. ISIS-linked extremists have used social media to focus group messages, disseminate ideological simulator games, and broadcast high production videos, and the group has created its own technologies, including a smartphone app released last year that amplifies its messaging campaigns. Governments are struggling to keep up. How should they

respond? For a start, they need to leverage the talent, creativity and capabilities of the private sector. Yet involving technology companies in countering extremism will be challenging. True, the U.S. government has been engaging Google, Twitter, Facebook and other large companies on the problem since at least 2008. But while this has generated a few initiatives, such as social media training for Muslim Americans and the Network Against Violent Extremism online network catalyzed by Google Ideas, we have yet to see the scale of involvement required for strategic impact. Part of the challenge is that, although large companies clearly want to help, they have to navigate complicated priorities that distinguish them from governments, such as shareholders, profits, brands and market forces. Just as importantly, these high-profile companies could face real safety risks. When Twitter shut down ISIS-affiliated accounts last year, for example, a prominent ISIS supporter called for the assassination of Twitter employees. Given recent attacks in Paris and Sydney, these kinds of threats are chilling. The Obama administration will therefore need to figure out how to help companies navigate the inherent risks of the private sector countering violent extremism. One solution is to encourage the involvement of more agile start-ups that are willing to move into niche markets like countering extremist messaging. These companies are lean, hungry and less encumbered by the risk calculations that circumscribe large companies. Moreover, the start-up community is increasingly emphasizing social impact as a core business imperative, and this trend likely will accelerate as more millennials start new businesses. Interestingly, research shows that millennials place a premium on investments that generate positive social impact. Just as importantly, the counter-extremism "marketplace" is in many ways better suited to small, flexible businesses than large companies. Radicalization is driven by a host of different factors (such as identity crises, a sense of disempowerment, a desire for adventure, and even misguided idealism), each of which represents a potential business opportunity. Large companies may not be interested in addressing these market needs if it takes them away from their core products and services, leaving room for a constellation of specialized start-ups. The Muslim youth market, in particular, is experiencing immense political, cultural and religious transformations, and many large companies are nervous about the volatility. As a result, the 500 million-strong Muslim youth market is woefully underserved. Start-ups, especially those from within Muslim communities, may be better positioned and motivated to address Muslim youth needs in a way that helps counter radicalization. At the White House Summit, the President will likely call on technology companies for help, and we encourage the administration to involve talented and passionate start-ups in addition to brand name companies. This week, to support the summit and facilitate greater private sector involvement, we will launch a specialized start-up incubator (Affinis Labs) and are forming a \$5 million private equity fund for start-ups involved in countering extremism. The reality is that ISIS operates like a mission-driven, agile start-up to spread its evil ideology, and we will not defeat it through government and large corporations alone. America is the vanguard of entrepreneurship and innovation, and there are start-ups ready to heed President Obama's call, including start-ups led by passionate Muslim Americans who are building businesses and social enterprises that challenge violent extremist narratives. We believe firmly that American entrepreneurs are ready to support the fight against radicalization.

Tech companies key to solve terror

Schechner and Gauthier '15 [Sam Schechner and David Gauthier-Villars Feb. 17, 2015 5:11 p.m. ET . Sam is a Europe Tech Correspondent, The Wall Street Journal. Sam covers technology across Europe, based out of the Wall Street Journal's Paris bureau. He has previously served as a French business correspondent and covered the U.S. television industry. Sam has been

a reporter for the Journal since 2005. David Gauthier-Villars is a Deputy Bureau Chief, The Wall Street Journal. Accessed June 25, 2015, “Tech Companies Are Caught in the Middle of Terror Fight” <http://www.wsj.com/articles/tech-companies-are-caught-in-the-middle-of-terror-fight-1424211060>]//JZ WB

French Interior Minister Bernard Cazeneuve heads to Silicon Valley this week to enlist a new force in his fight on terror: U.S. tech giants. Weeks after deadly terror attacks in Paris, and days after apparent copycat shootings in Denmark, France's top cop plans to meet on Friday with senior executives at Apple Inc., Google Inc., Facebook Inc., and Twitter Inc. His message: U.S. tech companies and social networks must do more to rid their services of extremist postings, and should open up encryption to ease government surveillance. “We are facing a new threat,” Mr. Cazeneuve said in an interview ahead of the trip. “We need tech companies to realize that they have an important role to play.” Mr. Cazeneuve’s West Coast tour—coming after a layover Wednesday and Thursday in Washington to attend a summit on terror—raises European pressure on U.S. tech companies over how best to use the Internet to fight terrorists. Executives say it thrusts them into a tricky dilemma—how to support their users’ privacy and free-speech rights while also being tough on terrorism. In Paris and other European capitals, government officials say Islamic State and other insurgencies have succeeded in harnessing social networks to rally scores of young Europeans to their cause, and lure hundreds of converts to the battlegrounds in Syria and Iraq. Online videos showing the beheading of U.S. reporter James Foley and other hostages by Islamic State are terrorism propaganda that must be censored, they say. But until recently, some of the same European governments were assailing some of the same companies for allegedly being overly cooperative with the U.S. National Security Agency, U.S. tech executives say. “Internet companies find themselves caught in the middle,” said Eduardo Ustaran, a privacy lawyer for Hogan Lovells who represents some tech companies. “On one hand, there is a need to make sure these horrible attacks don’t recur. “At a gathering of European law enforcement representatives in Luxembourg last October, U.S. companies including Google, Facebook, Twitter and Microsoft Corp. pledged to help governments. But in meetings since then, the European officials and company representatives have sparred on important issues, such as whether the companies can or should pre-emptively filter their services for terrorist content, or respond only when it is flagged by governments, people familiar with the meetings said. Mr. Cazeneuve, who has dealt with U.S. companies over tax issues during his one-year stint as budget minister until last spring, said he expects them to step up their effort in censoring content that could be regarded as hate speech. “What would be the interest of tech companies in broadcasting hateful images that incite terrorism?” he said. When it comes to terror, U.S. tech executives respond they already cooperate extensively with governments, particularly in emergencies like the ones France and Denmark recently endured, both by removing content from terrorist groups, and by turning over user data. On Jan. 7, when videos proliferated of masked gunmen shooting a French policeman at close range, Google’s YouTube was able to remove copies of the footage in minutes, French officials said. The company says it removed 14 million videos in 2014 for featuring gratuitous violence, incitement to violence or hate speech. That same day, Microsoft says it was able to turn over content from email accounts linked to the Kouachi brothers—suspected of being the killers—within some 45 minutes. The request came through an emergency channel from French prosecutors to the U.S. Federal Bureau of Investigation, Microsoft said. But people within the companies also say that they will only go so far, given the pressure they still feel to fight government surveillance in the wake of the Snowden leaks. “Over the last three years, first

Edward Snowden and now [Islamic State], we have seen the political debate about government access to information swing from one end of the spectrum to the other,” said Rachel Whetstone, Google’s global head of public policy, in a speech to the Bavarian parliament earlier this month. Ms. Whetstone is among the Google executives Mr. Cazeneuve is set to meet on Friday, his office said. One flash point on the agenda is encryption. Politicians and law-enforcement officials in the U.K., France, and U.S. have said that **encrypted communications on apps like Facebook’s WhatsApp or Apple’s new iPhone** pose a problem because companies say they don’t have the ability to unlock them even when they receive valid law-enforcement requests. Mr. Cazeneuve says he plans to push the topic in California. “It is a central issue,” he said. Apple Inc. Chief Executive Tim Cook defended the company’s stance last week, saying weakening privacy controls could “risk our way of life.” Other companies argue that creating back doors to encryption would give a leg up to criminal hackers, and weaken security for all Internet users. “Given most people use the Internet for the reasons it was intended, we shouldn’t weaken security and privacy protections for the majority to deal with the minority who don’t,” said Google’s Mr. Whetstone.

Cooperation Key to Stopping ISIS

US-led international cooperation is key to stop ISIS- unilateral action alone will inevitably fail

Katulis, Lang, and Singh 14 (Brian Senior Fellow at American Progress, Hardin Senior Fellow at American Progress and Vikram Vice President for National Security and International Policy at American Progress, Defeating ISIS: An Integrated Strategy to Advance Middle East Stability. <https://www.americanprogress.org/issues/security/report/2014/09/10/96739/defeating-isis-an-integrated-strategy-to-advance-middle-east-stability/>)

As with efforts to counter extremism elsewhere, defeating ISIS will require a concentrated effort over time. Any successful U.S. strategy must be built on a foundation of regional cooperation that requires coordinated action from U.S. partners—a central concept of the Counterterrorism Partnership Fund that President Barack Obama proposed earlier this year. The strategy will be multifaceted, involving intelligence cooperation, security support, vigorous regional and international diplomacy, strategic communications and public diplomacy, and political engagement. While military action alone will be insufficient to defeat ISIS, the United States and other nations may need to undertake airstrikes and provide military assistance to disrupt and degrade ISIS in Syria. These strikes should be conducted in concert with regional and international partners. Ideally, such airstrikes would receive the support from the United Nations or—absent action to authorize the use of force by the U.N. Security Council—from a coalition of America’s Gulf partners and North Atlantic Treaty Organization, or NATO, allies. As always, the United States should reserve the right to undertake unilateral military action to defend the homeland or protect U.S. personnel from imminent harm. Whether unilaterally or with partners, U.S. military strikes should be limited in terms of scope and duration and under clear oversight of Congress. As CAP said in June when it advocated for action against ISIS in Iraq, “The United States should not undertake military action lightly and should be wary of unintended consequences. But not all military action is the same. Ground troops or invasions to control a country are very different from limited air strikes or targeted assistance to help push back terrorist extremists.” Focusing too much on direct U.S. military action in the fight against ISIS ignores the equally important diplomatic and economic steps that will be required to defeat this extremist group. U.S. military strikes or even boots on the ground cannot defeat ISIS alone and could become a rallying cry and recruitment tool for extremists, repeating one of the most costly strategic errors of the 2003 Iraq War. At the same time, building a unified, committed coalition to effectively degrade ISIS will require intense diplomatic and military leadership from the United States to mobilize and coordinate partners. The United States must leverage its unique capabilities in the military, security assistance, and intelligence arenas. Working together, nations committed to defeating ISIS should take concerted action to empower regional and local forces to fight back against ISIS terrorism.

Arab-American Cooperation

Mass surveillance kills law enforcement coop with US-Arab Americans – that's key to check terror.

Risen '14

(Internally quoting Vanda Felbab-Brown, a senior fellow on foreign policy at the Brookings Institution. Tom Risen is a reporter for U.S. News & World Report. "Racial Profiling Reported in NSA, FBI Surveillance" - U.S. News & World Report - July 9, 2014 - <http://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance>)

The National Security Agency and the FBI have reportedly been overzealous trying to prevent terrorist attacks to the point that anti-Islamic racism in those agencies led to the surveillance of prominent Muslim-Americans, revealing a culture of racial profiling and broad latitude for spying on U.S. citizens. An NSA document leaked by former agency contractor Edward Snowden to reporter Glenn Greenwald shows 202 Americans targeted among the approximately 7,485 email addresses monitored between 2002 and 2008, Greenwald's news service The Intercept reports. To monitor Americans, government agencies must first make the case to the Foreign Intelligence Surveillance Court that there is probable cause that the targets are terrorist agents, foreign spies or "are or may be" abetting sabotage, espionage or terrorism. Despite this filter The Intercept identified five Muslim-Americans with high public profile including civil rights leaders, academics, lawyers and a political candidate. Racial profiling of Muslims by security officers has been a controversy since the terrorist attacks of 2001 spiked fears about al-Qaida trainees preparing more attacks. The New York Police Department has disbanded its unit that mapped New York's Muslim communities that designated surveillance of mosques as "terrorism enterprise investigations" after pressure from the Justice Department about aggressive monitoring by police. A 2005 FBI memo about surveillance procedures featured in The Intercept story uses a fake name "Mohammed Raghead" for the agency staff exercise. This latest report about email surveillance of successful Muslim-Americans is akin to "McCarthyism" that fed paranoia about communist spies during the Cold War, says Reza Aslan, a professor at the University of California, Riverside. The notion that these five upstanding American citizens, all of them prominent public individuals, represent a threat to the U.S. for no other reason than their religion is an embarrassment to the FBI and an affront to the constitution," Aslan says. There is a risk of radicalization among citizens Americans, evidenced by some who have gone to fight jihads in Syria and Somalia, but mass shootings carried out by U.S. citizens of various racial backgrounds occurs much more often, says Vanda Felbab-Brown, a senior fellow on foreign policy at the Brookings Institution. Since 1982, there have been at least 70 mass shootings across the U.S. "We have seen very little domestic terrorism in the U.S.," Felbab-Brown says. This lack of terrorism is due in part to the willingness of the Islamic community to cooperate with law enforcement to identify possible radical threats, out of gratitude that the U.S. is a stable, secure country compared with the Middle East, she says. That could go sour if law enforcement becomes too aggressive, too extreme," she says.

The turn's unique – relations are low now. We also control the vital internal link:

Ramirez '4

(et al; Deborah A. Ramirez, Professor of Law at Northeastern University. She holds a JD from Harvard University, "Developing partnerships between law enforcement and American Muslim, Arab, and Sikh communities: a promising practices guide" (2004). Partnering for Prevention & Community Safety Initiative Publications. Paper 4. <http://hdl.handle.net/2047/d20004127>)

For all these reasons, in a post-September 11th world, it is critical for law enforcement and the Muslim, Arab, and Sikh communities in this country to strengthen their relationships. Historically, these relationships have not existed in any significant way. Prior to September 11th, law enforcement primarily focused their community policing efforts on other communities of color – Latinos, Asians, African-Americans, etc. Similarly, hate crime enforcement efforts mostly focused on crimes against the gay community, Jews, Latinos, Asians and African-Americans. Consequently few state, local or federal law enforcement agencies had any significant contact with the Arab, Muslim, or Sikh

communities prior to September of 2001. It is the premise of the Partnering for Prevention and Community Safety Initiative that Americans will only truly be safe from terrorist attacks when law enforcement agencies adopts a strategy focused on building trust and strengthening relationships with the Muslim, Arab, and Sikh communities. This paradigm is not only more consistent with our constitutional ideals, it also represents our best hope for securing our homeland.

Coop with Arab-American communities is key to solving the war on terror. Ramirez '4

(et al; Deborah A. Ramirez, Professor of Law at Northeastern University. She holds a JD from Harvard University, "Developing partnerships between law enforcement and American Muslim, Arab, and Sikh communities: a promising practices guide" (2004). Partnering for Prevention & Community Safety Initiative Publications. Paper 4. <http://hdl.handle.net/2047/d20004127>)

At the same time law enforcement recognized that the tools used prior to September 11th were inadequate to the new post-September 11th task. Although traditional investigative tools had been useful in achieving a quick and thorough response to September 11th, law enforcement needed enhanced tools to effectively prevent future acts of terror. Specifically, September 11th reinforced the idea that for law enforcement agencies to effectively prevent future acts of terrorism, it would require the cooperation and assistance of the American Muslim, Arab, and Sikh communities. Embedded within these communities are the linguistic skills, information, and cultural insights necessary to assist law enforcement in its efforts to identify suspicious behavior. In order to have access to these critical tools and information, law enforcement recognized the need to build the bridges required for effective communication with these groups.

Arab-American coop is significantly hampered by federal intelligence gathering

Achtenberg '14

(et al; Roberta Achtenberg - currently serves as a Commissioner on the United States Commission on Civil Rights. She served as Assistant Secretary of the U.S. Department of Housing and Urban Development, becoming the first openly lesbian or gay public official in the United States whose appointment to a federal position was confirmed by the United States Senate. U.S. COMMISSION ON CIVIL RIGHTS – “FEDERAL CIVIL RIGHTS ENGAGEMENT WITH ARAB AND MUSLIM AMERICAN COMMUNITIES - POST 9/11” – September – available via google search)

The goals of constructive “partnership” engagement and “aggressive” intelligence gathering are prone to work at cross purposes. As the Commission found, “[f]ederal programs which intertwine civil rights protections with other policy and legal priorities undermine efforts to reduce prejudice and discrimination against American Arabs and Muslims.”² The Commission also identified as a Key Issue the fact that [i]nvestigatory enforcement techniques used by some federal agencies have had excessive overlap with those same agencies’ community engagement activities. This has made numerous Arab and Muslim Americans feel that they were being harassed and denied civil rights, and for some, lessened their trust in the very federal agencies that were in part supposed to be protecting them.

The turn's unique – federal policy hampers this coop now. Waxman '9

Matthew C. Waxman - Associate Professor, Columbia Law School; Member of the Hoover Institution Task Force on National Security and Law; Adjunct Senior Fellow, Council on Foreign Relations – “Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11” - JOURNAL OF NATIONAL SECURITY LAW & POLICY - Vol. 3:377 - http://jnslp.com/wp-content/uploads/2010/08/09_Waxman-Master-12-7-09-.pdf

In general, this means that federal coordination efforts and offers of assistance to state and local agencies can alter local police priorities from what the local political “market” might produce, but only to a point. A key question is what happens when federal national security priorities are too greatly misaligned from local political preferences. Some of the consequences of misalignment are illustrated in two frequently cited examples of local-federal tension in combating terrorism: Detroit’s response to federal requests to interview certain immigrants, and Portland, Oregon’s withdrawal from the FBI’s regional JTTF. In November 2001, the Justice Department requested that local police departments assist in interviewing 5,000 foreign men of Middle Eastern origin residing in their communities to determine whether any of them posed a terrorist threat or had useful information about possible terrorists. The Detroit Police Chief and local officials worried that these interviews might violate of state law and could alienate Arab-Americans. They therefore refused to participate in the federal initiative.⁷⁸ In 2005, Portland became the first city to remove its law enforcement agencies from the FBI-led JTTF. Key members of the city government worried that the JTTF’s surveillance activities might, while complying with federal law, not meet more stringent state law standards despite FBI assurances. Nor, due to secrecy rules, could city government leaders oversee whether city police officers participating in the JTTF were abiding by agreed-upon guidelines.⁷⁹ In both Detroit and Portland, pressures stemming from local accountability systems forced municipal agencies to opt out of the federal effort.⁸⁰ The Detroit greater metropolitan area is home to an especially large Arab-American community. Arab-American leaders voiced concern about the interview initiative, and the local police had worked hard over recent years to build a relationship of trust with the Arab-American community, a relationship the police feared could fray as a result of heavyhanded federal efforts.⁸¹ Portland, is an area known for its generally liberal orientation (in 2003 the city council publicly criticized and called for major changes in the USA PATRIOT Act, enacted by Congress soon after September 11 to expand domestic law enforcement and intelligence powers), and city officials were probably particularly sensitive about aggressive federal counterterrorism efforts after a Portland-area lawyer and convert to Islam was erroneously linked by the FBI to terrorist bombings in Madrid.

Even if the info's useful – it doesn't have to be collected in bulk". Targeted and narrow alternatives solve their link.

Wyden '14

(et al; This amicus brief issued by three US Senators - Ron Wyden, Mark Udall and Martin Heinrich. Wyden and Udall sat on the Senate Select Committee on Intelligence and had access to the meta-data program. “BRIEF FOR AMICI CURIAE SENATOR RON WYDEN, SENATOR MARK UDALL, AND SENATOR MARTIN HEINRICH IN SUPPORT OF PLAINTIFF-APPELLANT, URGING REVERSAL OF THE DISTRICT COURT” – Amicus Brief for *Smith v. Obama* – before the United States Ninth Circuit Court of Appeals - Appeal from the United States District Court District of Idaho The Honorable B. Lynn Winmill, Chief District Judge, Presiding Case No. 2:13-cv-00257-BLW – Sept 9th, 2014 – This Amicus Brief was prepared by CHARLES S. SIMS from the law firm PROSKAUER ROSE LLP. Continues to Footnote #6 – no text omitted. Amici” means “friend of the court” and – in this context - is legal

reference to Wyden, Udall, etc. This pdf can be obtained at: <https://www.eff.org/document/wyden-udall-heinrich-smith-amicus>)

The government possesses a number of legal authorities with which it may obtain the call records of suspected terrorists and those in contact with suspected terrorists. Amici have consistently argued that the bulk phone-records program needlessly tramples on Americans' privacy rights, particularly in light of the authorities available to the government that can also be used to acquire call records of suspected terrorists and those in contact with suspected terrorists in a targeted manner. See Press Release, Sen. Martin Heinrich, Udall, Heinrich Back Effort To End Dragnet Collection of Phone Data & Add Meaningful Oversight of Surveillance Programs (Oct. 29, 2013), <http://1.usa.gov/182XcfHE>; Press Release, Sen. Mark Udall, Surveillance Reform Package Ends Bulk Collection of Phone Records, Creates Constitutional Advocate for Secret Court (Sept. 25, 2013), <http://1.usa.gov/1bBGLku> ("Udall Reform Release"). Even the valid claims by intelligence officials about certain useful information obtained through the bulk phone-records program fail to explain why the government could not have simply obtained this information directly from phone companies using more calibrated legal instruments. A number of legal authorities would have allowed the government to do so. For example, the Stored Communications Act permit the government to obtain precisely the same call records that are now acquired through bulk collection under section 215 when they are "relevant and material" to an ongoing criminal investigation." 18 U.S.C. § 2703 (d). Individualized orders for phone records, as opposed to orders authorizing bulk collection, can also be obtained under section 215. 50 U.S.C. § 1861. National security letters, which do not require a court order, can also be used by the government to obtain call records for intelligence purposes. See 18 U.S.C. § 2709. The government can also acquire telephony metadata on a real-time basis by obtaining orders from either regular federal courts or the FISC for the installation of pen registers or trap-and-trace devices. See 18 U.S.C. §§ 3122, 3125; 50 U.S.C. § 1842. And the government may also seek call records using standard criminal warrants based on probable cause. See 18 U.S.C. § 2703 (c)(A); Fed. R. Crim. P. 17(c). The government can use many of these authorities without any more evidence than what is currently required to use the bulk phone-records database, with less impact on the privacy interests of innocent Americans.

Surveillance Violates Privacy

Inherency/Uniqueness

The NSA still collects phone records (Section 215) in bulk and collects internet data in a more targeted way

Nicholas Iovino, November 2, 2020, Courthouse News Service, Telecoms Customers Take Fight Over NSA Spying Programs to Ninth Circuit, <https://www.courthousenews.com/telecoms-customers-take-fight-over-nsa-spying-programs-to-ninth-circuit/>

Lead plaintiff Carolyn Jewel sued the NSA in 2008, long before NSA contractor Edward Snowden leaked a trove of classified records unveiling details about the NSA's multiple warrantless spying programs in 2013. The lawsuit claims the NSA used three programs to spy on American citizens in a way that violates the First and Fourth Amendments, the Wiretap Act, Stored Communications Act and Foreign Intelligence Surveillance Act. Those programs include the bulk collection of cellphone and landline records from phone companies, mass interception and searching of Americans' emails and other internet communications, and collection of metadata from internet communications, such as timestamps and "to" and "from" data from emails. The government has acknowledged the existence of those programs. It says the bulk collection of internet communications and metadata was discontinued and replaced with more targeted collection of data based on specific selection terms. The bulk collection of phone records continues.

Current cases

Nicholas Iovino, November 2, 2020, Courthouse News Service, Telecoms Customers Take Fight Over NSA Spying Programs to Ninth Circuit, <https://www.courthousenews.com/telecoms-customers-take-fight-over-nsa-spying-programs-to-ninth-circuit/>

In April 2019, U.S. District Judge Jeffery White issued summary judgment in favor of the NSA. He concluded that simply revealing whether classified evidence shows the NSA collected the plaintiffs' data would by itself threaten national security. During an appeals court hearing Monday, plaintiffs' attorney Richard Wiebe argued that a 2019 Ninth Circuit ruling forbids dismissing a case just because the government invokes its state secrets privilege. In Fazaga v. FBI, the Ninth Circuit reversed the dismissal of a lawsuit over mosque surveillance, finding the court should have reviewed classified evidence behind closed doors instead of dismissing constitutional claims based on the government's assertion of state secrets privilege. The government has until late December to appeal that decision to the Supreme Court. In that case, the Ninth Circuit ruled that courts should use the procedures described in Section 1806(f) of the Foreign Intelligence Surveillance Act of 1978

to review classified evidence behind closed doors to determine if a plaintiff has been subjected to unlawful surveillance.

NSA creates back doors to encrypted communications as part of its surveillance

Mailyn Fidler, 11-16, 20, Reporter's Committee, Seven years on, congressional oversight of National Security Agency policies is still a slog, <https://www.rcfp.org/tech-press-freedom-nov-15-2020/>

When Edward Snowden leaked classified information about U.S. government mass surveillance seven years ago, the former National Security Agency contractor sparked intense debate about — and reform of — many surveillance policies. Those conversations around reforming government surveillance practices have been especially important for journalists. As the Reporters Committee has previously argued, national security surveillance can chill or compromise newsgathering. Current discussions about proposed legislation that would prevent companies from using the strongest forms of encryption, such as the EARN IT Act, have resurfaced many concerns about government surveillance. But learning how NSA policies have changed is almost as hard as it was before Snowden's revelations, lawmakers are finding. **The NSA is resisting congressional efforts, led by Sen. Ron Wyden (D-Ore.), to improve transparency around its policies regarding the introduction of back doors into commercial products.** In response to these inquiries, NSA official Anne Neuberger told Reuters, "We don't share specific processes and procedures." But **the broad strokes of post-Snowden policies on other issues have been released, including the White House-initiated Vulnerability Equities Process, which governs the process by which government agencies decide whether to reveal or keep for national security surveillance purposes vulnerabilities in information systems and technologies.** Reuters reports that three former senior intelligence agency officials have said that the new NSA backdoor process requires them to "weigh the potential fallout" and to arrange for some kind of warning to the company if the back door is discovered by adversarial actors. **Backdoor access to devices matters to journalists who rely on commercial products to communicate with sources domestically and overseas — especially when these back doors are in commercial encryption products that journalists use to offer sources greater protection.** Documents released by Snowden revealed that the NSA worked with the Commerce Department to get a certain encryption standard accepted as the global default — in part because the agency knew how to break it and access encrypted data.

The FBI conducts back door searches

VIRGINIA L.GRADY, Federal Public Defender, October 29, 2020, US v. Muhrtov,
<https://www.aclu.org/legal-document/us-v-muhtorov-defendants-supplemental-reply-brief>

Backdoor searches are a key element of those procedures: the FBI is permitted and encouraged to routinely use backdoor searches, and agents conduct such queries in investigations millions of times each year. [Redacted], 402 F. Supp. 3d 45, 74-75 (FISC 2018).Indeed, the record continues to support the conclusion that FBI agents conducted backdoor searches part of their investigation of Mr. Muhtorov, as agents do “whenever the FBI opens a new national security investigation or assessment.”

Section 702 of FISA example

ACLU, November 17, 2020, <https://www.aclu.org/cases/us-v-muhtorov>, US v. Muhtorov

The ACLU and the Office of the Federal Public Defender of Colorado jointly represent Jamshid Muhtorov in his challenge to the constitutionality of Section 702 of the Foreign Intelligence Surveillance Act (FISA), and the lawfulness of other spying methods the government used against him. Mr. Muhtorov is a lawful permanent resident of the United States who hails from Uzbekistan. There, he led a regional branch of the country’s only human rights organization, and became one of the country’s most prominent human rights defenders. Due to his activism, Mr. Muhtorov and his family were persecuted by Uzbekistan’s ruling regime, and they eventually sought refuge abroad. In 2007, the United States granted Mr. Muhtorov, his wife, and their two young children granted admission to the United States as political refugees. They settled in Denver, Colorado, and became permanent residents. Shortly thereafter, the U.S. government began surveilling Mr. Muhtorov, and in 2012, the government charged him with providing material support to a terrorist organization in Uzbekistan. He was detained for six years before being brought to trial. In 2013, after Edward Snowden’s revelations about the scope of the National Security Agency’s mass surveillance, Mr. Muhtorov became the first person to receive notice from the government about the monitoring of his communications under Section 702 of FISA. This highly controversial statute allows the NSA to engage in dragnet, warrantless surveillance of Americans’ international phone calls, emails, chats, and web-browsing. Over the course of Mr. Muhtorov’s case, it became clear that the government’s investigation of him involved a variety of spying tools—many of which remain shrouded in secrecy—expanding beyond Section 702 surveillance. For years, federal agents tracked Mr. Muhtorov’s comings and goings. They installed bugs in his home, listening to the intimate details of his family life. They recorded his phone calls. And they intercepted untold amounts of his electronic communications. Before his trial, Mr. Muhtorov sought to suppress evidence obtained or derived from Section 702, on the grounds that this warrantless surveillance violates the Fourth Amendment and Article III of the Constitution. Mr. Muhtorov also moved for

disclosure of the government's surveillance applications, so that he could meaningfully challenge the government's legal and factual arguments. Finally, Mr. Muhtorov requested notice of the government's reliance on any undisclosed surveillance in its investigation—because without notice, he would have no way of challenging the lawfulness of those...

Section 702 Surveillance violates the Constitution

ACLU, November 17, 2020, <https://www.aclu.org/cases/us-v-muhtorov>, US v. Muhtorov

Under Section 702, the government intercepts billions of international communications sent by hundreds of thousands of people, including American citizens, lawful permanent residents, and others in the United States. The government stores these communications in massive databases, retains them for years, and searches them repeatedly for information about people in the United States—including in domestic criminal investigations. This surveillance takes place inside the United States, and with only very limited involvement by judges on the secret Foreign Intelligence Surveillance Court. All of this surveillance is conducted without a warrant, in violation of core Fourth Amendment protections. Mr. Muhtorov was one of the many people in the United States whose private communications have been vacuumed up, pooled together in government databases, and then examined by FBI agents without a warrant under Section 702.

FBI backdoor searches are especially invasive

VIRGINIA L.GRADY, Federal Public Defender, October 29, 2020, US v. Muhrtov,
<https://www.aclu.org/legal-document/us-v-muhtorov-defendants-supplemental-reply-brief>

Moreover, as the FISC has held, the FBI's record keeping with respect to backdoor searches has been nothing short of abysmal. [Redacted], 402 F. Supp. 3d at 67-68, 73-91. For years, the FBI did not even require agents to write down their reasons for targeting an American with a backdoor search, nor did the agency document the volume of U.S.-person queries of its Section 702 databases. Id. at 52-53, 68, 79, 88-91. By all indications, these problems beset the FBI's searches during the period relevant here. Indeed, even after Congress required the FBI to record the number of its U.S.-person queries in 2018, the agency failed to do so. If the Court deems the government's "fruit of the poisonous tree" claim relevant in any way, the FBI's failures to implement basic recordkeeping requirements related to backdoor searches are yet another reason to require disclosure and adversarial testing of its assertion.

FISC

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

Before trial, the government filed a notice advising Muhtorov that the government intended to offer into evidence “information obtained and derived from electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (“FISA”), as amended, 50 U.S.C. §§1801-1811 and 1821-1829.” ROA Vol. 1 at 220. Those provisions, referred to here as “traditional” FISA authority, permit certain electronic surveillance and physical searches based on an order from the Foreign Intelligence Surveillance Court (FISC). Before the FISC may issue a traditional FISA order, the FISC must find, among other things, probable cause to believe that the target is a foreign power or its agent. See 50 U.S.C. §§1801, 1804-05, 1821, 1823-24.. As discussed below, Section 702 was enacted in 2008 to augment traditional FISA by establishing supplemental procedures for authorizing targeted surveillance for intelligence purposes of foreign persons located outside the United States with the assistance of U.S. electronic communication service providers. See Clapper v. Amnesty Int'l USA, 568 U.S. 398, 404-06, 422 (2013). Under Section 702, instead of issuing traditional FISA orders, the FISC approves annual certifications that specify categories of foreign intelligence information the government is authorized to acquire and the procedures governing the collection. 50 U.S.C. § 1881a(h), (j). The FISC must find, among other things, that the “targeting procedures,” which ensure that the authorized surveillance is properly aimed at non-U.S. persons located outside the United States, are consistent with the statutory standards and the Fourth Amendment. Id. § 1881a(j)(2)(B), (j)(3). The FISC also must find that the “minimization procedures,” which restrict how the government treats information of U.S. persons who may communicate with the foreign targets, are likewise consistent with the statute and the Fourth Amendment.

Incidental data collection of US citizens doesn't violate the Fourth Amendment

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

The district court properly denied Muhtorov’s motion to suppress evidence derived from surveillance authorized under Section 702. The Section 702-authorized collection in this case, which targeted, for foreign intelligence purposes, a non-U.S. person located outside the United States with whom Muhtorov was communicating, was reasonable under the Fourth Amendment. First, the Fourth Amendment generally does not apply to non-U.S. persons abroad. The fact that surveillance targeting such persons also incidentally collects communications of U.S. persons does not trigger a warrant requirement under Appellate Case: 18- 13 well-established principles and precedent. Every court to review Section 702 surveillance has found the warrant requirement

inapplicable. Alternatively, Section 702 surveillance falls within the “foreign intelligence exception” to the warrant requirement. The Section 702 collection here also satisfied the Fourth Amendment’s reasonableness standard. The government has an interest of the utmost importance in obtaining foreign intelligence information to protect the United States from foreign threats, including international terrorism. That interest outweighs the privacy interests of U.S. persons such as Muhtorov whose communications are incidentally collected, particularly where, as here, the government followed court-approved procedures reasonably designed to protect such privacy interests.

Section 702 likely to exclude US citizens

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

The FISC has approved a series of Section 702 certifications dating back to 2008. The FISC has found that acquisitions under Section 702 were not subject to the Fourth Amendment’s warrant requirement because they target “persons reasonably believed to be located outside the United States,” who are “not protected by the Fourth Amendment,” and such targets “will have been assessed by [the government] to possess and/or to be likely to communicate foreign intelligence information.” In re DNI/AG Certification, No. 702(i)-08-01(FISC 2008)(“FISC 2008 Op.”)Mem. Op. at 35, 37.9TheFISC has also concluded that the acquisitions satisfied the Fourth Amendment’s reasonableness requirement “in view of the gravity of the government’s national security interests and the other safeguards embodied in the targeting and minimization procedures.” Id.at 38, 41

Incidental collection under section 702 is constitutional

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

Muhtorov argues (Br. 27) that the incidental acquisition of his communications pursuant to Section 702 collection targeting a non-U.S. person abroad “violated the Fourth Amendment’s warrant requirement.” But as the Ninth and Second Circuits unanimously held, the Fourth Amendment does not require a warrant where, as here, the government targets under Section 702 a non-U.S. person abroad even though such searches may incidentally collect some communications between the target and a U.S. person. United States v. Mohamud, 843 F.3d 420, 441 (9th Cir. 2016) (holding that “because the target of the surveillance was a non-U.S. person located outside of the United States at the time of the surveillance, the government

was not required to obtain a search warrant to collect” the emailcommunications of a U.S. person with the foreign national “as an incident to its lawful search of the foreign national’s email” under Section 702);United States v. Hasbajrami, 945 F.3d 641, 664 (2d Cir. 2019) (same)

The 4A does not apply outside the US

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

The Supreme Court has “inferred” from the Fourth Amendment that “a warrant must generally be secured” for government searches, but the Court has recognized reasonable “exceptions” from that “warrant requirement.” Kentucky v. King, 563 U.S. 452, 459 (2011). In United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), the Supreme Court recognized one such exception for searches directed against aliens outside the United States. Id. at 266-67. The Court rejected a warrant requirement in that case because the Fourth Amendment does not “restrain the actions of the Federal Government against aliens outside of the United States” and thus does not “apply to activities of the United States directed against aliens in foreign territory.” Id. at 266-67, 271; see id. at 263, 265. That limitation is consistent with decisions recognizing that “aliens receive [certain] constitutional protections when they have come within the territory of the United States and developed substantial connections with this country.” Id. at 271; see id. at 275 (Kennedy, J., concurring) (“[T]he Constitution does not create, nor do general principles of law create, any juridical relation between our country and some undefined, limitless class of noncitizens who are beyond our territory.”). Verdugo Urquidez therefore reflects the “well-established” principle that Fourth Amendment protection is otherwise “unavailable” to “aliens outside of our geographic borders.” Zadvydas v. Davis, 533 U.S. 678, 693 (2001). Disregarding that limitation “would have significant and deleterious consequences for the United States” in national security contexts. Verdugo-Urquidez, 494 U.S. at 273.

It's not practical to obtain a warrant in foreign situations

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

Several courts of appeal have recognized, as a variant of the special needs exception, a foreign-intelligence exception to the warrant requirement. See United States v. Duka, 671 F.3d 329, 341 (3d Cir. 2011) (citing cases); In re Directives, 551 F.3d at 1010-12. Foreign intelligence collection under Section 702 falls within that exception because the “programmatic purpose” of

obtaining foreign intelligence information goes “beyond any garden-variety law enforcement objective,” and “requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.” In re Directives, 551 F.3d at 1011

Surveillance under section 702 is critical to fight terrorism

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

The government's national security interest in conducting surveillance under Section 702 to combat terrorism and other national security threats“is an urgent objective of the highest order.”Mohamud, 843 F.3d at 441. See alsoIn re Directives, 551 F.3d at 1012. In addition, the Privacy and Civil Liberties Oversight Board (“PCLOB”)found that Section 702 is a uniquely valuable tool in the government’s efforts to combat terrorism. PCLOB Report at 104-08.And the urgency of the government’s interest is “greater, not less” when the foreign intelligence target communicates with associates in the United States. Hasbajrami, 945 F.3d at 667; see id.(“If it is reasonable—and indeed necessary to the national security—for intelligence agencies to monitor the communications of suspected foreign terrorists abroad, the need to keep track of the potential threat from abroad does not lessen because some of the suspect’s contacts turn out to be American nationals, or foreignnationals located within the United States”).

Section 702 procedures protect privacy

Jason Dunn, US Attorney, February 10, 2020, U.S. V. MUHTOROV - GOVERNMENT'S PUBLIC RESPONSE BRIEF, <https://www.aclu.org/legal-document/us-v-muhtorov-governments-public-response-brief>

The Privacy Interests of U.S. Persons Are Protectedby Stringent Safeguards and Procedures The government employs multiple safeguardsthat reasonably govern targeting decisions and the handling of U.S. persons’ information that may be acquired.a.CertificationSection 702 requires that the DNI and the Attorney General certify that procedures are in place to protect the privacy of U.S. persons. See50 U.S.C. § 1881a(a),(h), and (j). The DNI and the Attorney General must also certify that a significant purpose of the acquisition is to obtain foreign intelligence information, that guidelines have been adopted to ensure compliance with the limitations in Section 702(b), and that the guidelines, targeting and minimization procedures are consistent with the Fourth Amendment. See50 U.S.C. § 1881a(h)(2)(A). In requiring such high-level officialsto oversee collection underSection 702, the statutehelps ensure that Section 702is appropriately used for important foreign-intelligence purposes FISC ReviewThe government’s certification,

targeting procedures, and minimization procedures are all subject to FISC review. See 50 U.S.C. § 1881a(j)(3)(A). Prior FISC approval further supports the conclusion that Section 702 collection conducted pursuant to such procedures is constitutional. See Clapper, 568 U.S. at 414 (noting the importance of the requirement that the FISC “assess whether the Government’s targeting and minimization procedures comport with the Fourth Amendment”). The FISC subjects those procedures to exacting Fourth Amendment scrutiny. See, e.g., FISC 2008 Op. at 32–40; FISC 2011 Op., 2011 WL 10945618, at *5–6. In addition, “FISC review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather the Court also examines how the procedures have been and will be implemented.” [Caption Redacted], Mem. Op. at 3 (FISC Aug. 26, 2014) (“FISC 2014 Op.”). 13c. Targeting procedures Section 702 provides that targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1). The FISC repeatedly has found that the targeting procedures meet that standard, and reviewing courts have agreed. See Mohamud, 843 F.3d at 443. d. Minimization procedures The government also employs FISC-approved minimization procedures to limit the acquisition, retention, and dissemination of information concerning U.S. persons, consistent with the government’s foreign intelligence needs. See 50 U.S.C. § 1801(h)(1); PCLOB Report at 50 (The minimization procedures are “a set of controls on data to balance privacy and national security interests”). 14 Minimization procedures limit how long information concerning U.S. persons can be retained and how it can be disseminated. The procedures require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. See id. at 64–65. As the FISC has held, the minimization 15 (finding it “significant” in upholding the PAA that “effective minimization procedures are in place”) to “serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.”). Under Section 702, Congress and the Executive Branch have developed a balanced framework of court-approved procedures to enable foreign intelligence collection vital to the nation’s security while protecting constitutionally protected privacy interests. See *In re Directives*, 551 F.3d at 1016 (“[W]here the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts.”). These safeguards ensured that the collection in this case targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the privacy of U.S. persons. Courts reviewing incidental collection under Section 702 in circumstances similar to this case have found that the government’s actions were reasonable under the Fourth Amendment’s balancing test. This Court should likewise hold that the government’s Section 702 acquisition of foreign intelligence information in this case was reasonable. 3. Section 702 Collection Has Sufficient Particularity Muhtorov misses the mark in arguing (Br. 38–40) that Section 702 collection is constitutionally unreasonable because it lacks the “core safeguards” of a particularized court order or probable cause finding. Section 702 collection is sufficiently focused and reasonable, given its foreign-intelligence context. The government must determine that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information and that the person uses a specific communications “selector,” (such as an email

address), and the government acquires only communications involving that particular selector. See FISC 2011 Op., 2011 WL 10945618, at *7; PCLOB Report at 20-23, 32-33, 111-12. Section 702 does not authorize bulk collection. See 2014 FISC Op. at 26 (“acquisitions are not conducted in a bulk or indiscriminate manner”); PCLOB Report at 103. Although particularity may be a factor in assessing reasonableness, the Fourth Amendment “imposes no irreducible requirement” of individualized Appellate Case: 18-1366 Document: 010110302495 Date Filed: 02/10/2020 Page: 48 36 suspicion where the search is otherwise reasonable. King, 569 U.S. at 447 (citation omitted); see also In re Directives, 551 F.3d at 1013 (rejecting the petitioner’s attempt to “reincorporate . . . the same warrant requirements” governing domestic surveillance that the court had “already . . . held inapplicable” to surveillance targeting foreigners abroad). While the number of communications intercepted by the government could be voluminous, the collection is neither indiscriminate nor untethered to a vital national security interest. Rather, Section 702’s targeting procedures are sufficiently particularized for the purpose of the collection, and are thus reasonable under the Fourth Amendment. Indeed, with respect to this case, the district court found that the “[Section 702] surveillance at issue was narrowly tailored to the government’s foreign intelligence-gathering prerogatives.” Appellant’s App. 119; see also United States v. Hasbajrami, 2017 WL 1029500, at *13 (E.D.N.Y. Mar. 8, 2016) (finding that the collection in that case “was as particular as it gets” because it involved “the targeting of specific non-U.S. persons outside the United States for specific counter-terrorism purposes”). This Court’s review of the classified record will likewise show that the Section 702 collection here was appropriately “particular” and reasonable.... As the FISC has held, the minimization procedures reasonably protect the privacy interests implicated by querying using U.S. person identifiers, balanced against the government’s compelling foreign-intelligence interest in conducting such queries. In light of those procedures, there is no constitutional requirement of prior judicial review or other additional Fourth Amendment analysis of each individual query. The FISC-approved minimization procedures permit the government to review the information it lawfully collects under Section 702, which includes information concerning U.S. persons, to assess whether the information Appellate Case: 18-1366 Document: 010110302495 Date Filed: 02/10/2020 Page: 56 44 should be retained or disseminated. Accordingly, U.S. person information is by necessity already subject to review (and use) under those procedures. Under Section 702, the collection and communication-by-communication review of information is lawful under the Fourth Amendment, and there is no basis to require additional judicial process for the more focused review of the same information in response to tailored queries.

Privacy First

Freedom and dignity are ethically prior to security.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed. This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

Privacy must be valued above all else

Gould, 10- Associate Professor at the University of British Columbia Faculty of Law and a Research Associate at the Oxford University Centre for Criminology, (Benjamin, "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy", OVERVÅKNING I EN RETTSSTAT - SURVEILLANCE IN A CONSTITUTIONAL GOVERNMENT, 2010, PDF, page 45-47)//AP

This all of course leads us back to the question at the beginning of this chapter, namely: how much state surveillance is too much? Perhaps the first and most obvious response to this question is that the state should at all times be sensitive to the fact that privacy is a basic human right, and that it is essential to personal development, individual dignity, and the ability of citizens to engage in meaningful social relationships. We have, in the words of Article 8 of the European Convention on Human Rights, a right to "respect for private and family life" because without such privacy we can never truly flourish. Going further, however, the state must also recognize that privacy has an important role to play in the promotion of democracy and the meaningful exercise of a number of other fundamental rights, such as the right to freedom of expression and freedom of association. As a consequence, all state surveillance activities – regardless of whether the justification for such measures is the prevention of crime, the promotion of security, or even the efficient delivery of public services – must be evaluated in terms of the potential cost to political freedom and the maintenance of democratic values. This is particularly important given that, as Bennett and Raab rightly point out, the social value of privacy can be easily forgotten in our efforts to protect individuals from the personal effects of overzealous state surveillance. The social value [of

privacy] is underpowered and survives precariously unless it can be specifically reinforced by a change in the privacy culture, for it is powerfully challenged by the legacy of the conventional paradigm and by forces that tend to the protection of privacy seen as an individual value, if a value at all.⁶² Put simply, there is little point in the state seeking to create a society free from crime and secure against terrorist threats if the overall cost is a severe loss of personal freedom and the introduction of Orwellian, authoritarian government. Put more simply, we know that there is too much surveillance when citizens begin to fear the surveillance activities of the state, and no longer feel free to exercise their lawful rights for fear of unwanted scrutiny and possible censure. Finally, given that a democratic state can only be legitimate and thrive in an atmosphere of mutual trust between government and governed, it follows that any surveillance measure that threatens to erode or destroy that trust must be resisted, or at the very least its potential costs and benefits carefully considered. As anyone who has lived in a state where the rule of law is not taken for granted – and where there is little in the way of institutional trust – will be able to tell you, confidence in the institutions of government is hard won and easily lost.⁶³ For this reason, the presumption should be that any surveillance measure which is directed at the public at large – and which treats all citizens as potential threats or management challenges – has *prima facie* gone a step too far, and demands an extra-ordinary justification. According to this view, mass state surveillance should always be the exception and never the rule. In short, we will know when there is too much state surveillance when political rights and democratic participation are threatened, and it is at this point that the citizenry should demand that the state pulls back and accepts that there are times when it is better for the government to know less rather than more. Of course, some will say that we have already passed this point, that the current surveillance infrastructure already poses a serious threat to democracy and the rule of law. If this is true, then there is an even more pressing need for us to demand a halt to any further expansion in the surveillance apparatus of the state, and a fundamental reappraisal of the state's use of technologies like public area CCTV.

Privacy is a fundamental moral right.

Alfino and Mayes, 2003

Mark Alfino Department of Philosophy Gonzaga University G. Randolph Mayes Department of Philosophy California State University, Sacramento "Reconstructing the right to privacy." Social Theory and Practice 29.1 (2003): 1-18.

The core claim in our theory is that **privacy is a fundamental moral right**. The argument to support this claim is simple, but the consequences and implications of the argument are not. In this section, we focus on establishing the right to privacy as a fundamental moral right and elucidating some of the most obvious implications of the view. We leave further development of the view and an exploration of objections to the next section. In arguing for privacy as a fundamental moral right, we obviously assume that a scheme of rights and correlative duties is a well-justified way to describe social relations among individuals. Specifically, moral rights describe the legitimate exercise of power, both of individuals and others, severally and collectively. Rights can be thought of negatively as mutual protection schemes and positively as a reflection of our best understanding of how individuals establish and maintain their moral agency." At the heart of our understanding of moral agency is a belief about the ability of moral individuals to be "self-legislating" or autonomous. We will look at important differences of emphasis in different definitions of autonomy in a moment, but at present the important point is that in a system of rights and duties the concept of the self-legislating individual is central. In fact, most basic moral rights can be understood as explications of the concept of a self-legislating agent, or the implications of how such a person necessarily interacts with a physical and social world. For example, rights of due process are fundamental moral rights, because in an environment in which I could not be guaranteed a rational (due) process for losing rights and privileges, I could not formulate rational rules for my own conduct. Privacy plays a fundamental and ineliminable role in constructing personal autonomy. To see this, it may help to extend the juridical metaphor at the heart of the notion of autonomy. What kinds of law do agents legislate? To what realm of objects does such law apply? Of course, these are questions that Immanuel Kant posed and answered extensively.¹² Kant demonstrated that a basic heuristic of moral life is an analogy between physical space and the laws of nature that govern it, on the one hand, and moral space and the moral law on the other hand. This analogy lies at the heart of "rights talk." It is common to speak of rights as law-like background conditions from which we can

predict the outcome of claims and torts. Jurists and legislators use rights instrumentally—for good and ill—to establish various kinds of space: a private space of property relationships and private social relationships, a public space of communal expectations for fair treatment and access. When we grant "privilege" to specific kinds of relationships, such as the confidential conversations between priests and confessors or lawyers and their clients, we are using moral laws to configure moral space just as a divine creator might be imagined to configure physical space from a set of possible physical laws. Whether or not we grant moral space any ontological significance, it still helps to elucidate our basic theoretical framework. The analogy between moral and physical space also reminds us of the need to configure the moral space needed for individuals to become autonomous agents upon a realistic view of how individuals actually develop, both cognitively and emotionally. We can criticize competing explications of moral space by reference to our background knowledge of human behavior and development. Facts about our psychology do not by themselves justify moral rights. However, our understanding of the moral space that an autonomous agent inhabits and the moral laws that govern that space must cohere with our understanding of the laws of the physical world, especially those governing the psychological development of human animals and the physical conditions of their existence. Within these constraints we make a variety of choices about which aspects of our physical and psychic environment to value, and in so doing we construct the specific moral space that governs social life.

Additionally, because of foundational nature of privacy, it is not optional.

Allen, 2011

Anita. J.D., Ph.D, Henry R Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania School of Law. Unpopular privacy: what must we hide?. Oxford University Press, 2011. Pp 172-3

Since the 1970s, when scholars first began to analyze privacy in earnest, philosophers have linked the experience of privacy with dignity, autonomy, civility, and intimacy. They linked it also to repose, self-expression, creativity, and reflection. They tied it to the preservation of unique preferences and distinct traditions.

Privacy is a foundational good. The argument that privacy is a right whose normative basis is respect for persons opens the door to the further argument that privacy is also potentially a duty. "To respect someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one's decision," S. I. Benn wrote.³⁵ And to respect oneself may require taking into account the way in which one's personality and life enterprises could be affected by decisions to dispense with foundational goods that are lost when one decides to flaunt, expose, and share rather than to reserve, conceal, and keep. The idea that the experience of privacy is ethically mandatory is logically consistent with leading normative accounts. It is consistent with Robert Post's (citing Erving Goffman and Jeffrey Reiman) "characterization of respecting privacy as respecting civility norms" of deference and demeanor.³⁶ It is likewise consistent with Helen Nissenbaum's analysis of privacy. She defines privacy and its value in relation to norms of the appropriateness of specific behaviors and the distribution of certain information in social and cultural context.⁴⁰ If people are completely morally and legally free to pick and choose the privacy they will experience, such as deferential civility, appropriateness and limited data flow, they are potentially deprived of highly valued states that promote their vital interests, and those of fellow human beings with whom they associate. We need to restrain choice—if not by law, then somehow. **Respect for privacy rights and the ascription of privacy duties must both be a part of a society's formative project for shaping citizens.**

Lior Jacob Strahilevitz has argued that privacy violations can be understood as rechanneling information flow, so that information unknown or obscure in a network becomes known: "Where a defendant's (in a suit alleging informational privacy invasion disclosure materially alters the flow of otherwise obscure information through a social net-work, such that what would have otherwise remained obscure becomes widely known, the defendant should be liable for public disclosure of private facts."⁴¹ Viewed in this way, it may not seem to matter that privacy is invaded unless the person whose information flows out against his will cares. We have to go back to dignitarian ideals about privacy to see why we, as liberals, should care about optional dismissals of privacy. Jeffrey Reiman defined privacy as the "social rituals" that serve to teach us that we are distinct moral persons and autonomous moral agents.⁴² Liberals agree that there is something wrong with being watched and investigated all the time. As legal theorist Daniel Solove argues, surveillance can make "a person feel extremely uncomfortable" and can lead to "self-censorship and inhibition."⁴³ Surveillance is a form of social control. As such, it impacts freedom. I have been urging that

dispensing with one's privacy is yielding to social control, and that that impacts freedom, too.
Realizing this, the notion that some privacy should not be optional, waivable, or alienable should have instant credibility.

Privacy = Gateway Right

The impact is the loss of personal autonomy and agency. Privacy is a gateway right, it enables all of our other freedoms.

PoKempne 14,

Dinah, General Counsel at Human Rights Watch, “The Right Whose Time Has Come (Again): Privacy in the Age of Surveillance” 1/21/14 <http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance>

Technology has invaded the sacred precincts of private life, and unwarranted exposure has imperiled our security, dignity, and most basic values. The law must rise to the occasion and protect our rights. Does this sound familiar? So argued Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article announcing “The Right to Privacy.” We are again at such a juncture. The technological developments they saw as menacing—photography and the rise of the mass circulation press—appear rather quaint to us now. But the harms to emotional, psychological, and even physical security from unwanted exposure seem just as vivid in our digital age. Our renewed sense of vulnerability comes as almost all aspects of daily social life migrate online. At the same time, corporations and governments have acquired frightening abilities to amass and search these endless digital records, giving them the power to “know” us in extraordinary detail. In a world where we share our lives on social media and trade immense amounts of personal information for the ease and convenience of online living, some have questioned whether privacy is a relevant concept. It is not just relevant, but crucial. Indeed, privacy is a gateway right that affects our ability to exercise almost every other right, not least our freedom to speak and associate with those we choose, make political choices, practice our religious beliefs, seek medical help, access education, figure out whom we love, and create our family life. It is nothing less than the shelter in which we work out what we think and who we are; a fulcrum of our autonomy as individuals. The importance of privacy, a right we often take for granted, was thrown into sharp relief in 2013 by the steady stream of revelations from United States government files released by former National Security Agency (NSA) contractor Edward Snowden, and published in the Guardian and other major newspapers around the world. These revelations, supported by highly classified documents, showed the US, the UK, and other governments engaged in global indiscriminate data interception, largely unchecked by any meaningful legal constraint or oversight, without regard for the rights of millions of people who were not suspected of wrongdoing. The promise of the digital age is the effortless, borderless ability to share information. That is its threat as well. As the world’s information moves into cyberspace, surveillance capabilities have grown commensurately. The US now leads in ability for global data capture, but other nations and actors are likely to catch up, and some already insist that more data be kept within their reach. In the end, there will be no safe haven if privacy is seen as a strictly domestic issue, subject to many carve-outs and lax or non-existent oversight. Human Rights Watch weighed in repeatedly throughout 2013 on the human rights implications of Snowden’s revelations of mass surveillance, and the need to protect whistleblowers. This essay looks at how the law of privacy developed, and where it needs to reach today so that privacy is globally respected by all governments, for all people. Global mass surveillance poses a threat to human rights and democracy, and once again, the law must rise to the challenge.

Privacy = Moral Obligation

Equal freedom establishes privacy not only as a duty but also as a right

Mokrosinska, 2014

Dorota, Research Fellow in Philosophy at the University of Amsterdam, The Netherlands (2014), Privacy and the Integrity of Liberal Politics: The Case of Governmental Internet Searches. Journal of Social Philosophy, 45: 369–389. doi: 10.1111/josp.12068

I close my argument by drawing attention to the value and the normative status of privacy in political practice. I have argued that privacy is implicated in the concept of public justification that liberals place at the core of the concept of political legitimacy. Public justification requires that people explain to one another how the principles and policies they advocate can be supported by reasons that everyone can reasonably accept. That requirement is substantially linked to the idea of the equal freedom of individuals: equal freedom between individuals acting in the political domain is not realized unless policies are justified to all those who are subject to them. Political liberals tie the concept of public justification to an obligation that falls on individuals as members of political societies. In this context, Rawls speaks of a “duty of civility,”⁶² Lafont and Audi speak of a similar duty.⁶³ Now one cannot appeal to reasons that everyone can accept unless one holds back and refrains from bringing under collective attention one's unreasonable and comprehensive views. This is to say that one cannot perform the duty of civility unless one brackets such material as private. From this perspective, privacy is an aspect of the duty of civility and a condition of equal freedom. Equal freedom requires not only that individuals withhold their unreasonable and/or comprehensive views from the political forum. It also requires that they not attend to similar material in others. Given that such material is equally dysfunctional to the political realm, its exposure would be equally threatening to equal freedom. From that perspective, refraining from seeking, scrutinizing and exposing unreasonable and/or comprehensive beliefs of others is another aspect of the duty of civility. The same point can be expressed in the language of rights. If one's equal freedom cannot be realized unless others refrain from attending to one's (unreasonable) comprehensive views, then one is entitled, by virtue of equal freedom, that they do so. In this sense, **equal freedom establishes privacy not only as a duty but also as a right.**

Moral obligation to protect privacy — just as important as any other right

Gavison 12 — Ruth E. Gavison, Professor of Human Rights Law at Hebrew University Law Faculty. Born in Jerusalem. Received an LLB (cum laude) in 1969, LLM (summa cum laude) in 1971, and BA in economics and philosophy (1970), all from Hebrew University. Law clerk at the Israel Supreme Court (Justice Benjamin Halevi). Admitted to the Israeli bar in 1971. In 1975 she received a D.Phil. in legal philosophy from Oxford University, 2012 (“Privacy and the Limits of Law,” *Yale Law Journal*, Vol 28 No. 3, Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957, Accessed on 7-15-15)

It is here that understanding the reasons for the new concern with privacy becomes crucial. It is true that individuals today enjoy more opportunities for privacy in some areas, but this observation, taken alone, is misleading. The rarity of actions is not a good indication of the need for privacy, or of the extent to which invasions are undesirable. We enjoy our privacy not because of new opportunities for seclusion or because of greater control over our interactions, but be- cause of our anonymity, because no one is interested in us. The moment someone becomes sufficiently interested, he may find it quite easy to take all that privacy away. He may follow us all the time, obtain information about us from a host of data systems, record our conversations, and intrude into our bedrooms. What protects privacy is not the difficulty of invading it, but the lack of motive and interest of others to do so. The important point, however, is that if our privacy is invaded, it may be invaded today in more serious and more permanent ways than ever before. Thus, although most of us are unlikely to experience a substantial loss of

privacy, we have an obligation to protect those who lose their anonymity. In this sense, privacy is no different from other basic entitlements. We are not primarily concerned with the rights of criminal suspects because we have been exposed to police brutality ourselves. We know that we may be exposed to it in the future, but, more generally, we want to be part of a society that is committed to minimizing violations of due process.

NSA bulk surveillance violates a global obligation to protect privacy, that of a social contract

(**Wittes 15**, Benjamin Wittes, Monday, November 11, 2013, 5:05 PM, Acc. 7-15-2015, "A Global Human Right to Privacy?", Lawfare, <http://www.lawfareblog.com/global-human-right-privacy>, editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution) LS

It's time for governments to come clean about their practices, and not wait for the newest revelations. All should acknowledge a global obligation to protect everyone's privacy, clarify the limits on their own surveillance practices (including surveillance of people outside their own borders), and ensure they don't trade mass surveillance data to evade their own obligations. Of course it is important to protect security, but western allies should agree that mass, rather than narrowly targeted, surveillance is never a normal or proportionate measure in a democracy. Washington is finally grappling with the Snowden revelations, holding hearings and considering legislation that might help to rein in the NSA's seemingly unconstrained power. Some of these bills would limit or end bulk data collection, institute greater transparency, and give the secret court that oversees surveillance requests a more adversarial character. These are important proposals, but none include protection for non-Americans abroad. The US has the capacity to routinely invade the digital lives of people the world over, but it barely recognises any privacy interest of those outside the US (emphasis added). Roth's article echoes arguments made recently by David Cole on Just Security (here and here), to which Orin Kerr responded (here and here) on Lawfare. I fully agree with Orin's response to Cole, which essentially posits that the US government's obligation to respect the privacy of its citizens and those within its territory stems from a social contract not present with everyone else in the world.

Privacy sustains a sense a self-agency

Magi, **Trina J.**, "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature" (2011). University Libraries Faculty and Staff Publications. Paper 4.

2. Privacy affirms self-ownership and the ability to be a moral agent—Jeffrey Reiman identifies privacy as the “social ritual by which we show one another that we regard each person as the owner of [her]self, [her] body, and [her] thoughts” [27, p. 205]. Through privacy, he says, society lets the individual know he or she has the ability and the authority to withdraw from others' scrutiny, and “those who lose this ability and authority are thereby told that they don’t belong to themselves; they are specimens belonging to those who would investigate them” [27, p. 205]. Reiman claims that we understand only selves that think of themselves as “owning themselves” to be “moral selves”—selves that accept ownership of and responsibility for their actions [27, p. 206]. Understood this way, privacy is a fundamental right that enables people to think of their existence as their own and “protects the individual’s interest in becoming, being, and remaining a person” [17, p. 44]. As evidence (though not proof) of the fact that privacy is essential to the creation and maintenance of selves, Reiman refers to Goffman’s study “On the Characteristics of Total Institutions,” which says that such institutions (e.g., prisons) include deprivation of privacy as an essential ingredient in achieving their goal of mortification of the self [17, p. 40].

Security and Liberty trade-off

Vermeule and Posner, [Posner is an American law professor and son of the United States Court of Appeals for the Seventh Circuit judge Richard Posner. He is an expert in law and economics, international law, contract law, and bankruptcy, among other areas. As of 2014, he

was the 4th most-cited legal scholar in the United States.] [Vermeule is a graduate of Harvard College (A.B., 1990) and Harvard Law School. Vermeule clerked for Supreme Court Associate Justice Antonin Scalia and Judge David Sentelle of the U.S. Court of Appeals for the District of Columbia Circuit.] “Terror In The Balance” Pgs 21-26, **2007**

The general framework for our position is the tradeoff thesis. With other scholars, we argue that there is a tradeoff between security and liberty. The basic idea of the tradeoff is not original with us;⁷ indeed, it is one of the oldest theories of emergency powers. Our contribution is to analyze the comparative statics of institutional performance, of both government and courts, in striking the security-liberty balance during both emergencies and normal times. We pursue the tradeoff thesis to its ultimate conclusions without flinching at its implications, particularly its implications for judicial review of government action in times of emergency. The tradeoff thesis can be stated in simple terms. Both security and liberty are valuable goods that contribute to individual well-being or welfare. Neither good can simply be maximized without regard to the other. The problem from the social point of view is to optimize: to choose the joint level of liberty and security that maximizes the aggregate welfare of the population. Liberty, of course, has many different strands—there are many different kinds of negative and positive freedom—but those complexities are not material to our approach. As political theorist Jon Elster puts it, “[t]he metric for security can be established as the risk of harm. The metric for liberty is more difficult to determine, since the value includes such disparate components as freedom of speech, freedom of association, due process, and privacy. To get around this problem we basically have to ignore it, by stipulating that we have some way of aggregating the components of liberty into an aggregate measure.”⁸ In our view, any conceptual imprecision that arises from this aggregation does not affect the lower-level institutional problems we will discuss. To motivate the tradeoff theory, consider the wide range of real-world settings in which security and liberty, in its various aspects, trade off against one another: Security and privacy. Under the USA PATRIOT Act, passed in 2001 and renewed in 2005 and 2006, executive officials may inspect records held by businesses and other institutions, including the records held by libraries and bookstores about the activities of their patrons. As a doctrinal matter, such records do not carry a "reasonable expectation of privacy" sufficient to trigger the Fourth Amendment's protections against unreasonable searches and seizures. Nonetheless, civil libertarians have protested that this provision of the USA PATRIOT Act goes too far in authorizing governmental intrusion on personal information and chills the exercise of free speech. Security and due process. After the 9/11 attacks, President George W. Bush issued an executive order that created military commissions to try noncitizen detainees charged with being enemy combatants. The order granted defendants some procedural protections but far fewer than would be afforded in ordinary criminal trials; most notably, the fact finder is not a jury but a panel of military officers, and proof is by a less stringent standard than that used in criminal trials, which require proof beyond a reasonable doubt.⁹ Recently, the Supreme Court invalidated, on statutory grounds, part of the administration's scheme. Apart from trials before military commissions, the president has also claimed the authority to detain citizen or noncitizen enemy combatants for the duration of hostilities. A decision by the Supreme Court, Hamdi v. United States,¹⁰ placed some procedural restrictions on executive detention of enemy combatants but left open the possibility that military tribunals charged with reviewing combatant status, rather than judicial hearings, will satisfy those restrictions. In these respects, the law of military detention and military commissions sacrifices due process protections to expedite the handling of suspected enemy combatants. Security and free speech. In the United Kingdom, after the July 7, 2005, attacks on the London bus and train system, Parliament enacted major legislation, the Terrorism Act 2006, that curtails speech in the name of security. Among other broad provisions, the law prohibits statements that directly or indirectly encourage terrorist acts and proscribes organizations that glorify terrorism.¹¹ At the same time, however, the U.K. government has also sought to restrict speech along another margin, by prohibiting "hate speech" directed against Muslims.¹² We return to the latter point in chapter 3. These proposals build on existing laws,¹³ enacted after 9/11, that have allowed the conviction of radical Muslim clerics for inciting "racial and religious hatred" and violence.¹⁴ In the United States, a similar (albeit much more tentative) reform involves changes in FBI guidelines, after 9/11, that permitted agents to enter public places—including mosques—to monitor possible terrorist activity.¹⁵ Security and nondiscrimination. After 9/11, federal agencies engaged in the profiling of possible terrorists on racial, ethnic, national, and religious grounds. Examples include the special registration program, now defunct, which required aliens in the United States from a designated list of (almost exclusively) Muslim nations to register with the Immigration and Naturalization Service (INS); the Absconder Initiative, under which aliens from nations with substantial al Qaeda presence were targeted for removal; and Operation Liberty Shield, which subjected asylum applicants from such nations to mandatory detentions.¹⁶ These were explicit policies; some critics have also claimed that federal officials have engaged in covert ethnic or racial profiling in airport screening and other security-related searches.¹⁷ These are examples in which government has curtailed civil liberties or civil rights, as compared to some baseline set by preexisting rights or by the ordinary legal system, in the name of increased security during an emergency. Of course, nothing so far said shows that these policies are good, that these restrictions of civil liberty really have increased security, or that judges should uphold the relevant policies. They do show, however, that in many domains government officials believe or at least say that an increase in security requires restricting liberty. It is occasionally suggested that some examples of this sort involve tradeoffs within the domain of

security, rather than between security and liberty. If government officials take intrusive action in order to fight terrorism, this can cause a kind of insecurity to those affected. But putting the problem this way does not eliminate the tradeoff; it just relabels it. We might then speak of a tradeoff between "security type 1"—the social good that is increased to the extent that the terrorist threat is reduced—and "security type 2"—the social good that is reduced by governmental measures aimed at reducing the terrorist threat. It is not clear what this relabeling accomplishes, so we will stick with the conventional terms. The claim that security and liberty trade off against one another implies that respecting civil liberties often has real costs in the form of reduced security. Sometimes civil libertarians deny this; below, we offer an interpretation of that position. It is clear, however, that sometimes tangible security harms do in fact occur when claims of civil liberties are respected. Consider the following examples: 9/11 and the Intelligence Wall In 1978, Congress passed the Foreign Intelligence Surveillance Act,¹⁸ creating procedures for judicial oversight of searches and wiretaps in cases involving foreign agents and intelligence. The act provided that the "primary purpose" of the surveillance must be to gather foreign intelligence information. By a complex process of institutional change, the provision came to be interpreted—probably erroneously¹⁹—as having created a "wall," or barrier, to information sharing between intelligence and law enforcement. The rationale for the wall was civil libertarian, resting on fears that law enforcement would exploit intelligence information to bring ordinary criminal prosecutions; it was never clearly explained why such a practice would be bad. By the late 1990s, the prevailing understanding was that the wall was quite thick. This was itself an erroneous construal of internal Justice Department guidelines issued in 1995; but it was predictable that the guidelines would be misinterpreted by field agents in the FBI and elsewhere, as the guidelines had been made extremely complex and refined, in an effort to show punctilious respect for civil liberties.²⁰ Although counterfactuals are uncertain, it is plausible that, absent the wall, the 9/11 attacks would have been thwarted—as the 9/11 Commission found.²¹ The commission documented a series of instances in which the CIA possessed information that would have helped the FBI, whose agents were intermittently on the trail of the 9/11 attackers. At crucial junctures, the wall blocked information sharing between these agencies. Screening and Profiling The 9/11 Commission also found that the attacks could have been prevented by more aggressive screening and profiling at immigration points. "More than half of the 19 hijackers were flagged by the Federal Aviation Administration's profiling system when they arrived for their flights, but the consequence was that bags, not people, were checked."²² The commission urged both a more systematic combination of immigration enforcement functions with counterterrorism functions and expanded discretion for line officials to use discretionary, intuitive judgment to screen out threats.²³ These two reforms—combination rather than separation of functions and increased discretion for executive officers—are the sort of adjustment that governments routinely make during times of emergency and that are hallmarks of the administrative state where economic regulation is concerned, but that civil libertarians resist. Coercive Interrogation Statutes and treaties prohibit torture by the U.S. government; although the term is narrowly defined, the so-called McCain Amendment, enacted in 2006, also prohibits "cruel, inhuman and degrading" treatment.²⁴ The civil libertarian arguments for such prohibitions are obvious, and we evaluate them in chapter 6. Here, we merely note strong evidence that coercive interrogation, in both its stronger and weaker forms, saves lives (that could not be saved through other means at acceptable cost). The director of the Central Intelligence Agency has stated that coercive interrogation has produced actionable intelligence that has helped to thwart terrorist attacks;²⁵ in chapter 6, we recount evidence from Israel to the same effect and rebut critiques of that evidence. Quite probably, respecting the civil liberties of those who would otherwise be subject to coercive interrogation effectively causes the deaths of some unknown and unidentifiable set of terrorism victims. Free Speech (and Democracy) Consider the striking finding that press freedoms are positively correlated with greater transnational terrorism; nations with a free press are more likely to be targets of such terrorism.²⁶ Correlation is not causation, but there are obvious mechanisms that might explain this, such as the ability of terrorists to exploit free media coverage to spread fear and dramatize their cause and the freedom of the press to reveal security secrets. According to the 9/11 Commission's report, "al Qaeda's senior leadership had stopped using a particular means of communication almost immediately after a leak to the Washington Times."²⁷

27 The Bush administration says that the New York Times's leak of the National Security Agency's surveillance program has alerted terrorists that the United States is monitoring communications they may have believed were secure. And the British government believes that fundamentalist mullahs used sermons to recruit terrorists and encourage terrorism.²⁸ More broadly still, democracies in general are more often subjected to suicide attacks²⁹ and terrorism of all sorts, both domestic and transnational, while authoritarian regimes suffer much less from these harms.³⁰ Of course, not every issue of security policy presents such a tradeoff. At certain levels or in certain domains, security and liberty can be complements as well as substitutes. Liberty cannot be enjoyed without security, and security is not worth enjoying without liberty. And, in some circumstances, it is possible that there are policies, other than the ones that government adopts, that would increase both security and liberty. In some situations, rational policymakers can increase security at no cost to liberty, or increase liberty at no cost to security. But it is plausible to assume that advanced liberal democracies rarely overlook such opportunities, as we discuss shortly. Only a very dysfunctional government would decline to adopt policies that draw political support from both proponents of increased security and proponents of increased liberty.

Privacy - Deontology

Privacy is Kantian — key to human dignity

Buitelaar, 2014

J. C. Professor, Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands "Privacy and Narrativity in the Internet Era." *The Information Society* 30.4 (2014): 266-281.

There are manifold definitions and views of privacy. A seminal starting point is that of Warren and Brandeis (1890), namely, that privacy should be regarded as a general right to the immunity of the person. The right to privacy, as part of the more general right to the immunity of the person, is related to the right to one's personality. From this point of view it can be argued that the value of privacy is grounded in the principle of permitting and protecting an autonomous life (Kant 1996; Rössler 2001). The moral philosopher Kant was an early proponent of the view of the intrinsic value of human dignity (Kant 1996). Kant did, however, put a constraint on this view, namely, that humans owe themselves a duty of self-esteem but also a claim to and the duty to respect other humans. In Article 1 of the Universal Declaration of Human Rights, this Kantian principle of intrinsic human dignity is adopted, where the declaration states that all human beings are born free and equal in dignity and rights. This inherent dignity accounts for the possession of inalienable human rights. These rights find their origin in the capacity of the human being to reflect and make choices. A. R. Miller combines these two concepts to explain the importance of informational self-determination for preservation of privacy: "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to himself, a power that often is essential to maintaining social relationships and personal freedom" (Miller 1971, 25). If the individual can no longer determine to what extent they reveal themselves to the outside world, privacy is robbed of its core value, which is the opportunity to freely decide for oneself. The intrinsic dignity of the individual, from the liberal point of view at least, guarantees the autonomy to act freely and thus make the choices that allow a person to flourish and to develop their personality. This is also the principle of personal freedom enshrined in the German Constitution. Furthermore, privacy provides the individual with a safe place, where they can decide for themselves which relations they enter into. I maintain that they can only do so if they can control who has access to them. When this situation exists, they have the assurance that they can control the patterns of behavior they want to adopt.

Privacy good – Post Liberal

Privacy is key to self-articulation and critical independence.

Cohen, 2012

Julie E. Professor Georgetown University Law Center . Configuring the Networked Self : Law, Code, and the Play of Everyday Practice. Cumberland, RI, USA: Yale University Press, 2012. 149-50

Choices about privacy are choices about the scope for self-articulation. They are, therefore, choices about room to pursue the (unattainable, yet vitally important) liberal ideals of autonomy and critical independence. By this, I do not intend either to romanticize privacy or to readmit the liberal conception of privacy for fixed, autonomous selves through the back door. I mean only to make a narrower claim about the importance of some of liberalism's cultural and political aspirations. In a society committed at least to the desirability of the liberal ideal of self-determination, pervasive transparency and exposure are troubling because they constrain the range of motion for the development of subjectivity through both criticism and performance, and these conditions do not automatically cease to be troubling when the subjects of surveillance have indicated their willing surrender. Such a society values neither the docile bodies of Foucauldian theory, the assimilated denizens of Deleuzian systems of social control, nor the fragmentary, infinitely protean selves posited by performance theorists. It follows that choices about privacy are constitutive not simply of civil society, as some privacy theorists would have it, but of a particular type of civil society that prizes particular types of activities and particular types of subjects. In this respect, privacy functions as a sort of social Rorschach test, and not simply because norms about acceptable levels of privacy vary from culture to culture. Privacy exemplifies a culture's normative, collective commitments regarding the scope of movement, both literal and metaphorical, accorded to its members. The privacy that emerges as most important for fulfilling these commitments is best described as an interest in breathing room to engage in socially situated processes of boundary management. Privacy is not only about refusing access, visibility, or interference with particular decisions. It is also and more generally about preventing the seamless imposition of patterns predetermined by others. The privacy embedded in social practices of boundary management by situated subjects preserves room for the development of a critical, playful subjectivity that is always-already intersubjective— informed by the values of families, confidants, communities, and cultures. In a world with effective boundary management, however, there is play in the joints, and that is better than the alternative. And on this understanding, privacy implicates not only individual interests, but also collective interests in human flourishing and in the ongoing development of a vibrant culture. **Privacy's goal**, simply put, **is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep.**

Diminished privacy inhibits citizenship and ultimately democracy

Julie E. Cohen, Professor at Georgetown University Law Center, May

2013 “WHAT PRIVACY IS FOR”, Harvard Law Review, Volume 126, Number 7,

http://www.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf, JL @ DDI

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of

government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing. It is useful to begin by considering the relationship between citizenship and political and economic institutions. That institutions shape opportunities for the exercise of citizenship is, I think, an unremarkable proposition. Citizenship is more than a status. It is also a set of practices — voting, public debate, and so on — and so the scope for the practice of citizenship will be defined in part by the practices that existing institutions encourage, permit, or foreclose. Less often acknowledged is that institutions configure citizens, inculcating habits of mind and behavior that lend themselves more readily to certain types of practices than to others. Institutions shape not only the scope but also the capacity for citizenship. One of the lessons of American experiments in democracy building, beginning in the 1980s in the former Soviet Union and continuing most recently in Afghanistan and Iraq, is that democracy is difficult to jumpstart. Well-functioning state and market institutions cannot be built in the span of a grant-funded research project or a military campaign. Their rhythms and norms must be learned and then internalized, bringing into being the habits of mind and behavior that democratic citizenship requires.

Alt Fails – Aff key

Rejection of the liberal self fails – only recovering the value of privacy while understanding dangers of neoliberalism/etc can maintain the room for the development of subjectivity.

Cohen, 2013 Julie E., Professor Georgetown University Law Center “What Privacy Is For.” Harvard Law Review, Vol. 126, 2013. Available at SSRN: <http://ssrn.com/abstract=2175406>

I call this vision of selfhood a postliberal one because its relationship to liberalism requires something more difficult and much more productive than antagonism: a realistic appraisal of the liberal model’s undeniable faults and equally undeniable virtues. Liberal selfhood has an important role to play within privacy theory, but that role is different from the one that most privacy scholars have assumed. The liberal self is an aspiration — an idealized model of identity formation that can be approached only incompletely, if at all. This does not mean that all of its attributes are equally attractive and worth pursuing. Certain features of liberal selfhood have been roundly and justifiably critiqued, most notably its abstraction from embodied reality and its independence from relational ties.¹⁹ But others — most notably the liberal self’s capacity for critical independence of thought and judgment, its commitments to self-actualization and reason, and its aspiration to cosmopolitanism — are essential tools for identifying and pursuing the material and political conditions for self-fulfillment and more broadly for human flourishing.²⁰

But here we must come back to privacy, for the development of critical subjectivity is a realistic goal only to the extent that privacy comes into play. Subjectivity is a function of the interplay between emergent selfhood and social shaping; privacy, which inheres in the interstices of social shaping, is what permits that interplay to occur. Privacy is not a fixed condition that can be distilled to an essential core, but rather “an interest in breathing room to engage in socially situated processes of boundary management.”²¹ It enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making.

And once this point is established, privacy’s dynamism becomes clear. Lack of privacy means reduced scope for self-making — along the lines of the liberal ideal, or along other lines. Privacy does not negate social shaping. “In a world with effective boundary management, however, there is play in the joints, and that is better than the alternative. . . . Privacy’s goal, simply put, is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep.”²² Privacy will not always produce expressions of subjectivity that have social value, and here I mean expressly to leave open the question whether there might be particular types of privacy claims that do not merit protection or even respect.²³ Even so, privacy is one of the resources that situated subjects require to flourish.

The current system is a modulated society created by both the government and private sector that inhibits citizenship and democracy

Julie E. Cohen, Professor at Georgetown University Law Center, May

2013 “WHAT PRIVACY IS FOR”, Harvard Law Review, Volume 126, Number 7,

http://www.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf, JL @ DDI

While modulation could be undertaken by the government, within systems of informational capitalism it is more typically and effectively undertaken by private actors. Following Manuel Castells, I use “informational capitalism” to refer to the alignment of capitalism as a mode of production with informationalism as a mode of development: “[c]apitalism is oriented toward profit-maximizing, that is, toward increasing the amount of surplus appropriated by capital on the basis of the private control over the means of production and circulation,” while “informationalism is oriented . . . toward the accumulation of knowledge and towards higher levels of complexity in information processing.”³⁶ In the contemporary information economy, private sector firms like Google, Facebook, and data broker Acxiom use flows of information about consumer behavior to target advertisements, search results, and other content. Advertisers and other client firms rely on the flows of information to construct pricing and risk management templates that maximize their ability to identify high-value consumers and to extract surplus from all consumers. Still other firms rely on flows of information to authenticate access to places (such as workplaces and gaming environments), services (such as banking and telecommunications), and networked information resources (such as software and databases). Information from and about consumers feeds into sophisticated systems of predictive analytics so that surveillant attention can be personalized more precisely and seamlessly. Government is an important secondary beneficiary of informational capitalism, routinely accessing and using flows of behavioral and communications data for its own purposes. The embedding of surveillance functionality within market and political institutions produces “surveillant assemblage[s],” in which information flows in circuits that serve the interests of powerful entities, both private and public.³⁷ In the modulated society, surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power. The surveillant assemblages of informational capitalism do not have as their purpose or effect the “normalized soul training” of the Orwellian nightmare.³⁸ They beckon with seductive appeal. Individual citizen consumers willingly and actively participate in processes of modulation, seeking the benefits that increased personalization can bring. For favored consumers, these benefits may include price discounts, enhanced products and services, more convenient access to resources, and heightened social status.³⁹ Within surveillant assemblages, patterns of information flow are accompanied by discourses about why the patterns are natural and beneficial, and those discourses foster widespread internalization of the new norms of information flow. For all of these reasons, a critique of surveillance as privacy invasion “does not do justice to the productive character of consumer surveillance.”⁴⁰ Modulation is a mode of privacy invasion, but it is also a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories. Yet to speak of networked processes of surveillance and modulation in the industrial era vernacular, as systems for “manufacturing consent,” would be too crude.⁴¹ Rather, in a much more subtle process of continual feedback, stimuli are tailored to play to existing inclinations, nudging them in directions that align with profit-maximizing goals.⁴² So too with political inclinations; particularly as search and social networking become more seamlessly integrated, networked citizen-consumers move within personalized “filter bubbles” that conform the information environment to their political and ideological commitments.⁴³ This is conducive to identifying and targeting particular political constituencies,⁴⁴ but not necessarily to fostering political dialogue among diverse constituencies in ways that might enable them to find common ground. By these increasingly ordinary processes, both public and private regimes of surveillance and modulation diminish the capacity for democratic self-government. To be clear, I do not mean to suggest that surveillance is never necessary, nor that it is inevitably pernicious. Governments require some kinds of knowledge about people to govern effectively. I also want expressly to leave open the question whether national security imperatives might justify certain types of heightened surveillance. But in for a penny should not mean in for a pound. Citizens of the modulated society are not the same citizens that the liberal democratic political tradition assumes, nor do their modulated preferences even approximately resemble the independent decisions, formed through robust and open debate, that liberal democracy requires to sustain and perfect itself. The modulated society is the consummate social and intellectual rheostat, continually adjusting the information environment to each individual’s comfort level. Liberal democratic citizenship requires a certain amount of discomfort — enough to motivate citizens to pursue improvements in the realization of political and social ideals. The modulated citizenry lacks the wherewithal and perhaps even the desire to practice this sort of citizenship. If this sounds like science fiction, it shouldn’t. Like the liberal self, liberal democracy has always been an ideal to be pursued and approximated. A polity’s ability to approximate liberal democracy has both institutional and material preconditions. In the generations following the framing of the U.S. Constitution, those who sought to build a functioning liberal democracy had to contend with the gulf between liberalism’s

aspirations to egalitarianism and the concentration of political power in an entitled minority of white male property and slave owners. In the generations to come, those who seek to maintain a functioning liberal democracy will need to contend with the gulf between liberalism's aspirations to self-government by an informed and vigilant citizenry and the relatively blunted capacities of a modulated citizenry. To put the point a different way, the liberal self and the liberal democratic society are symbiotic ideals. Their inevitably partial, imperfect realization requires habits of mind, of discourse, and of self-restraint that must be learned. Those are the very same habits that support a mature, critical subjectivity, and they require privacy to form. The institutions of modulated democracy, which systematically eradicate breathing space for dynamic privacy, deny both critical subjectivity and critical citizenship the opportunity to flourish. The liberal democratic society will cease to be a realistic aspiration unless serious attention is given to the conditions that produce (aspiring) liberal selves.

Perm – Semantic Discontinuity

Perm do both- Semantic Discontinuity and contradiction is necessary to create zones of privacy

Julie E. Cohen, Professor at Georgetown University Law Center, May

2013 “WHAT PRIVACY IS FOR”, Harvard Law Review, Volume 126, Number 7,

http://www.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf, JL @ DDI

Second and relatedly, effective protection for dynamic privacy requires affirmative measures designed to preserve and widen interstitial spaces within information processing practices on both sides of the public-private divide. Adequate breathing room for personal boundary management exists when legal, technical, and commercial architectures are characterized by a condition that I have called semantic discontinuity.⁸¹ Semantic discontinuity is “the opposite of seamlessness: it is a function of interstitial complexity within the institutional and technical frameworks that define information rights and obligations and establish protocols for information collection, storage, processing, and exchange.”⁸² Semantic discontinuity helps to separate contexts from one another, thereby preserving breathing room for personal boundary management and for the play of everyday practice. It is a condition that we should not lightly leave behind. A regulatory agenda for effective privacy protection should include the development of criteria for assessing semantic discontinuity and strategies for creating and maintaining adequate baseline levels.

Reinforcing these gaps in coverage, creating semantic discontinuity, allows for situated subjects to thrive and protects privacy

(Ohm 13, Paul Ohm, 3-8-2012, "Mind the Gap (Symposium on Configuring the Networked Self)," Professor of Law at the Georgetown University Law Center, No Publication, <http://concurringopinions.com/archives/2012/03/mind-the-gap.html#more-59174>)

In this post, I want to focus on “semantic discontinuity,” the label Cohen gives to the most novel and interesting construct in the book. Semantic discontinuity is one of three “principles that should inform the design of legal and technical architectures,” along with “access to knowledge” and “operational transparency.” In her words, “semantic discontinuity is the opposite of seamlessness. . . . It is a function of interstitial complexity within . . . institutional and technical frameworks.” It serves a “vital” function, “creat[ing] space for the semantic indeterminacy that is a vital and indispensable enabler of the play of everyday practice.” (Kindle location 4288)

In other words, semantic discontinuity valorizes noise, inefficiency, constraints, and imperfections. As this list illustrates, the most striking thing about this book is the size of the herd of sacred cows it leads to the slaughter. But, to repeat the question Cohen asked during this symposium, how do you operationalize semantic discontinuity? Focusing on privacy law, semantic discontinuity leads to what she calls a principle of “just aggregation,” which will animate “interventions aimed at preserving the commercial, technical, and spatial disconnects that separate contexts from one another.” (Kindle 4843) To put it more metaphorically and concretely, “privacy law and policy should reinforce and widen gaps within the semantic web so that situated subjects can thrive.” (Kindle 4765) This is heady stuff, and I really love it. I am attracted to this metaphor, that privacy law (and copyright law, and unauthorized access law) must protect, create, or widen “gaps” in enforcement, coverage, and definition. It provides a goal with an easy-to-

understand label, built upon a deep theoretical base, for defending aggressive regulatory interventions that are likely to improve privacy.

Resistance is not achieved through a set goal or method, rather these gaps are created through acting in unexpected methods, reinforcing contradictions to create unpredictable ways

(Ohm 13, Paul Ohm, 3-8-2012, "Mind the Gap (Symposium on Configuring the Networked Self)," Professor of Law at the Georgetown University Law Center, No Publication, <http://concurringopinions.com/archives/2012/03/mind-the-gap.html#more-59174>)

I think we need to do more work to better explain what the “gaps” of information privacy law should look like. As a modest start, I would like to make a claim about the nature of these gaps, one I see woven throughout the book, but never stated plainly enough: we will be forced to carve out these gaps using machetes not scalpels. It seems hard, almost by definition, to design legal or technological architectures finely-tuned to bolster “the play of everyday practice” and foster “evolving subjectivity.” The very ideas of play and subjectivity seem tied in important ways to the unexpected. As Cohen puts it: [A]n important function of play is the opening of spaces or gaps into which evolving subjectivity (and also evolving collectivity) might move. Evolving subjectivity, or the everyday practice of self, responds to the play-of-circumstances in unanticipated and fundamentally unpredictable ways. . . [T]he play-of-circumstances operates as a potent engine of cultural dynamism, mediating both evolving subjectivity and evolving collectivity, and channeling them in unexpected ways. (Kindle 2591) (emphases added). By calling for machetes, I understand that I might be confusing the thing we are trying to produce with the tool we need to produce it. It may be that a precisely defined, narrowly tailored, and rigidly constructed set of “gaps” in law or technology might somehow best foster “fundamentally unpredictable” results. But I doubt it. It seems to me that the type of architecture best suited to channeling responses “in unexpected ways” will themselves be unpredictably lumpy, misshapen and even somewhat illogical. As Cohen explains in the most bumper-sticker-worthy passage in the book, **“privacy consists in setting of limits precisely where logic would object to drawing lines.”** (Kindle 4846)

Greatest Hits of Rights Cards

This is not a question of uniqueness – it is a linear disadvantage – infringements on liberty must be rejected at all costs or we forfeit to totalitarianism.

Petro, Toledo Law Review, **1974** (Sylvester, Spring, page 480)

However, one may still insist, echoing Ernest Hemingway - "I believe in only one thing: liberty." And it is always well to bear in mind David Hume's observation: "It is seldom that liberty of any kind is lost all at once." Thus, it is unacceptable to say that the invasion of one aspect of freedom is of no import because there have been invasions of so many other aspects. That road leads to chaos, tyranny, despotism, and the end of all human aspiration. Ask Solzhenitsyn. Ask Milovan Djilas. In sum, if one believed in freedom as a supreme value and the proper ordering principle for any society aiming to maximize spiritual and material welfare, then every invasion of freedom must be emphatically identified and resisted with undying spirit.

Don't evaluate the reactions of others to your ethical decision – that method of calculation invites the worst form of nihilism and ongoing atrocities

Alan **Gewirth**, Professor Emeritus of Philosophy at the University of Chicago, PhD in philosophy from Columbia University, **1982**, Human Rights: Essays on Justification and Application, p. 229-230

None of the above distinctions, then, serves its intended purpose of defending the absolutist against the consequentialist. They do not show that the son's refusal to torture his mother to death does not violate the other persons' rights to life and that he is not morally responsible for their deaths. Nevertheless, the distinctions can be supplemented in a way that does serve to establish these conclusions. The required supplement is provided by the principle of the intervening action. According to this principle, when there is a causal connection between some person A's performing some action (or inaction) X and some other person C's incurring a certain harm Z, A's moral responsibility for Z is removed if, between X and Z, there intervenes some other action Y of some person B who knows the relevant circumstances of his action and who intends to produce Z or who produces Z through recklessness. The reason for this removal is that B's intervening action Y is the more direct or proximate cause of Z and, unlike A's action (or inaction), Y is the sufficient condition of Z as it actually occurs." An example of this principle may help to show its connection with the absolutist thesis. Martin Luther King Jr. was repeatedly told that because he led demonstrations in support of civil rights, he was morally responsible for the disorders, riots, and deaths that ensued and that were shaking the American Republic to its foundations." By the principle of the intervening action, however, it was King's opponents who were responsible because their intervention operated as the sufficient conditions of the riots and injuries. King might also have replied that the Republic would not be worth saving if the price that had to be paid was the violation of the civil rights of black Americans. As for the rights of the other Americans to peace and order, reply would be that these rights cannot justifiably be secured at the price of the rights of blacks. It follows from the principle of the intervening action that it is not the son but rather the terrorists who are morally as well as causally responsible for the many deaths that do or may ensue on his refusal to torture his mother to death. The important point is not that he lets these persons die rather than kill them, or that he does not harm them but only fails to help them or that he intends their deaths only obliquely but not directly. The point is rather that it is only through the intervening lethal actions of the terror that his refusal eventuates in the many deaths. Since the moral responsibility is not the son's, it does not affect his moral duty not to torture his mother to death, so that her correlative right remains absolute.

Violations of liberty negate the value to existence.

Raz, Philosopher, **1986**

(Joseph, *The Morality of Freedom*, page 307)

One way to test the thesis of the primacy of action reasons is to think of a person who is entirely passive and is continuously led, cleaned, and pumped full with hash, so that he is perpetually content, and wants nothing but to stay in the same condition. It's a familiar imaginary horror. How do we rank the success of such a life? It is not the worst life one can have. It is simply not a life at all. It lacks activity, it lacks goals. To the extent that one is tempted to judge it more harshly than that and to regard it as a 'negative life' this is because of the wasted potentiality. It is a life which could have been and was not. We can isolate this feature by imagining that the human being concerned is mentally and physically effected in a way which rules out the possibility of a life with any kind of meaningful pursuit in it. Now it is just not really a life at all. This does not preclude one from saying that it is better than human life. It is simply sufficiently unlike human life in the respects that matter that we regard it as only a degenerate case of human life. But clearly not being alive can be better than that life.

Rights must come first or they will always be violated in the name of security

George **Kateb**, Professor of Politics at Princeton University, 1992, *The Inner Ocean: Individualism and Democratic Culture*, p. 5

All I wish to say now is that unless rights come first they are not rights. They will tend to be sacrificed to some purpose deemed higher than the equal dignity of every individual. There will be little if any concept of the integrity or inviolability of each individual. The group or the majority or the good or the sacred or the vague fixture will be preferred. The beneficiaries will be victimized along with the victims because no one is being treated as a person who is irreplaceable and beyond value. To make rights anything but primary, even though in the name of human dignity, is to injure human dignity.

Utilitarian ethics sacrifice the individual at the altar of maximization of general utility making the grossest rights violations both inevitable and frequent

Christopher H. **Schroeder**, Professor of Law, Duke University; Visiting Professor of Law, UCLA 1985-86, 1986, *Columbia Law Review, Rights Against Risks*, 86 Colum. L. Rev. 495

The anxiety to preserve some fundamental place for the individual that cannot be overrun by larger social considerations underlies what H.L.A. Hart has aptly termed the "distinctively modern criticism of utilitarianism,"⁵⁸ the criticism that, despite its famous slogan, "everyone [is] to count for one," utilitarianism ultimately denies each individual a primary place in its system of values. Various versions of utilitarianism evaluate actions by the consequences of those actions to maximize happiness, the net of pleasure over pain, or the satisfaction of desires.⁶⁰ Whatever the specific formulation, the goal of maximizing some measure of utility obscures and diminishes the status of each individual. It reduces the individual to a conduit, a reference point that registers the appropriate "utiles," but does not count for anything independent of his monitoring function.⁶¹ It also produces moral requirements that can trample an individual, if necessary, to maximize utility, since once the net effects of a proposal on the maximand have been taken into account, the individual is expendable. Counting pleasure and pain equally across individuals is a laudable proposal, but counting only pleasure and pain permits the grossest inequities among individuals and the [*509] trampling of the few in furtherance of the utility of the many. In sum, utilitarianism makes the status of any individual radically contingent. The individual's status will be preserved

only so long as that status contributes to increasing total utility. Otherwise, the individual can be discarded.

The disads serve to destroy the rights of individuals – violating rights in the name of survival destroys the value to life

Daniel Callahan, Institute of Society and Ethics, 1973, The Tyranny of Survival, p. 91-93

The value of survival could not be so readily abused were it not for its evocative power. But abused it has been. In the name of survival, all manner of social and political evils have been committed against the rights of individuals, including the right to life. The purported threat of Communist domination has for over two decades fueled the drive of militarists for ever-larger defense budgets, no matter what the cost to other social needs. During World War II, native Japanese-Americans were herded, without due process of law, to detention camps. This policy was later upheld by the Supreme Court in Korematsu v. United States (1944) in the general context that a threat to national security can justify acts otherwise blatantly unjustifiable. The survival of the Aryan race was one of the official legitimations of Nazism. Under the banner of survival, the government of South Africa imposes a ruthless apartheid, heedless of the most elementary human rights. The Vietnamese war has seen one of the greatest of the many absurdities tolerated in the name of survival: the destruction of villages in order to save them. But it is not only in a political setting that survival has been evoked as a final and unarguable value. The main rationale B. F. Skinner offers in *Beyond Freedom and Dignity* for the controlled and conditioned society is the need for survival. For Jacques Monod, in *Chance and Necessity*, survival requires that we overthrow almost every known religious, ethical and political system. In genetics, the survival of the gene pool has been put forward as sufficient grounds for a forceful prohibition of bearers of offensive genetic traits from marrying and bearing children. Some have even suggested that we do the cause of survival no good by our misguided medical efforts to find means by which those suffering from such common genetically based diseases as diabetes can live a normal life, and thus procreate even more diabetics. In the field of population and environment, one can do no better than to cite Paul Ehrlich, whose works have shown a high dedication to survival, and in its holy name a willingness to contemplate governmentally enforced abortions and a denial of food to surviving populations of nations which have not enacted population-control policies. For all these reasons it is possible to counterpose over against the need for survival a "tyranny of survival." There seems to be no imaginable evil which some group is not willing to inflict on another for sake of survival, no rights, liberties or dignities which it is not ready to suppress. It is easy, of course, to recognize the danger when survival is falsely and manipulatively invoked. Dictators never talk about their aggressions, but only about the need to defend the fatherland to save it from destruction at the hands of its enemies. But my point goes deeper than that. It is directed even at a legitimate concern for survival, when that concern is allowed to reach an intensity which would ignore, suppress or destroy other fundamental human rights and values. The potential tyranny survival as value is that it is capable, if not treated sanely, of wiping out all other values. Survival can become an obsession and a disease, provoking a destructive singleness of mind that will stop at nothing. We come here to the fundamental moral dilemma. If, both biologically and psychologically, the need for survival is basic to man, and if survival is the precondition for any and all human achievements, and if no other rights make much sense without the premise of a right to life—then how will it be possible to honor and act upon the need for survival without, in the process, destroying everything in human beings which makes them worthy of survival. To put it more strongly, if the price of survival is human degradation, then there is no moral reason why an effort should be made to ensure that survival. It would be the Pyrrhic victory to end all Pyrrhic victories.

Policymakers cannot take into account improbable worst case scenarios like the disads – worst case scenarios do not prove the undesirability of the plan

Nicholas **Rescher**, Professor of Philosophy at the University of Pittsburgh, **1983**, Risk: A Philosophical Introduction to the Theory of Risk Evaluation and Management, p. 50

The "worst possible case fixation" is one of the most damaging modes of unrealism in deliberations about risk in real-life situations. Preoccupation about what might happen "if worst comes to worst" is counterproductive whenever we proceed without recognizing that, often as not, these worst possible outcomes are wildly improbable (and sometimes do not deserve to be viewed as real possibilities at all). The crux in risk deliberations is not the issue of loss "if worst comes to worst" but the potential acceptability of this prospect within the wider framework of the risk situation, where we may well be prepared "to. take our chances," considering the possible advantages that beckon along this route. The worst threat is certainly something to be borne in mind and taken into account, but it is emphatically not a satisfactory index of the overall seriousness or gravity of a situation of hazard.

Surveillance Bad – Totalitarianism

The impact is Totalitarianism, the loss of autonomy due to surveillance enables “turnkey totalitarianism,” destroying democracy.

Haggerty, 2015

Kevin D. Professor of Criminology and Sociology at the University of Alberta, “What’s Wrong with Privacy Protections?” in A World Without Privacy: What Law Can and Should Do? Edited by Austin Sarat p. 230

Still others will say I am being alarmist. My emphasis on the threat of authoritarian forms of rule inherent in populations open to detailed institutional scrutiny will be portrayed as overblown and over dramatic, suggesting I veer towards the lunatic fringe of unhinged conspiracy theorists.⁶⁶ But one does not have to believe secret forces are operating behind the scenes to recognize that our declining private realm presents alarming dangers. Someone as conservative and deeply embedded in the security establishment as William Binney – a former NSA senior executive – says the security surveillance infrastructure he helped build now puts us on the verge of “turnkey totalitarianism.”⁶⁷ The contemporary expansion of surveillance, where monitoring becomes an ever-more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger of this situation is how our existing surveillance practices can be turned to oppressive uses. From this point forward our expanding surveillance infrastructure stands as a resource to be inherited by future generations of politicians, corporate actors, or even messianic leaders. Given sufficient political will this surveillance infrastructure can be re-purposed to monitor – in unparalleled detail – people who some might see as undesirable due to their political opinions, religion, skin color, gender, birthplace, physical abilities, medical history, or any number of an almost limitless list of factors used to pit people against one another. The twentieth century provides notorious examples of such repressive uses of surveillance. Crucially, those tyrannical states exercised fine-grained political control by relying on surveillance infrastructures that today seem laughably rudimentary, comprised as they were of paper files, index cards, and elementary telephone tapping.⁶⁸ It is no more alarmist to acknowledge such risks are germane to our own societies than it is to recognize the future will see wars, terrorist attacks, or environmental disasters – events that could themselves prompt surveillance structures to be re-calibrated towards more coercive ends. Those who think this massive surveillance infrastructure will not, in the fullness of time, be turned to repressive purposes are either innocent as to the realities of power, or whistling past a graveyard. But one does not have to dwell on the most extreme possibilities to be unnerved by how enhanced surveillance capabilities invest tremendous powers in organizations. Surveillance capacity gives organizations unprecedented abilities to manipulate human behaviors, desires, and subjectivities towards organizational ends – ends that are too often focused on profit, personal aggrandizement, and institutional self-interest rather than human betterment.

Privacy restrains tyrannical governments through critical strategization

Goold, 10- Associate Professor at the University of British Columbia Faculty of Law and a Research Associate at the Oxford University Centre for Criminology, (Benjamin, “How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy”, OVERVÅKNING I EN RETTSSTAT - SURVEILLANCE IN A CONSTITUTIONAL GOVERNMENT, 2010, PDF, page 41-44)//AP

As has already been noted, one of the main reasons why we value privacy so highly is because it is essential to the exercise of individual autonomy and the proper development of the self. But while it is perhaps easy to see how privacy is fundamentally important to each of us as individuals, it is also crucial to remember that privacy has a vital public dimension as well. As Priscilla Regan argues in Legislating Privacy, the value of privacy stretches well beyond its usefulness in helping individuals maintain a sense of dignity or construct personal relationships. For Regan, privacy is also important because it serves “common, public, and collective purposes”.⁵⁵ Drawing on John Stuart Mill’s writings on the struggle between liberty and authority, Regan argues that privacy is essential to the maintenance of democracy, primarily because it ensures that citizens are able to hold elected governments to account and place limits on the expansion of the state: A public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on government or on the use of power ... Privacy in this sense is not important just to individual liberty but also to civil or social liberty because it helps to establish the boundaries for the exercise of power.⁵⁶ How is this limitation achieved? How does protecting privacy impose limits on the exercise of power by the state? On the one hand, privacy helps to place limits on the state by making it clear that there are certain places the state cannot go and certain things it cannot expect to know. As Regan points out, in the US context this view of privacy has been crucial to the development of the Fourth Amendment, and the development of rules regarding the investigatory powers of the police and other law enforcement agencies. As Justice Felix Frankfurter observed over 60 years ago in *Wolf v. Colorado*, the “security of one’s privacy against intrusion by the police – which is at the core of the Fourth Amendment – is basic to a free society”.⁵⁷ More crucially, however, privacy’s public value also stems from its importance to the exercise of other, more obviously political rights. It is difficult imagine, for example, being able to enjoy freedom of expression, freedom of association, or freedom of religion without some accompanying right to privacy. Individuals not only need to be able to be alone with their own thoughts, but they also need to be free to share those thoughts with others without being subject to the watchful, possibly critical, eye of the state. Indeed, one of the greatest dangers of unfettered mass surveillance – particularly mass covert surveillance such as communications monitoring – is the potential chilling effect on political discourse, and on the ability of both individuals and groups to express their views through comment, protest and other forms of peaceful civil action.⁵⁸ Sadly, we are already beginning to see signs in countries like the UK and the US of surveillance being used as a means of suppressing criticism and political speech. Although it is often claimed that the police record public demonstrations and rallies with a view to detecting and investigating possible criminal and terrorist behavior, the reality is that such tactics are now commonly used at almost every type of protest, ranging from anti-war marches to environmental group protests, often not with the intention of arresting or charging individuals with a crime, but rather in the hope that it will cause them to alter their behavior and become effectively self-policing. Equally, the mass and routine monitoring of electronic communications like email – as revealed in a recent European Court of Human Rights judgment against the UK – may severely affect the ability of individuals to share their views with others or to be willing to criticize the government in their private communications.⁵⁹ By ensuring that there is a limit on what the state can know about us, privacy not only helps to protect individual autonomy, but also leaves us free to use that autonomy in the exercise of other fundamental rights like the right to free speech. As Thomas Emerson has argued: In its social impact a system of privacy is vital to the working of the democratic process. Democracy assumes that the individual citizen will actively and independently participate in making decisions and operating in the institutions of society. An individual is capable of such a role only if he can at some points separate himself from the pressure and conformities of collective life.⁶⁰

Surveillance Bad – Democracy -Chilling Effect

Surveillance creates conformity, that chills dissent.

Desai, 2014

Deven R. Associate Professor of Law and Ethics, Georgia Institute of Technology, Scheller College of Business; J.D. Yale Law School; "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding." *Notre Dame L. Rev.* 90 (2014): 579.

As scholars of association might say, with surveillance the room to disagree about what the common good is diminishes. n261 [*623] One way to think of the problem is as the need for anonymity. Christopher Slobogin has explained that perspective: "Anonymity in public promotes freedom of action and an open society. Lack of public anonymity promotes conformity and an oppressive society." n262 He calls this problem "public privacy." n263 That seeming oxymoron captures the need to be public, yet private from government oversight. It is anonymity to the government that matters. That anonymity may be based on protections from direct surveillance or protections from the government accessing third party, private sector records of recent and past communications and acts. Julie Cohen has shown why that is so. n264 Surveillance changes behaviors, because "the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior." n265 Instead of robust, diverse, and challenging ideas, we will favor the "the bland and the mainstream." n266 We end up with a diminished "capacity to act and to decide," which leads to "the highest possible degree of compliance with [what the state determines is] the model ... citizen." n267 This problem is a type of chilling effect. n268

Surveillance destroys democracy because it chills free expression and dissent.
Schneier 2015

Bruce Schneier a fellow at the Berkman Center for Internet and Society at Harvard Law School, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the CTO at Resilient Systems, 3/2/15, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, p, 90

Surveillance has a potentially enormous chilling effect on society. US Supreme Court Justice Sonia Sotomayor recognized this in her concurring opinion in a 2012 case about the FBI's installing a GPS tracker in someone's car. Her comments were much broader: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantity of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society." Columbia University law professor Eben Moglen wrote that "omnipresent invasive listening creates fear. And that fear is the enemy of reasoned, ordered liberty." Surveillance is a tactic of intimidation. In the US, we already see the beginnings of this chilling effect. According to a Human Rights Watch report, journalists covering stories on the intelligence community, national security, and law enforcement have been significantly hampered by government surveillance. Sources are less likely to contact them, and they themselves are worried about being prosecuted. Human Rights Watch concludes that stories in the national interest that need to be reported don't get reported, and that the public is less informed as a result. That's the chilling effect right

there. Lawyers working on cases where there is some intelligence interest—foreign government clients, drugs, terrorism—are also affected. Like journalists, they worry that their conversations are monitored and that discussions with their clients will find their way into the prosecution's hands. Post-9/11 surveillance has caused writers to self-censor. They avoid writing about and researching certain subjects; they're careful about communicating with sources, colleagues, or friends abroad. A Pew Research Center study conducted just after the first Snowden articles were published found that people didn't want to talk about the NSA online. A broader Harris poll found that nearly half of Americans have changed what they research, talk about, and write about because of NSA surveillance. Surveillance has chilled Internet use by Muslim Americans, and by groups like environmentalists, gun-rights activists, drug policy advocates, and human rights workers. After the Snowden revelations of 2013, people across the world were less likely to search personally sensitive terms on Google. A 2014 report from the UN High Commissioner on Human Rights noted, "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. This isn't paranoia. In 2012, French president Nicolas Sarkozy said in a campaign speech, "Anyone who regularly consults internet sites which promote terror or hatred or violence will be sentenced to prison." This fear of scrutiny isn't just about the present; it's about the past as well. Politicians already live in a world where the opposition follows them around constantly with cameras, hoping to record something that can be taken out of context. Everything they've said and done in the past is pored through and judged in the present, with an exactitude far greater than was imaginable only a few years ago. Imagine this being normal for every job applicant.

Surveillance Bad – Democracy

Democratic Societies cannot function with secret governmental programs

Neil M. Richards, Professor of Law, Washington University School of Law, 05-20-13

{Harvard Law Review: Volume 126, Number 7 - May 2013: The Dangers of Surveillance} Pgs. 1959-1961

Democratic societies should prohibit the creation of any domestic surveillance programs whose existence is secret. In a democratic society, the people, and not the state apparatus, are sovereign. In American law, this tradition goes back to James Madison, and it lies at the very heart of both First Amendment theory and American constitutionalism itself.¹²³ These principles are reflected at the core of modern information law. For example, the Supreme Court has made clear that the federal Freedom of Information Act¹²⁴ protects at its core the “citizens’ right to be informed about ‘what their government is up to.’”¹²⁵ As Professor Henry Steele Commager put it aptly, “[t]he generation that made the nation thought secrecy in government [to be] one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to.”¹²⁶ The illegitimacy of secret surveillance also lies at the heart of information-privacy law, which remains guided by the “Fair Information Practices” drafted by the U.S. Department of Health, Education, and Welfare in 1973.¹²⁷ The Code of Fair Information Practices recommended by the Department has continued to influence information privacy law throughout the world,¹²⁸ and the first of its five principles is the commitment that “there must be no personal-data recordkeeping systems whose very existence is secret.”¹²⁹ Requiring the existence of domestic-surveillance programs to be disclosed solves a practical problem that has bedeviled courts trying to assess legal challenges to secret surveillance programs. How can plaintiffs prove injury if the government is not required to admit whether surveillance exists in the first place? A prohibition on secret surveillance programs solves this problem. When government programs are public — when we have no secret surveillance — courts will be able to assess their legality in the open. The NSA wiretapping program was hard to challenge because its details were shrouded in secrecy, denials, and unassessable invocations of national security interests.¹³⁰ At the same time, its shadowy nature created an even greater threat to intellectual privacy in particular because no one knew if her telephone calls were being listened to or not. Requiring disclosure of the existence and capabilities of domestic-surveillance programs to the general public makes them amenable to judicial and public scrutiny to ensure their compatibility with the rule of law. At the same time, the prohibition on secret surveillance systems does not require the government to notify individual targets of surveillance that they are being watched. But fundamentally, surveillance requires legal process and the involvement of the judiciary to ensure that surveillance is targeted, justified, and no more extensive than is necessary. Thus, while covert domestic surveillance can be justified in discrete (and temporary) instances when there is advance judicial process, blanket surveillance of all Internet activity menaces our intellectual privacy and gives the government too much power to blackmail or discriminate against the subjects of surveillance. In a free society, all forms of surveillance must be ultimately accountable to a self governing public, and for this reason, secret domestic-surveillance programs of any kind are illegitimate.

Surveillance destroys democracies

Neil M. Richards, Professor of Law, Washington University School of Law, 05-20-13

{Harvard Law Review: Volume 126, Number 7 - May 2013: The Dangers of Surveillance} Pgs. 1951-1952

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries. But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.⁹⁵ Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.⁹⁶ Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

Democracy good – Growth

Democracy is key to growth – encourages political stability

Feng 97 (Yi Feng, Luther Lee Jr. Memorial Chair in Government at Claremont Graduate University and PhD in Political Science at the University of Rochester, “Democracy, Political Stability and Economic Growth”, July 1997, British Journal of Political Science / Volume 27 / Issue 03 / pp 413 – 414) //mL

This article contributes to the study of the political economy of growth in three respects. First, the simultaneous approach to the study of the relationships between growth and political stability, and between growth and democracy, allows us to identify the indirect effect of democracy on growth through its impact on political stability. Secondly, this work isolates three discrete forms of political stability, thus clarifying earlier misconceptions about regime stability and government stability. The findings reported here support Alesina et al. in the sense that regime change affects growth adversely.⁸⁰ At the same time, they also replicate Londregan and Poole's evidence that growth has a negative effect on coups d'e'tat.⁸¹ Additionally, they show support for the argument that growth increases the probability of the same party remaining in power.⁸² Thus, the inclusion of democracy as an endogenous variable strengthens the feedback between growth and political instability. Thirdly, the ambiguous total effect of democracy on growth is exposed. While democracy may have a negative direct effect on growth, it can have a positive indirect effect on growth through its impact on the probability of regular and irregular government changes. On the one hand, major regular government change has a positive effect on growth and regime change has a negative effect on growth; on the other, democracy has a positive impact on major regular government change and a negative impact on regime change. Overall, therefore, democracy promotes growth indirectly by inducing major regular government change and inhibiting irregular government change. By differentiating political instability and the impact on political instability of democracy, this article shows that the ‘compatibility school’ and the ‘conflict school’ can both be correct, depending on the balance between the direct and indirect effects of democracy on growth. Democracy tends to have a positive effect on economic growth by inhibiting extra-constitutional political change and favouring constitutional political change. Democracy provides a stable political environment which reduces unconstitutional government change at the macro level; yet along with regime stability, democracy offers flexibility and the opportunity for substantial political change within the political system. Together with the positive indirect effects on growth of democracy through investment and education, this juxtaposition of macropolitical certainty and micropolitical adjustability may be regarded as the ultimate basis for sustainable economic growth and expansion.

Global Totalitarianism

The Internet has turned into a global spying regime

William Marsden, Montreal Gazette, March 15, 2015, Cyber-spying thrives as technology makes it easier; Canada was likely among the countries who shared citizens' personal data, p. A7

Eighteen months ago, National Security Agency cyber spy Edward Snowden shocked the world when he emerged from the shadows to reveal the biggest government surveillance program mankind has ever known. **By collecting bulk data on phone calls, emails and other social media communications, the U.S. government was essentially monitoring the private lives of pretty well everybody with a phone and/or Internet connection.** Americans, Canadians, Europeans, Asians - it didn't matter. We had all come under suspicion. Boosted by a decades-old intelligence gathering and sharing agreement called the "Five Eyes" - U.S., Canada, Britain, Australia and New Zealand - there was every reason to believe that not only was the U.S. sharing this information with its partners, but also these countries were watching their citizens with similar vigour. The blowback was ferocious, and U.S. President Barack Obama eventually promised action in 2014. The expectation was that the NSA would be reined in. Well, 2014 has come and gone. What's happened? "Really shockingly little has been done," said Liza Goitein, a surveillance law expert at the Brennan Center for Justice. Bottom line is the government is still collecting your data. **The Internet, once viewed as freedom's friend, has now become suspicious, a digitalized spy regime shattering traditional concepts of personal privacy and civil rights - and perhaps even democracy.** When even the most backward of countries - North Korea - can hack into a large high-tech company like Sony, what does that say about the future? Harold Polham, a political scientist who specializes in surveillance at Dickinson College in Pennsylvania, has acquiesced to this new reality because it is the only world they know. "In the next 10 years we may have lost our ability to put an end to this," he said. "It'll be a fait accompli."

Surveillance is Totalitarian

Government surveillance is totalitarian

Neil Richards, 2013, law professor, Washington University School of Law, Harvard Law Review, PRIVACY AND TECHNOLOGY: THE DANGERS OF SURVEILLANCE, p. 1934

From the Fourth Amendment to George Orwell's Nineteen Eighty-Four, and from the Electronic Communications Privacy Act to films like Minority Report and The Lives of Others, **our law and culture are full of warnings about state scrutiny of our lives.** These warnings are commonplace, but they are rarely very specific. Other than the vague threat of an Orwellian dystopia, as a society we don't really know why surveillance is bad and why we should be wary of it. To the extent that the answer has something to do with "privacy," we lack an understanding of what "privacy" means in this context and why it matters. We've been able to live with this state of affairs largely because the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states **But these warnings are no longer science fiction. The digital technologies that have revolutionized our daily lives have also created minutely detailed records of those lives.** In an age of terror, our government has shown a keen willingness to acquire this data and use it for unknown purposes. We know that governments have been buying and borrowing private-sector databases, and **we recently learned that the National Security Agency (NSA) has been building a massive data and supercomputing center in Utah, apparently with the goal of intercepting and storing much of the world's Internet communications for decryption and analysis.** Although we have laws that protect us against government surveillance, secret government programs cannot be challenged until they are discovered. And even when they are, **our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms.** The Supreme Court recently reversed the only major case to hold to the contrary, in Clapper v. Amnesty International USA, finding that the respondents' claim that their communications were likely being monitored was "too speculative." But the important point is that our society lacks an understanding of why (and when) government surveillance is harmful. Existing attempts to identify the dangers of surveillance are often unconvincing, and they generally fail to speak in terms that are likely to influence the law. In this Article, I try to explain the harms of government surveillance. Drawing on law, history, literature, and the work of scholars in the emerging interdisciplinary field of "surveillance studies," I offer an account of what those harms are and why they matter. I will move beyond the vagueness of current theories of surveillance to articulate a more coherent understanding and a more workable approach. At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, **surveillance is harmful because it can chill the exercise of our civil liberties.** With respect to civil liberties, consider surveillance of people **when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues.** Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy." A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as **discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.** At a practical level, I propose a set of four principles that should guide the future development of surveillance law, allowing for a more appropriate balance between the costs and benefits of government surveillance. First, we must recognize that surveillance transcends the public/private divide. Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers. Second, we must recognize that secret

surveillance is illegitimate and prohibit the creation of any domestic-surveillance programs whose existence is secret. Third, we should recognize that total surveillance is illegitimate and reject the idea that it is acceptable for the government to record all Internet activity without authorization. **Government surveillance of the Internet is a power with the potential for massive abuse.** Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process before it is authorized. We should carefully scrutinize any surveillance that threatens our intellectual privacy. Fourth, we must recognize that **surveillance is harmful. Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination; accordingly, we must recognize surveillance as a harm in constitutional standing doctrine.** Explaining the harms of surveillance in a doctrinally sensitive way is essential if we want to avoid sacrificing our vital civil liberties.

Surveillance gives the government more power than Stalin had

Jonathan Schell, September 4, 2013, The Nation, Edward Snowden and Chelsea Manning, the new Dissidents? <http://www.thenation.com/article/176032/edward-snowden-and-chelsea-manning-new-dissidents> DOA: 2-23-15

And certainly, the four Poles, of all people, are as fully aware as any sensible person of the abyss of difference that separates the Obama administration from, say, the regime of Joseph Stalin, slayer of tens of millions of his own people. And yet **it is chillingly true** at the same time that **the US government has gone further than any previous government—not excluding Stalin’s—in setting up machinery that satisfies certain tendencies that are in the genetic code of totalitarianism. One is the ambition to invade personal privacy without check or possibility of individual protection. This was impossible in the era of mere phone wiretapping, before the recent explosion of electronic communications—before the cellphones that disclose the whereabouts of their owners, the personal computers with their masses of personal data and easily penetrated defenses, the e-mails that flow through readily tapped cables and servers, the biometrics, the street-corner surveillance cameras.** But now, to borrow the name of an intelligence program from the Bush years, “Total Information Awareness” is technologically within reach. The Bush and Obama administrations have taken giant strides in this direction. That China and Russia—and Britain, and many other countries—have done the same is hardly comforting to the humble individual under the eye of the universal spying apparatus. **A second totalitarian tendency has been the ambition to control the entire globe—a goal built into fascist as well as communist ideologies of the early twentieth century. In Hannah Arendt’s words, “Evidence that totalitarian governments aspire to conquer the globe and bring all countries on earth under their domination can be found repeatedly in Nazi and Bolshevik literature.”** Neither achieved it, or even came close. But now, in the limited arena of information, a sort of shadow or rudiment of this ambition is near realization by the “sole superpower,” the United States. **Much attention has been paid to Americans’ loss of privacy rights, but relatively overlooked in the debate over the government’s surveillance activities** (at least in the United States) **has been that all foreign communications—including those occurring in the lands of close allies, such as Germany—are fair game and are being swept into the US data banks.** The extent of the US global reach over information was mirrored in Snowden’s fate. Astonishingly, almost no fully democratic country would have him. (The conspicuous exception was Bolivia, whose president suffered the indignity of a forced diversion and landing of his plane when he was suspected of carrying Snowden to safety.) Almost all others, including Poland, bowed to US pressure, actual or potential, to refuse Snowden protection. The Polish letter writers were scandalized by this spectacle. “The fact that only dictatorial governments agreed to give him shelter shames the democratic states,” they wrote. “Our democracies discredit themselves with their indifference and cowardice in this matter.” What happened to Snowden in Moscow diagrammed the new global reality. He wanted to leave Russia, but the State Department, in an act of highly dubious legality, stripped him of his passport, leaving him—for purposes of travel, at least—stateless. Suddenly, he was welcome nowhere in the great wide world, which shrank down to a single point: the transit lounge at Sheremetyevo. Then, having by its own action trapped him in Russia, the administration mocked and

reviled him for remaining in an authoritarian country. **Only in unfree countries was Edward Snowden welcome. What we are pleased to call the “free world” had become a giant prison for a hero of freedom.**

Surveillance shifts the balance of power to the state

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

The danger posed by the state operating a massive secret surveillance system is far more ominous now than at any point in history. **While the government, via surveillance, knows more and more about what its citizens are doing, its citizens know less and less about what their government is doing, shielded as it is by a wall of secrecy. It is hard to overstate how radically this situation reverses the defining dynamic of a healthy society or how fundamentally it shifts the balance of power toward the state.** **Bentham’s Panopticon, designed to vest unchallengeable power in the hands of authorities, was based on exactly this reversal:** “The essence of it,” he wrote, rests in “the centrality of the inspector’s situation” combined with the “most effectual contrivances for seeing without being seen.” In a healthy democracy, the opposite is true. Democracy requires accountability and consent of the governed, which is only possible if citizens know what is being done in their name. The presumption is that, with rare exception, they will know everything their political officials are doing, which is why they are called public servants, working in the public sector, in public service, for public agencies. Conversely, the presumption is that the government, with rare exception, will not know anything that law-abiding citizens are doing. That is why we are called private individuals, functioning in our private capacity. Transparency is for those who carry out public duties and exercise public power. Privacy is for everyone else. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Location 2912). Henry Holt and Co.. Kindle Edition.

NSA surveillance monitors all aspects of daily life for millions of Americans

T.C. Slottek, December 12, 2013, “The NSA is out of control and must be stopped,” The Verge, <http://www.theverge.com/2013/12/12/5200142/end-the-nsa-nightmare> DOA: 2-25-15

The National Security Agency is breaking trust in democracy by breaking trust in the internet. Every day, the NSA records the lives of millions of Americans and countless foreigners, collecting staggering amounts of information about who they know, where they've been, and what they've done. Its surveillance programs have been kept secret from the public they allegedly serve and protect. **The agency operates the most sophisticated, effective, and secretive surveillance apparatus in history.** Recent disclosures about the intelligence gathering activities of the NSA, and the ensuing federal response, have demonstrated that **the agency is a rogue state** — unaccountable and out of control. **Intelligence community leaders have openly lied to elected officials and the public about the nature and extent of the agency's data collection efforts.** And despite their responsibility in carefully overseeing intelligence agencies, President Obama and Congress have shown no credibility as custodians of the NSA. So far, **Congress has shown far less tolerance for baseball players allegedly lying about personal steroid use than military leaders lying about surveillance programs that undermine the bill of rights.** After more than a decade of legal adventurism, secret presidential orders, and deceptive wordplay, **policymakers and intelligence officials have erected a surveillance apparatus that can track the location of hundreds of millions of people, collect the phone records of the entire nation, and tap into the very backbone of the internet.** Every day, the NSA collects millions of electronic records belonging to people who are not suspected of any wrongdoing. It may even know what you're up to in *World of Warcraft*, because the bad guys are apparently slaying dragons while they plot terror attacks. The secret court responsible for overseeing the NSA's activities is required to, on a yearly basis, approve only general guidelines on how the government intends to collect intelligence on foreigners. **The NSA is not supposed to spy on American citizens, but it "incidentally" collects vast amounts of data on them anyway.** Intelligence

Community director James Clapper and others have defended these practices by contorting words like "collection" and "surveillance" in ways that make Bill Clinton's 1998 soliloquy on the meaning of the word "is" look like amateur bullshitting. In 2005, then-Senator Obama opposed changes to the Patriot Act that would have allowed what he called "government fishing expeditions targeting innocent Americans." Obama said the government needed "to show the American people that the federal government will only issue warrants and execute searches because it needs to, not because it can." As president, Obama has not only extended Bush-era programs, but expanded the NSA's ability to conduct indiscriminate, warrantless surveillance. Despite his endorsement of NSA bulk surveillance, President Obama may not even know everything the agency is up to; the White House and the NSA can't even agree about whether the president knew the agency was tapping German Chancellor Angela Merkel's phone. Obama allegedly spent five years in office without knowing his military was eavesdropping on world leaders. Congress has operated with similar blinders despite its permissive attitude on bulk spying, though now it complains that the NSA hasn't shared enough in its annual show-and-tell sessions. In the face of this ignorance, several Congressional leaders now want to retroactively authorize the NSA's mass spying programs rather than audit them.

Threat from state surveillance greater today than ever

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Writing in the New York Times in 2005, James Bamford observed that the threat from state surveillance is far more dire today than it was in the 1970s: "With people expressing their innermost thoughts in e-mail messages , exposing their medical and financial records to the Internet, and chatting constantly on cellphones, the agency virtually has the ability to get inside a person's mind." Church's concern, that any surveillance ability "could be turned around on the American people," is precisely what the NSA has done post-9/ 11. Despite operating under the Foreign Intelligence Surveillance Act, and despite the prohibition on domestic spying embedded in the agency's mission from the start, many of its surveillance activities are now focused on US citizens on US soil. Even absent abuse, and even if one is not personally targeted, a surveillance state that collects it all harms society and political freedom in general. Progress both in the United States and other nations was only ever achieved through the ability to challenge power and orthodoxies and to pioneer new ways of thinking and living. Everyone, even those who do not engage in dissenting advocacy or political activism, suffers when that freedom is stifled by the fear of being watched. Hendrik Hertzberg, who downplayed concerns about the NSA programs, nonetheless acknowledged that "harm has been done. The harm is civic. The harm is collective . The harm is to the architecture of trust and accountability that supports an open society and a democratic polity." Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2777-2782). Henry Holt and Co.. Kindle Edition.

The scope of the surveillance is totalitarian

Noam Chomsky, MIT, June, 2014, A Surveillance State Beyond Imagination Is Being Created in One of the World's Freest Countries, <http://www.alternet.org/civil-liberties/noam-chomsky-surveillance-state-beyond-imagination-being-created-one-freest> DOA: 2-20-15

In the past several months, we have been provided with instructive lessons on the nature of state power and the forces that drive state policy. And on a closely related matter: the subtle, differentiated concept of transparency. The source of the instruction, of course, is the trove of documents about the National Security Agency surveillance system released by the courageous fighter for freedom Edward J. Snowden, expertly summarized and analyzed by his collaborator Glenn Greenwald in his new book, " *No Place to Hide.*" The documents unveil a remarkable project to expose to state scrutiny vital information about

every person who falls within the grasp of the colossus - in principle, every person linked to the modern electronic society. Nothing so ambitious was imagined by the dystopian prophets of grim totalitarian worlds ahead. It is of no slight import **that the project is being executed in one of the freest countries in the world, and in radical violation of the U.S. Constitution's Bill of Rights, which protects citizens from "unreasonable searches and seizures," and guarantees the privacy of their "persons, houses, papers and effects."** Much as government lawyers may try, there is no way to reconcile these principles with the assault on the population revealed in the Snowden documents. **It is also well to remember that defense of the fundamental right to privacy helped to spark the American Revolution.** In the 18th century, **the tyrant was the British government, which claimed the right to intrude freely into the homes and personal lives of American colonists. Today it is American citizens' own government that arrogates to itself this authority.**

NSA's capabilities create tyranny through chilling thought and expression

David John Morotta, June 8, 2014, Capability is Tyranny,
<http://www.forbes.com/sites/davidmarotta/2014/06/08/capability-is-tyranny/> DOA: 2-20-15

In other words, I have a gun, which could be pointed at you, but don't worry because I have self-control. I won't point it at you yet.

Glenn Greenwald, the journalist at The Guardian who worked with Snowden, had a very different take. In an interview with CATO Institute, Greenwald said, "**This is what the existence of a surveillance state does, and it's what Jeremy Bentham recognized, which is that if you can create institutions where the people you are trying to control—inmates or students or patients in a psychiatric ward—know that they can be watched at any moment, even if they don't know when they are being watched or if they are being watched, the fact that they know that they can be watched at any moment means that they will assume that they are always being watched and therefore will act accordingly—meaning in compliance with the dictative authorities.**"

Even the phrase “I have nothing to fear because I have nothing to hide,” Greenwald claims is a sort of bargain. He says, "**If you become sufficiently obedient and compliant and passive and non-threatening, . . . you can be unmolested by power.**" He reminds us that "**in even the worst tyrannies, people who don’t bother tyrants are never or rarely targeted with oppressive behavior.**" In 2013, Snowden said in a video interview with Glenn Greenwald and Laura Poitras that he released all this information on U.S. surveillance because "I don't wanna live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity, or love, or friendship is recorded, and that's not something I'm willing to support, it's not something I'm willing to build, and it's not something I'm willing to live under." He repeated those sentiments this March when he was interviewed by Chris Anderson at the same TED talk as Ledgett. Snowden said **we should be able to live our lives “without wondering about how these events are going to look to an agent of the government, possibly not even your government, years in the future.”** Many of us have been reminded of George Orwell's novel "Nineteen Eighty-Four" about a dystopian political future where "Big Brother Is Watching You." **You can be punished for thinking socially unacceptable thoughts, or “thoughtcrimes.”** John Whitehead—local attorney, author and founder of The Rutherford Institute, a nonprofit civil liberties and human rights organization whose international headquarters are located in Charlottesville—wrote "Orwell's Nightmare: The NSA and Google—Big Brother Meets Big Business." He said, "What Google's vast acquisition and analysis of information indicates is that **we are entering what some have called an age of infopolitics, in which the human person is broken down into data sets to be collated and analyzed, and used for a variety of purposes, including marketing, propaganda, and the squelching of dissent.** As philosopher Colin Koopman notes, **we may soon find ourselves in a more efficient version of the McCarthy era, in**

which one's personal beliefs or associations become fodder for the rising corporate surveillance state. Anyone who has read the Orwell novel remembers that Big Brother is terrifying because he is watching you, not because he is threatening to feed you to hungry rats, which does happen to the main character. **Watching is sufficient to create tyranny.** We liken it to the policy of mutually ensured destruction used by countries with nuclear weapons. The threat of annihilation is sufficient to create obedience and cooperation. In Snowden's March 2014 appearance, he urged technological leaders as well as average citizens to take back the Internet. He saw reform occurring not in the halls of Congress but in the cubicles of computer programmers: "We need to encode our values not just in writing but in the structure of the Internet." He called for every Web page you visit to have encryption, arguing, "The reason this matters is today, if you go to look at a copy of '1984' on Amazon.com, the NSA can see a record of that, the Russian intelligence service can see a record of that, the Chinese service can see a record of that, the French service, the German service, the services of Andorra. They can all see it because it's unencrypted. The world's library is Amazon.com, but they do not support encryption by default. . . . All companies need to move to an encrypted browsing habit by default for all users who haven't taken any action or picked any special methods on their own. That'll increase the privacy and the rights that people enjoy worldwide." Remember, remember the fifth of June, when Edward Snowden sacrificed his life that you might fight to regain yours before it was too late. **This is one of the most critical issues of our time. Those who stand by and do nothing are complicit in aiding the loss of freedoms for others.** We all must fight to protect the rights of others. Be more outraged.

Totalitarian surveillance society

Chuck Douglas is a former congressman for the Second District of New Hampshire and a former New Hampshire Supreme Court and Superior Court judge, Concord Monitor, May 23, 2014, <http://www.concordmonitor.com/home/12076097-95/my-turn-its-time-for-america-to-scale-back-surveillance DOA: 2-20-15>

One year ago, Americans would not be discussing the issue of the NSA data collection program because none of us even knew about the massive phone metadata collection programs by our government. In fact, in April of last year, Sen. Ron Wyden asked Intelligence Director James Clapper at a hearing **if the government had been collecting metadata on all domestic phone calls. Clapper, under oath, denied it.** The scope of secret government snooping programs came to light only because of the disclosures by Edward Snowden in June. When George Orwell wrote 1984 years ago, the all-seeing state, or "Big Brother," was represented by a two-way television set installed in each home. **In our own modern world, the all-seeing one lives in every location-tracking cell phone we willingly carry with us day and night.** **A surveillance society is taking root. Video cameras peer constantly from lamp poles and storefronts. Satellites and drones float through the skies. Smartphones relay a barrage of information about their owners to sentinel towers across the land. License-plate cameras and fast-pass lanes track the movements of our cars. Under a program code-named PRISM, the National Security Agency reached out to nine internet companies, including Google and Yahoo, to covertly gain access to their data, from email to online searches.** By 2011, the military agency's database was pulling in 1.8 billion phone records a day in addition to listening to German Chancellor Angela Merkel's cell phone. Apparently **we are all suspects.** An indication of how bad the situation has become is that the National Rifle Association has joined the ACLU in suing to stop the daily collecting of phone data. In January, the Republican Party's National Committee voted to ask Congress to end the program. The Democrats have been silent. **Historically, the anti-privacy apex was the Soviet Union. Its founder, Vladimir Lenin said, "We recognize nothing private."** But our American Bill of Rights specifically tells our government what it cannot do about invading privacy. The fundamental value captured in the Fourth Amendment to the United States is: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." This security is central to the right of privacy, which Supreme Court Justice Louis Brandeis famously described as: "The right to be left alone — the most comprehensive of rights and the right most valued by civilized men." But **how can we be secure in our homes and communications if warrantless government agencies use a secret court on an ex parte**

basis to gather information? The metadata collection program under section 215 of the Patriot Act does not require a warrant or even probable cause. To justify it the government says courts have frequently applied a judicially created exception to the Fourth Amendment to assert that records of individuals' phone calls, location, internet use, and more collected by the companies lack constitutional protection when they turn it over to the NSA, a military agency headed by a General. The access is granted by the Foreign Intelligence Surveillance Court, which hears only from the government in secret sessions. In most instances, the applicability of the Fourth Amendment turns on whether or not an individual has a "reasonable expectation of privacy" in their call data. Last year, two federal judges that have ruled on the Big Brother collection program split in December. In *ACLU v. Clapper* in the Southern District of New York, Judge Pauley gave deference to the executive branch. But in *Kayman v. Obama*, Judge Leon, a Bush appointee on the district court for D.C., held the metadata program unconstitutional, saying: "It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the government." I clearly believe Judge Leon got it right. **Trusting any government to always do the right thing is dangerous and our founders knew it! And, by the way, who we really are supposed to trust are 5 million people with secret and top-secret clearances, or one out of every 70 Americans.** It is time to end this unconstitutional program and restore our reasonable expectation of privacy.

Surveillance enables global tyranny

Eben Moglen, May 27, 2014, The Guardian, <http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy> (Eben Moglen is professor of law and legal history at Columbia University, and is founder, director-counsel and chairman of Software Freedom Law Centre, which provides pro bono legal representation and related services to not-for-profit developers of free software and open source software) DOA: 2-23-15

The power of that Roman empire rested in its leaders' control of communications. The Mediterranean was their lake. **Across their European empire, from Scotland to Syria, they pushed roads that 15 centuries later were still primary arteries of European transportation. Down those roads the emperor marched his armies. Up those roads he gathered his intelligence.** The emperors invented the posts to move couriers and messages at the fastest possible speed. **Using that infrastructure,** with respect to everything that involved the administration of power, **the emperor made himself the best-informed person in the history of the world. That power eradicated human freedom.** "Remember," said Cicero to Marcellus in exile, "wherever you are, you are equally within the power of the conqueror." The empire of the United States after the second world war also depended upon control of communications. This was more evident when, a mere 20 years later, the United States was locked in a confrontation of nuclear annihilation with the Soviet Union. In a war of submarines hidden in the dark below the continents, capable of eradicating human civilisation in less than an hour, the rule of engagement was "launch on warning". Thus the United States valued control of communications as highly as the Emperor Augustus. Its listeners too aspired to know everything. We all know that the United States has for decades spent as much on its military might as all other powers in the world combined. Americans are now realising what it means that we applied to the stealing of signals and the breaking of codes a similar proportion of our resources in relation to the rest of the world. The US system of listening comprises a military command controlling a large civilian workforce. That structure presupposes the foreign intelligence nature of listening activities. Military control was a symbol and guarantee of the nature of the activity being pursued. Wide-scale domestic surveillance under military command would have violated the fundamental principle of civilian control. Instead what it had was a foreign intelligence service responsible to the president as military commander-in-chief. The chain of military command absolutely ensured respect for the fundamental principle "no listening here". The boundary between home and away distinguished the permissible from the unconstitutional. The distinction between home and away was at least technically credible, given the reality of 20th-century communications media, which were hierarchically organised and very often state-controlled. **When the US government chose to listen to other governments abroad – to their militaries, to their diplomatic communications, to their policymakers where possible – they were listening in a world**

of defined targets. The basic principle was: hack, tap, steal. We listened, we hacked in, we traded, we stole. In the beginning we listened to militaries and their governments. Later we monitored the flow of international trade as far as it engaged American national security interests. **The regime that we built to defend ourselves against nuclear annihilation was restructured at the end of the 20th century.** In the first place, the cold war ended and the Soviet Union dissolved. An entire establishment of national security repurposed itself. We no longer needed to spy upon an empire with 25,000 nuclear weapons pointed at us. **Now we spied on the entire population of the world, in order to locate a few thousand people intent on various kinds of mass murder. Hence, we are told, spying on entire societies is the new normal.** In the second place, the nature of human communication changed. We built a system for attacking fixed targets: a circuit, a phone number, a licence plate, a locale. The 20th-century question was how many targets could be simultaneously followed in a world where each of them required hack, tap, steal. But we then started to build a new form of human communication. **From the moment we created the internet, two of the basic assumptions began to fail: the simplicity of "one target, one circuit" went away, and the difference between home and abroad vanished too.** That distinction vanished in the United States because so much of the network and associated services, for better and worse, resided there. The question "Do we listen inside our borders?" was seemingly reduced to "Are we going to listen at all?" At this point, a vastly imprudent US administration intervened. Their defining characteristic was that they didn't think long before acting. Presented with a national calamity that also constituted a political opportunity, nothing stood between them and all the mistakes that haste can make for their children's children to repent at leisure. What they did – in secret, with the assistance of judges appointed by a single man operating in secrecy, and with the connivance of many decent people who believed themselves to be acting to save the society – was to unchain the listeners from law. Not only had circumstances destroyed the simplicity of "no listening inside", not only had fudging with the foreign intelligence surveillance act carried them where law no longer provided useful landmarks, but they actually wanted to do it. Their view of the nature of human power was Augustan, if not august. They wanted what it is forbidden to wise people to take unto themselves. And so they fell, and we fell with them. Our journalists failed. The New York Times allowed the 2004 election not to be informed by what it knew about the listening. Its decision to censor itself was, like all censorship and self-censorship, a mortal wound inflicted on democracy. We the people did not demand the end at the beginning. And now we're a long way in. **Our military listeners have invaded the centre of an evolving net, where conscriptable digital superbrains gather intelligence on the human race for purposes of bagatelle and capitalism. In the US, the telecommunications companies have legal immunity for their complicity, thus easing the way further.** The invasion of our net was secret, and we did not know that we should resist. But resistance developed as a fifth column among the listeners themselves. In Hong Kong, Edward Snowden said something straightforward and useful: analysts, he said, are not bad people, and they don't want to think of themselves that way. But they came to calculate that if a programme produced anything useful, it was justified. It was not the analysts' job to weigh the fundamental morality for us. In a democracy, that task is given by the people to the leaders they elect. **These leaders fell – and we fell with them – because they refused to adhere to the morality of freedom.** The civilian workers in their agencies felt their failure first. From the middle of last decade, people began to blow whistles all over the field. These courageous workers sacrificed their careers, frightened their families, sometimes suffered personal destruction, to say that there was something deeply wrong. The response was rule by fear. Two successive US administrations sought to deal with the whistleblowers among the listeners by meting out the harshest possible treatment. Snowden said in Hong Kong that he was sacrificing himself in order to save the world from a system like this one, which is "constrained only by policy documents". The political ideas of Snowden are worthy of our respect and our deep consideration. But for now it is sufficient to say that he was not exaggerating the nature of the difficulty. Because of Snowden, we now know that the listeners undertook to do what they repeatedly promised respectable expert opinion they would never do. They always said they would not attempt to break the crypto that secures the global financial system. That was false. When Snowden disclosed the existence of the NSA's Bullrun programme we learned that NSA had lied for years to the financiers who believe themselves entitled to the truth from the government they own. **The NSA had not only subverted technical standards, attempting to break the encryption that holds the global financial industry together, it had also stolen the keys to as many vaults as possible.** With this disclosure the NSA forfeited respectable opinion around the world. Their reckless endangerment of those who don't accept danger from the United States government was breathtaking. **The empire of the United States was the empire of exported liberty.** What it had to offer all around the world was liberty and freedom. **After colonisation, after European theft, after forms of**

state-created horror, it promised a world free from state oppression. Last century we were prepared to sacrifice many of the world's great cities and tens of millions of human lives. We bore those costs in order to smash regimes we called "totalitarian", in which the state grew so powerful and so invasive that it no longer recognised any border of private life. We desperately fought and died against systems in which the state listened to every telephone conversation and kept a list of everybody every troublemaker knew. But in the past 10 years, after the morality of freedom was withdrawn, the state has begun fastening the procedures of totalitarianism on the substance of democratic society. There is no historical precedent for the proposition that the procedures of totalitarianism are compatible with the system of enlightened, individual and democratic self-governance. Such an argument would be doomed to failure. It is enough to say in opposition that omnipresent invasive listening creates fear. And that fear is the enemy of reasoned, ordered liberty. It is utterly inconsistent with the American ideal to attempt to fasten procedures of totalitarianism on American constitutional self-governance. But there is an even deeper inconsistency between those ideals and the subjection of every other society on earth to mass surveillance. Some of the system's servants came to understand that it was being sustained not with, but against, democratic order. They knew their vessel had come unmoored in the dark, and was sailing without a flag. When they blew the whistle, the system blew back at them. In the end – at least so far, until tomorrow – there was Snowden, who saw everything that happened and watched the fate of others who spoke up. He understood, as Chelsea Manning also always understood, that when you wear the uniform you consent to the power. He knew his business very well. Young as he was, as he said in Hong Kong, "I've been a spy all my life." So he did what it takes great courage to do in the presence of what you believe to be radical injustice. He wasn't first, he won't be last, but he sacrificed his life as he knew it to tell us things we needed to know. Snowden committed espionage on behalf of the human race. He knew the price, he knew the reason. But as he said, only the American people could decide, by their response, whether sacrificing his life was worth it. So our most important effort is to understand the message: to understand its context, purpose, and meaning, and to experience the consequences of having received the communication. Even once we have understood, it will be difficult to judge Snowden, because there is always much to say on both sides when someone is greatly right too soon. In the United States, those who were "premature anti-fascists" suffered. It was right to be right only when all others were right. It was wrong to be right when only people we disagreed with held the views that we were later to adopt ourselves. Snowden has been quite precise. He understands his business. He has spied on injustice for us and has told us what we require in order to do the job and get it right. And if we have a responsibility, then it is to learn, now, before somebody concludes that learning should be prohibited. In considering the political meaning of Snowden's message and its consequences, we must begin by discarding for immediate purposes pretty much everything said by the presidents, the premiers, the chancellors and the senators. Public discussion by these "leaders" has provided a remarkable display of misdirection, misleading and outright lying. We need instead to focus on the thinking behind Snowden's activities. What matters most is how deeply the whole of the human race has been ensnared in this system of pervasive surveillance. We begin where the leaders are determined not to end, with the question of whether any form of democratic self-government, anywhere, is consistent with the kind of massive, pervasive surveillance into which the United States government has led not only its people but the world. This should not actually be a complicated inquiry. For almost everyone who lived through the 20th century – at least its middle half – the idea that freedom was consistent with the procedures of totalitarianism was self-evidently false. Hence, as we watch responses to Snowden's revelations we see that massive invasion of privacy triggers justified anxiety among the survivors of totalitarianism about the fate of liberty. To understand why, we need to understand more closely what our conception of "privacy" really contains.

Surveillance destroys privacy, which is critical to democracy

Eben Moglen, May 27, 2014, The Guardian, <http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy> (Eben Moglen is professor of law and legal history at Columbia University, and is founder, director-counsel and chairman of Software Freedom Law Centre, which provides pro bono legal representation and related services to not-for-profit developers of free software and open source software) DOA: 2-23-15

Our concept of "privacy" combines three things: first is secrecy, or our ability to keep the content of our messages known only to those we intend to receive them. **Second is anonymity**, or secrecy about **who** is sending and receiving messages, where the content of the messages may not be secret at all. It is very important that anonymity is an interest we can have both in our publishing and in our reading. **Third is autonomy**, or our ability to make our own life decisions free from any force that has violated our secrecy or our anonymity. **These three – secrecy, anonymity and autonomy – are the principal components of a mixture we call "privacy". Without secrecy, democratic self-government is impossible. Without secrecy, people may not discuss public affairs with those they choose, excluding those with whom they do not wish to converse. Anonymity is necessary for the conduct of democratic politics. Not only must we be able to choose with whom we discuss politics, we must also be able to protect ourselves against retaliation for our expressions of political ideas.** Autonomy is vitiated by the wholesale invasion of secrecy and privacy. **Free decision-making is impossible in a society where every move is monitored, as a moment's consideration of the state of North Korea will show, as would any conversation with those who lived through 20th-century totalitarianisms, or any historical study of the daily realities of American chattel slavery before our civil war. In other words, privacy is a requirement of democratic self-government.** The effort to fasten the procedures of pervasive surveillance on human society is the antithesis of liberty. This is the conversation that all the "don't listen to my mobile phone!" misdirection has not been about. If it were up to national governments, the conversation would remain at this phoney level forever. **The US government and its listeners have not advanced any convincing argument that what they do is compatible with the morality of freedom, US constitutional law or international human rights.** They will instead attempt, as much as possible, to change the subject, and, whenever they cannot change the subject, to blame the messenger. One does not need access to classified documents to see how **the military and strategic thinkers in the United States adapted to the end of the cold war by planning pervasive surveillance of the world's societies.** From the early 1990s, the public literature of US defence policy shows, strategic and military planners foresaw a world in which the United States had no significant state adversary. Thus, we would be forced to engage in a series of "asymmetric conflicts", meaning "guerrilla wars" with "non-state actors". In the course of that redefinition of US strategic posture, the military strategists and their intelligence community colleagues came to regard US rights to communications privacy as the equivalent of sanctuary for guerrillas. They conceived that it would be necessary for the US military, the listeners, to go after the "sanctuaries". Then, at the opening of the 21st century, a US administration that will go down in history for its tendency to think last and shoot first bought – hook, line and sinker – the entire "denying sanctuary", pervasive surveillance, "total information awareness" scheme. Within a very short time after January 2002, mostly in secret, they put it all together. The consequences around the world were remarkably uncontroversial. By and large, states approved or accepted. After September 2001, the United States government used quite extraordinary muscle around the world: you were either with us or against us. Moreover, many other governments had come to base their national security systems crucially on cooperation with American listening. By the time the present US administration had settled into office, senior policymakers thought there was multilateral consensus on listening to other societies: it could not be stopped and therefore it shouldn't be limited. The Chinese agreed. The US agreed. The Europeans agreed; their position was somewhat reluctant, but they were dependent on US listening and hadn't a lot of power to object. Nobody told the people of the world. By the end of the first decade of the 21st century, a gap opened between what the people of the world thought their rights were and what their governments had given away in return for intelligence useful only to the governments themselves. This gap was so wide, so fundamental to the meaning of democracy, that those who operated the system began to disbelieve in its legitimacy. As they should have done. **Snowden** saw what happened to other whistleblowers, and behaved accordingly. His political theory has been quite exact and entirely consistent. He **says the existence of these programmes, undisclosed to the American people, is a fundamental violation of American democratic values. Surely there can be no argument with that.** Snowden's position is that efforts so comprehensive, so overwhelmingly powerful, and so conducive to abuse, should not be undertaken save with democratic consent. He has expressed recurrently his belief that the American people are entitled to give or withhold that informed consent. But Snowden has also identified the fastening of those programmes on the global population as a problematic act, which deserves a form of moral and ethical analysis that goes beyond mere *raison d'état*. Hopelessness is merely the condition they want you to catch, not one you have to have. I think Snowden means that we should make those decisions not in the narrow, national self-interest, but with some heightened moral sense of what is appropriate for a nation that holds itself out as a beacon of liberty to humanity. We can speak, of

course, about American constitutional law and about the importance of American legal phenomena – rules, protections, rights, duties – with respect to all of this. But we should be clear that, when we talk about the American constitutional tradition with respect to freedom and slavery, we're talking about more than what is written in the law books. We face two claims – you meet them everywhere you turn – that summarise the politics against which we are working. One argument says: "It's hopeless, privacy is gone, why struggle?" The other says: "I'm not doing anything wrong, why should I care?" These are actually the most significant forms of opposition that we face in doing what we know we ought to do. In the first place, **our struggle to retain our privacy is far from hopeless.** Snowden has described to us what armour still works. His purpose was to distinguish between those forms of network communication that are hopelessly corrupted and no longer usable, those that are endangered by a continuing assault on the part of an agency gone rogue, and those that, even with their vast power, all their wealth, and all their misplaced ambition, conscientiousness and effort, they still cannot break. Hopelessness is merely the condition they want you to catch, not one you have to have. So far as the other argument is concerned, we owe it to ourselves to be quite clear in response: "If we are not doing anything wrong, then we have a right to resist." If we are not doing anything wrong, then we have a right to do everything we can to maintain the traditional balance between us and power that is listening. We have a right to be obscure. We have a right to mumble. We have a right to speak languages they do not get. We have a right to meet when and where and how we please. **We have an American constitutional tradition against general warrants. It was formed in the 18th century for good reason. We limit the state's ability to search and seize to specific places and things that a neutral magistrate believes it is reasonable to allow.** That principle was dear to the First Congress, which put it in our bill of rights, because it was dear to British North Americans; because in the course of the 18th century they learned what executive government could do with general warrants to search everything, everywhere, for anything they didn't like, while forcing local officials to help them do it. That was a problem in Massachusetts in 1761 and it remained a problem until the end of British rule in North America. Even then, it was a problem, because the presidents, senators and chancellors were also unprincipled in their behaviour. Thomas Jefferson, too, like the president now, talked a better game than he played. This principle is clear enough. But there are only nine votes on the US supreme court, and only they count right now. We must wait to see how many of them are prepared to face the simple unconstitutionality of a rogue system much too big to fail. But because those nine votes are the only votes that matter, the rest of us must go about our business in other ways. The American constitutional tradition we admire was made mostly by people who had fled Europe and come to North America in order to be free. It is their activity, politically and intellectually, that we find deposited in the documents that made the republic. But there is a second constitutional tradition. It was made by people who were brought here against their will, or who were born into slavery, and who had to run away, here, in order to be free. This second constitutional tradition is slightly different in its nature from the first, although it conduces, eventually, to similar conclusions. We face two claims. One says: 'It's hopeless, privacy is gone, why struggle?' The other: 'I'm not doing anything wrong, why should I care?'. These are actually the most significant forms of opposition we face. **Running away from slavery is a group activity. Running away from slavery requires the assistance of those who believe that slavery is wrong. People in the United States have forgotten how much of our constitutional tradition was made in the contact between people who needed to run away in order to be free and people who knew that they needed to help, because slavery is wrong.** We have now forgotten that in the summer of 1854, when Anthony Burns – who had run away from slavery in Richmond, Virginia – was returned to slavery by a state judge acting as a federal commissioner under the second fugitive slave act, Boston itself had to be placed under martial law for three whole days. Federal troops lined the streets, as Burns was marched down to Boston Harbor and put aboard a ship to be sent back to slavery. If Boston had not been held down by force, it would have risen. When Frederick Douglass ran away from slavery in 1838, he had the help of his beloved Anna Murray, who sent him part of her savings and the sailor's clothing that he wore. He had the help of a free black seaman who gave him identity papers. Many dedicated people risked much to help him reach New York. **Our constitutional tradition is not merely contained in the negative rights found in the bill of rights. It is also contained in the history of a communal, often formally illegal, struggle for liberty against slavery. This part of our tradition says that liberty from oppressive control must be accorded people everywhere, as a right.** It says that slavery is simply wrong, that it cannot be tolerated or justified by the master's fear or need for security. So the constitutional tradition Americans should be defending now is a tradition that extends far beyond whatever boundary the fourth amendment has in space, place, or time. Americans should be defending not merely a right to be free from the oppressive attentions of the national

government, not merely fighting for something embodied in the due process clause of the 14th amendment. We should rather be fighting against the procedures of totalitarianism because slavery is wrong. Because fastening the surveillance of the master on the whole human race is wrong. Because providing the energy, the money, the technology, the system for subduing everybody's privacy around the world – for destroying sanctuary in American freedom of speech – is wrong. Snowden has provided the most valuable thing that democratic self-governing people can have, namely information about what is going on. If we are to exercise our rights as self-governing people, using the information he has given us, we should have clear in our minds the political ideas upon which we act. They are not parochial, or national, or found in the records of supreme court decisions alone. A nation conceived in liberty, and dedicated to the proposition that all men are created equal, enslaved millions of people. It washed away that sin in a terrible war. Americans should learn from that, and are called upon now to do so. Knowing what we know, thanks to Snowden, citizens everywhere must demand two things of their governments: "In the first place," we must say to our rulers, "you have a responsibility, a duty, to protect our rights by guarding us against the spying of outsiders." Every government has that responsibility. It must protect the rights of its citizens to be free from intrusive mass surveillance by other states. No government can pretend to sovereignty and responsibility unless it makes every effort within its power and its means to ensure that outcome. In the second place, every government must subject its domestic listening to the rule of law. The overwhelming arrogance of the listeners and the foolishness of the last administration has left the US government in an unnecessary hole. Until the last administration unchained the listeners from law, the US government could have held up its head before the world, proclaiming that only its listeners were subject to the rule of law. It would have been an accurate boast. For almost nothing, history will record, they threw that away. To the citizens of the United States, a greater responsibility is given. The government is projecting immensities of power into the destruction of privacy in the world's other societies. It is doing so without any democratic check or control, and its people must stop it. Americans' role as the beacon of liberty in the world requires no less of us. Freedom has been hunted round the globe. Asia and Africa have long expelled her. Europe has been bullied into treating her like a stranger and Britain would arrest her at Heathrow if she arrived. The president of the United States has demanded that no one shall receive the fugitive, and maybe only the Brazilian president, Dilma Rousseff, wants to prepare in time an asylum for mankind. Political leaders around the world have had much to say since Snowden began his revelations, but not one statement that consisted of "I regret subjecting my own people to these procedures". The German chancellor, though triumphantly re-elected with not a cloud in her political sky, is in no position to say, "I agreed with the Americans to allow 40m telephone calls a day to be intercepted in Germany; I just want them to stop listening to my phone!" The US listeners are having a political crisis beyond their previous imagining. They do not like to appear in the spotlight, or indeed to be visible at all. Now they have lost their credibility with the cybersecurity industry, which has realised that they have broken their implicit promises about what they would not hack. The global financial industry is overwhelmed with fear at what they've done. The other US government agencies they usually count on for support are fleeing them. We will never again have a similar moment of political disarray on the side that works against freedom. Not only have they made the issue clear to everybody – not only have they created martyrs in our comrades at Fort Leavenworth, at the Ecuadorian embassy in London and at an undisclosed location in Moscow – not only have they lit this fire beyond the point where they can piss it out, but they have lost their armour. They stand before us in the fullness of who they really are. It is up to us to show that we recognise them. What they have done is to build a state of permanent war into the net. Twelve years into a war that never seems to end, they are making the net a wartime place forever. We must reimagine what a net at peace would look like: cyberpeace. Young people around the world now working on the theory of cyberpeace are doing the most important political work of our time. We will now have to provide what democracies provide best, which is peace. We have to be willing to declare victory and go home. When we do, we have to leave behind a net that is no longer in a state of war, a net which no longer uses surveillance to destroy the privacy that founds democracy. This is a matter of international public law. In the end this is about something like prohibiting chemical weapons, or landmines. A matter of disarmament treaties. A matter of peace enforcement. What if every book for the past 500 years had been reporting its readers at headquarters? The difficulty is that we have not only our good and patriotic fellow citizens to deal with, for whom an election is a sufficient remedy, but we have also an immense structure of private surveillance that has come into existence. This structure has every right to exist in a free market, but is now creating ecological disaster from which governments alone have benefited. We have to consider not only, therefore, what our politics are with respect to the states, but also

with respect to the enterprises. Instead we are still at a puppet show in which the people who are the legitimate objects of international surveillance – namely politicians, heads of state, military officers, and diplomats – are screaming about how they should not be listened to. As though they were us and had a right to be left alone. And that, of course, is what they want. They want to confuse us. They want us to think that they are us – that they're not the people who allowed this to happen, who cheered it on, who went into business with it. We must cope with the problems their deceptions created. Our listeners have destroyed the internet freedom policy of the US government. They had a good game so long as they could play both sides. But now we have comrades and colleagues around the world who are working for the freedom of the net in dangerous societies; they have depended upon material support and assistance from the United States government, and they now have every reason to be frightened. What if the underground railroad had been constantly under efforts of penetration by the United States government on behalf of slavery? **What if every book for the past 500 years had been reporting its readers at headquarters?** The bad news for the people of the world is we were lied to thoroughly by everybody for nearly 20 years. The good news is that Snowden has told us the truth. Edward Snowden has revealed problems for which we need solutions. The vast surveillance-industrial state that has grown up since 2001 could not have been constructed without government contractors and the data-mining industry. Both are part of a larger ecological crisis brought on by industrial overreaching. We have failed to grasp the nature of this crisis because we have misunderstood the nature of privacy. Businesses have sought to profit from our confusion, and governments have taken further advantage of it, threatening the survival of democracy itself. **In this context, we must remember that privacy is about our social environment, not about isolated transactions we individually make with others. When we decide to give away our personal information, we are also undermining the privacy of other people. Privacy is therefore always a relation among many people, rather than a transaction between two.** Many people take money from you by concealing this distinction. They offer you free email service, for example. In return, they want you to let them read all the mail. Their stated purpose is advertising to you. It's just a transaction between two parties. Or, they offer you free web hosting for your social communications, and then they watch everybody looking at everything. This is convenient, for them, but fraudulent. If you accept this supposedly bilateral offer, to provide email service to you for free as long as it can all be read, then everybody who corresponds with you is subjected to this bargain. If your family contains somebody who receives mail at Gmail, then Google gets a copy of all correspondence in your family. If another member of your family receives mail at Yahoo, then Yahoo receives a copy of all the correspondence in your family as well. **Perhaps even this degree of corporate surveillance of your family's email is too much for you. But as Snowden's revelations showed, to the discomfiture of governments and companies alike, the companies are also sharing all that mail with power – which is buying it, getting courts to order it turned over, or stealing it – whether the companies like it or not.** The same will be true if you decide to live your social life on a website where the creep who runs it monitors every social interaction, keeping a copy of everything said, and also watching everybody watch everybody else. If you bring new "friends" to the service, you are attracting them to the creepy inspection, forcing them to undergo it with you. This is an ecological problem, because our individual choices worsen the condition of the group as a whole. The service companies' interest, but not ours, is to hide this view of the problem, and concentrate on getting individual consent. From a legal perspective, the essence of transacting is consent. If privacy is transactional, your consent to surveillance is all the commercial spy needs. But if privacy is correctly understood, consent is usually irrelevant, and focusing on it is fundamentally inappropriate. We do not, with respect to clean air and clean water, set the limits of tolerable pollution by consent. We have socially established standard of cleanliness, which everybody has to meet. Environmental law is not law about consent. But with respect to privacy we have been allowed to fool ourselves. **We've lost the ability to read anonymously. Without anonymity in reading there is no freedom of mind, there's literally slavery** What is actually a subject of environmental regulation has been sold to us as a mere matter of bilateral bargaining. The facts show this is completely untrue. An environmental devastation has been produced by the ceaseless pursuit of profit from data-mining in every legal way imaginable. Restraints that should have existed in the interest of protection against environmental degradation have never been imposed. There is a tendency to blame oversharing. We are often told that the real problem of privacy is that kids are just sharing too darn much. When you democratise media, which is what we are doing with the net, ordinary people will naturally say more than they ever said before. This is not the problem. In a free society people should be protected in their right to say as much or as little as they want. The real problem is that we are losing the anonymity of reading, for which nobody has contracted at all. We have lost the ability to read anonymously, but the loss is concealed from us because of the way we

built the web. We gave people programs called "browsers" that everyone could use, but we made programs called "web servers" that only geeks could use – very few people have ever read a web server log. This is a great failing in our social education about technology. It's equivalent to not showing children what happens if cars collide and people aren't wearing seat belts. We don't explain to people how a web server log captures in detail the activity of readers, nor how much you can learn about people, because of what and how they read. **From the logs, you can learn how long each reader spends on each page, how she reads it, where she goes next, what she does or searches for on the basis of what she's just read.** If you can collect all that information in the logs, then you are beginning to possess what you ought not to have. Without anonymity in reading there is no freedom of the mind. Indeed, there is literally slavery. Reading was the pathway, the abolitionist Frederick Douglass wrote, from slavery to freedom. Writing his memoir of his own journey, Douglass recalled that when one of his owners tried to prevent him from reading, "I now understood what had been to me a most perplexing difficulty – to wit, the white man's power to enslave the black man." But what if every book and newspaper he touched had reported him? If you have a Facebook account, Facebook is surveilling every single moment you spend there. Moreover, much more importantly, every web page you touch that has a Facebook "like" button on it which, whether you click the button or not, will report your reading of that page to Facebook. If the newspaper you read every day has Facebook "like" buttons or similar services' buttons on those pages, then Facebook or the other service watches you read the newspaper: it knows which stories you read and how long you spent on them. Every time you tweet a URL, Twitter is shortening the URL for you. But it is also arranging that anybody who clicks on that URL will be monitored by Twitter as they read. You are not only helping people know what's on the web, but also helping Twitter read over everybody's shoulder everything you recommend. This isn't transactional, this is ecological. This is an environmental destruction of other people's freedom to read. Your activity is designed to help them find things they want to read. Twitter's activity is to disguise the surveillance of the resulting reading from everybody. We allowed this system to grow up so quickly around us that we had no time to understand its implications. By the time the implications have been thought about, the people who understand are not interested in talking, because they have got an edge, and that edge is directed at you. Commercial surveillance then attracts government attention, with two results that Snowden has documented for us: complicity and outright thievery. **The data-mining companies** believed, they say, that they were merely in a situation of complicity with government. Having created unsafe technological structures that mined you, they thought they were merely engaged in undisclosed bargaining over how much of what they had on you they should deliver. This was, of course, a mingled game of greed and fear. What the US data-mining companies basically believed, or wanted us to believe they believed until Snowden woke them, was that by complicity they had gained immunity from actual thievery. But we have now learned their complicity bought them nothing. They **sold us out halfway, and government stole the rest.** They discovered that what they had expected by way of honesty from the US listeners, the NSA and other agencies, they hadn't got at all. The US listeners' attitude evidently was: "What's ours is ours, and what's yours is negotiable. Unless we steal it first." Like the world financial industry, the great data-mining companies took the promises of the US military listeners too seriously. That, at any rate, is the charitable interpretation of their conduct. They thought there were limits to what power would do. **Thanks to Snowden, for the data-miners, as for the US listeners, the situation is no longer politically controllable. They have lost their credibility, their trustworthiness, before the world. If they fail to regain their customers' trust, notwithstanding how convenient, even necessary, their services may seem to us, they are finished.** Environmental problems – such as climate change, water pollution, slavery, or the destruction of privacy – are not solved transactionally by individuals. It takes a union to destroy slavery. The essence of our difficulty, too, is union. Another characteristic of the great data-miners is that there is no union within or around them. They are now public corporations, but the union of shareholders is ineffective in controlling their environmental misdoing. These companies are remarkably opaque with respect to all that they actually do, and they are so valuable that shareholders will not kill the goose that lays the golden egg by inquiring whether their business methods are ethical. A few powerful individuals control all the real votes in these companies. Their workforces do not have a collective voice. Snowden has been clear all along that the remedy for this environmental destruction is democracy. But he has also repeatedly pointed out that, where workers cannot speak up and there is no collective voice, there is no protection for the public's right to know. When there is no collective voice for those who are within structures that deceive and oppress, then somebody has to act courageously on his own. Before Augustus, the Romans of the late republic knew the secrecy of the ballot was essential to the people's right. **In every country in the world that holds meaningful elections, Google knows how you are going to vote. It's**

already shaping your political coverage for you, in your customised news feed, based upon what you want to read, and who you are, and what you like. Not only does it know how you're going to vote, it's helping to confirm you in your decision to vote that way – unless some other message has been purchased by a sponsor. Without the anonymity of reading there is no democracy. I mean of course that there aren't fair and free elections, but much more deeply than that I mean there is no such thing as free self-governance. And we are still very ill-informed, because there are no unions seeking to raise ethical issues inside the data-miners, and we have too few Snowdens. The futures of the data-miners are not all the same. Google as an organisation has concerned itself with the ethical issues of what it does from the very beginning. Larry Page and Sergey Brin [the founders of Google] did not stumble randomly on the idea that they had a special obligation not to be evil. They understood the dangerous possibilities implicit in the situation they were creating. It is technically feasible for Google to make Gmail into a system that is truly secure and secret, though not anonymous, for its users. Mail could be encrypted – using public keys in a web of trust – within users' own computers, in their browsers; email at rest at Gmail could be encrypted using algorithms to which the user, rather than Google, has the relevant keys. Google would be forgoing Gmail's scant profit, but its actions would be consistent with the idea that the net belongs to its users throughout the world. In the long run it is good for Google to be seen not only to believe, but to act upon, this idea, for it is the only way for it to regain those users' trust. There are many thoughtful, dedicated people at Google who must choose between doing what is right and blowing the whistle on what is wrong. The situation at Facebook is different. Facebook is strip-mining human society. Watching everyone share everything in their social lives and instrumenting the web to surveil everything they read outside the system is inherently unethical. But we need no more from Facebook than truth in labelling. We need no rules, no punishments, no guidelines. We need nothing but the truth. Facebook should lean in and tell its users what it does. It should say: "We watch you every minute that you're here. We watch every detail of what you do. We have wired the web with 'like' buttons that inform on your reading automatically." To every parent Facebook should say: "Your children spend hours every day with us. We spy upon them much more efficiently than you will ever be able to. And we won't tell you what we know about them." Only that, just the truth. That will be enough. But the crowd that runs Facebook, that small bunch of rich and powerful people, will never lean in close enough to tell you the truth. Mark Zuckerberg recently spent \$30m (£18m) buying up all the houses around his own in Palo Alto, California. Because he needs more privacy. So do we. We need to make demands for that privacy on both governments and companies alike. Governments, as I have said, must protect us against spying by other governments, and must subject their own domestic listening to the rule of law. Companies, to regain our trust, must be truthful about their practices and their relations with governments. We must know what they really do, so we can decide whether to give them our data. The president must end this war in the net, which deprives us of civil liberties under the guise of depriving foreign bad people of sanctuary A great deal of confusion has been created by the distinction between data and metadata, as though there were a difference and spying on metadata were less serious. Illegal interception of the content of a message breaks your secrecy. Illegal interception of the metadata of a message breaks your anonymity. It isn't less, it's just different. Most of the time it isn't less, it's more. In particular, the anonymity of reading is broken by the collection of metadata. It wasn't the content of the newspaper Douglass was reading that was the problem – it was that he, a slave, dared to read it. The president can apologise to people for the cancellation of their health insurance policies, but he cannot merely apologise to the people for the cancellation of the constitution. When you are president of the United States, you cannot apologise for not being on Frederick Douglass's side. Nine votes in the US supreme court can straighten out what has happened to our law. But the US president has the only vote that matters concerning the ending of the war. All the governmental destruction of privacy that has been placed atop the larger ecological disaster created by industry, all of this spying is wartime stuff. The president must end this war in the net, which deprives us of civil liberties under the guise of depriving foreign bad people of sanctuary. A man who brings evidence to democracy of crimes against freedom is a hero. A man who steals the privacy of societies for his profit is a villain. We have sufficient villainy and not enough heroism. We have to name that difference strongly enough to encourage others to do right. We have seen that, with the relentlessness of military operation, the listeners in the US have embarked on a campaign against the privacy of the human race. They have compromised secrecy, destroyed anonymity, and adversely affected the autonomy of billions of people. They are doing this because they have been presented with a mission by an extraordinarily imprudent US administration, which – having failed to prevent a very serious attack on civilians at home, largely by ignoring warnings – decreed that it would never again be put in a position where it "should have known". The UK government must cease to vitiate

the civil liberties of its people. It must cease to deny the freedom of the press. The fundamental problem was the political, not the military, judgment involved. When military leaders are given objectives, they achieve them at whatever collateral cost they are not explicitly prohibited from incurring. That is why we regard civilian control of the military as a sine qua non of democracy. Democracy also requires an informed citizenry. About this, Snowden agrees with Thomas Jefferson [the chief author of America's Declaration of Independence], and pretty much everybody else who has ever seriously thought about the problem. Snowden has shown us the immense complicity of all governments. He has shown, in other words, that everywhere the policies the people want have been deliberately frustrated by their governments. They want to be protected against the spying of outsiders. They want their own government's national security surveillance activities to be conducted under the independent scrutiny that characterises the rule of law. In addition, the people of the United States are not ready to abandon our role as a beacon of liberty to the world. We are not prepared to go instead into the business of spreading the procedures of totalitarianism. We never voted for that. The people of the US do not want to become the secret police of the world. If we have drifted there because an incautious administration empowered the military, it is time for the people of the United States to register their conclusive democratic opinion. We are not the only people in the world to have exigent political responsibilities. The government of the UK must cease to vitiate the civil liberties of its people, it must cease to use its territory and its transport facilities as an auxiliary to American military misbehaviour. And it must cease to deny freedom of the press. It must stop pressuring publishers who seek to inform the world about threats to democracy, while it goes relatively easy on publishers who spy on the families of murdered girls. The chancellor of Germany must stop talking about her mobile phone and start talking about whether it is OK to deliver all the telephone calls and text messages in Germany to the US. Governments that operate under constitutions protecting freedom of expression have to inquire, urgently, whether that freedom exists when everything is spied on, monitored, listened to. In addition to politics, we do have lawyering to do. Defending the rule of law is always lawyers' work. In some places those lawyers will need to be extremely courageous; everywhere they will need to be well trained; everywhere they will need our support and our concern. But it is also clear that subjecting government listening to the rule of law is not the only lawyers' work involved. As we have seen, the relations between the military listeners of the United States, listeners elsewhere in the world, and the big data-mining businesses are too complex to be safe for us. Snowden's revelations have shown that the US data-mining giants were intimidated, seduced, and also betrayed by the listeners. This should not have surprised them, but it apparently did. Many companies manage our data; most of them have no enforceable legal responsibility to us. There is lawyers' work to do there too. In the US, for example, we should end the immunity given to the telecommunications operators for assisting illegal listening. Immunity was extended by legislation in 2008. When he was running for president, Barack Obama said that he was going to filibuster that legislation. Then, in August 2008, when it became clear that he was going to become the next president, he changed his mind. Not only did he drop his threat to filibuster the legislation, he interrupted his campaigning in order to vote for immunity. We need not argue about whether immunity should have been extended. We should establish a date – perhaps 21 January 2017 – after which any telecommunications operator doing business in the US and facilitating illegal listening should be subject to ordinary civil liability. An interesting coalition between the human rights lawyers and commercial class action litigators would grow up immediately with very positive consequences. The people of the United States are not ready to abandon our role as a beacon of liberty to the world. We are not prepared to go instead into the business of spreading the procedures of totalitarianism. If non-immunisation extended to non-US network operators that do business in the United States, such as Deutsche Telekom, it would have enormous positive consequences for citizens of other countries as well. In any country where de facto immunity presently exists and can be withdrawn, it should be lifted. The legal issues presented by the enormous pile of our data in other people's hands are well-known to all systems of law. The necessary principles are invoked every time you take your clothes to the cleaners. English-speaking lawyers refer to these principles as the law of "bailment". What they mean is, if you entrust people with your stuff, they have to take care of it as least as well as they take care of their own. If they fail, they are liable for their negligence. We need to apply the principle of trust in bailment, or whatever the local legal vocabulary is, to all that data we have entrusted to other people. This makes them legally responsible to us for the way they take care of it. There would be an enormous advantage in treating personal data under the rules of bailment or its equivalent. Such rules are governed by the law where the trust is made. If the dry cleaner chooses to move your clothes to another place where a fire breaks out, it doesn't matter where that fire happened: the relevant law is the law of the place where they took the clothes from you. The big data-mining companies

play this game of lex loci server all the time: "Oh we are not really in country X, we're in California, that's where our computers are." This is a bad legal habit. We would not be doing them a grave disservice if we helped them out of it. Then there is lawyering to be done in international public law. We must hold governments responsible to one another for remedying current environmental devastation. The two most powerful governments in the world, the US and China, now fundamentally agree about their policy with respect to threats in the net. The basic principle is: "Anywhere in the net there is a threat to our national security, we're going to attack it." The US and the Soviet Union were in danger of poisoning the world in the 1950s through atmospheric testing of nuclear weapons. To their credit, they were able to make a bilateral agreement prohibiting it. The US and the government of China could agree not to turn the human race into a free-fire zone for espionage. But they won't. We must pursue legal and political redress for what has been done to us. But politics and law are too slow and too uncertain. Without technical solutions we are not going to succeed, just as there is no way to clean up the air and the water or positively affect global climate without technological change. Everywhere, businesses use software that secures their communications and much of that software is written by us. The "us" I mean here is those communities sharing free or open source software, with whom I have worked for decades. Protocols that implement secure communications used by businesses between themselves and with consumers (HTTPS, SSL, SSH, TLS, OpenVPN etc) have all been the target of the listeners' interference. Snowden has documented their efforts to break our cryptography. The US listeners are courting global financial disaster. If they ever succeed in compromising the fundamental technical methods by which businesses communicate securely, we would be one catastrophic failure away from global financial chaos. Their conduct will appear to the future to be as economically irresponsible as the debasing of the Roman coinage. It is a basic threat to the economic security of the world. The bad news is that they have made some progress towards irremediable catastrophe. First, they corrupted the science. They covertly affected the making of technical standards, weakening everyone's security everywhere in order to make their own stealing easier. Second, they have stolen keys, as only the best-financed thieves in the world can do. Everywhere encryption keys are baked into hardware, they have been at the bakery. At the beginning of September when Snowden's documents on this subject first became public, the shock waves reverberated around the industry. But the documents released also showed that the listeners are still compelled to steal keys instead of breaking our locks. They have not yet gained enough technical sophistication to break the fundamental cryptography holding the global economy together. Making public what crypto NSA can't break is the most inflammatory of Snowden's disclosures from the listeners' perspective. As long as nobody knows what the listeners cannot read, they have an aura of omniscience. Once it is known what they cannot read, everyone will use that crypto and soon they cannot read anything any more. Snowden has disclosed that their advances on our fundamental cryptography were good but not excellent. He is also showing us that we have very little time to improve our own cryptography. We must hurry to recover from the harm done to us by technical standards corruption. From now on, the communities that make free software crypto for everyone else must assume that they are up against "national means of intelligence". In this trade, that is bad news for developers, because that's the big leagues. When you play against their opposition, even the tiniest mistake is fatal. It's as though every factory in our society had an advanced fire safety system - while everybody's home had nothing. Second, we must change the technical environment so it is safer for ordinary people and small businesses. This is largely about spreading technologies big businesses have been using for a decade and a half. Far too little has so far happened along these lines. It's as though every factory in our society had an advanced fire safety system – smoke detectors, carbon monoxide detectors, sprinklers, high pressure hoses, fancy fire extinguishers – while everybody's home had nothing. We must commoditise personal uses of the communication security and privacy technologies that businesses have already adopted. This has to be as simple as installing a smoke detector, hanging a fire extinguisher on the wall, talking to your kids about which door to use if the stairs are burning, or even putting a rope ladder in a second-floor window. None of this solves the problem of fire. But if a blaze breaks out, these simple measures will save your child's life. There are many software projects and startup companies working on these measures. My FreedomBox is one such non-profit project. But I am particularly delighted to see we are beginning to have commercial competition. Businesses are now aware: the people of the world have not agreed that the technology of totalitarianism should be fastened on every household. If the market offers them good products that make this spying harder, they will buy and use them. We must commoditise personal uses of the communication security and privacy technologies that businesses have already adopted. If the market offers them good products that make this spying harder, they will buy and use them. Snowden's courage is exemplary. But he ended his effort because we needed to know now. We have to inherit his understanding

of that fierce urgency. Our politics can't wait. Not in the US, where the war must end. Not around the world, where people must demand that governments fulfil the basic obligation to protect their security. We need to decentralise the data. If we keep it all in one great big pile – if there's one guy who keeps all the email and another guy who manages all the social sharing – then there isn't really any way to be any safer than the weakest link in the fence around those piles. But if everyone is keeping her and his own, then the weak links on the outside of any fence get the attacker exactly one person's stuff. Which, in a world governed by the rule of law, might be optimal: one person is the person you can spy on because you've got probable cause. Email scales beautifully without anybody at the centre keeping all of it. We need to make a mail server for people that costs five bucks and sits on the kitchen counter where the telephone answering machine used to be. If it breaks, you throw it away. Decentralised social sharing is harder, but not so hard that we can't do it. For the technologically gifted and engaged around the world this is the big moment, because if we do our work correctly freedom will survive and our grandkids will say: "So what did you do back then?" The answer could be: "I made SSL better." Snowden has nobly advanced our effort to save democracy. In doing so he stood on the shoulders of others. The honour will be his and theirs, but the responsibility is ours. It is for us to finish the work that they have begun. We must see to it that their sacrifices have meaning. That this nation, and all the nations, shall have a new birth of freedom, and that government of the people, by the people, for the people shall not perish from the Earth. The NSA, like the totalitarian spy agencies of the past, believes it is entitled to all the world's knowledge. Directly following 9/11, the Bush administration began a data-mining program called "Total Information Awareness," and the NSA has stated publicly that it intends to "live on the network." That arrogance belies an underlying naivety about our true ability to prevent violence, which at some point no amount of secret billions in the spy budget will change. And aggressive behavior — like tapping the phones of world leaders and spying on hundreds of millions of foreign nationals — has negative consequences for us, whatever our intentions are. While some legitimate foreign surveillance is necessary, the NSA's unlimited ambitions, which includes efforts to undermine the encryption standards we rely on for basic privacy, undermines overall trust in the internet for everyone. American exceptionalism cannot justify making our friends insecure; it ought to demand the opposite. In an 1822 letter to Kentucky Lt. Governor W.T. Barry, James Madison wrote that "a popular Government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or perhaps both." Madison's letter, originally espousing a robust public education system for Kentucky, has since been used as an appeal for open government. "A people who mean to be their own governors," Madison wrote, "must arm themselves with the power which knowledge gives." Today, the people appear utterly unarmed against the National Security Agency, which holds a incredible amount of knowledge about citizens while withholding essential facts about how it spies on them. That secret knowledge is secret power, which is anathema to democracy when in the hands of an unaccountable elite. During colonial rule, "general warrants" from the British crown threatened the safe spaces of American social life by allowing the King's agents to search anyone, anywhere, at any time, regardless of whether they were suspected of a crime. Today, many of those spaces are on the internet — a place we can no longer trust to be secure from our own military, which considers many parts of your electronic life beyond the protections of the Bill of Rights. Only by ending the bulk surveillance of American citizens immediately, and by rebuilding the federal oversight intended to keep the NSA from violating the law, can trust in our democracy be restored.

Tyranny Creep

Mass surveillance leads to creeping tyranny

T.C. Slottek, December 12, 2013, "The NSA is out of control and must be stopped," The Verge,
<http://www.theverge.com/2013/12/12/5200142/end-the-nsa-nightmare>

Of course, none of the NSA's surveillance programs, irrational "homeland security" policies, or limitless wars started in the past decade would be possible without the nagging specter of terrorism. In the years following 9/11, President Bush, President Obama, and Congressional leaders have obsequiously accepted dubious claims about the threat of terrorism, eroding the Fourth and Fifth Amendments in the expanding intelligence bureaucracy's wake. Even calls to rein in the NSA from the most reform-minded members of Congress are framed by the specious idea that terrorism is the nation's supreme hazard. "Our first priority is to keep Americans safe from the threat of terrorism," Senator Ron Wyden wrote in a November op-ed. Nevermind the fact that Americans are roughly four times more likely to be killed by lightning than by a terrorist. You would think the National Weather Service might be able to get a larger piece of the federal pie, or at least a color-coded thunderstorm advisory system. Instead, we have airport pat downs and PRISM Do we need to be afraid of the NSA, as one might be afraid of a boot stamping on a human face, forever? Probably not. But the erosion of American civil liberties won't appear out of thin air as an Orwellian caricature of totalitarianism. It looks more like a computer server silently blinking in a Utah data center, as it reconstructs the connective tissue of your entire life: a thorough diagram of your existence that can be recalled at any time by someone with the right permission level and the right query. Who'll be behind the machines in four years? How about in 20? Who will our enemies be then?

Surveillance Bad – Social Control

Surveillance creates social control.

Schneier 15 Bruce Schneier is an internationally renowned security technologist, called a "security guru" by The Economist. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc., 3/2/15, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, p.96

INHIBITING DISSENT AND SOCIAL CHANGE These chilling effects are especially damaging to political discourse. There is value in dissent. And, perversely, there can be value in lawbreaking. These are both ways we improve as a society. **Ubiquitous mass surveillance is the enemy of democracy, liberty, freedom, and progress.**

Defending this assertion involves a subtle argument something I wrote about in my previous book Liars and Outliers—but it's vitally important to society. Think about it this way. Across the US, states are on the verge of reversing decades old laws about homosexual relationships and marijuana use. If the old laws could have been perfectly enforced through surveillance, society would never have reached the point where the majority of citizens thought those things were okay. There has to be a period where they are still illegal yet increasingly tolerated, so that people can look around and say, "You know, that wasn't so bad." Yes, the process takes decades, but it's a process that can't happen without lawbreaking. Frank Zappa said something similar in 1971: "Without deviation from the norm, progress is not possible." The perfect enforcement that comes with ubiquitous government surveillance chills this process. We need imperfect security—systems that free people to try new things, much the way off-the-record brainstorming sessions loosen inhibitions and foster creativity. If we don't have that, we can't slowly move from a thing's being illegal and not okay, to illegal and not sure, to illegal and probably okay, and finally to legal. This is an important point. Freedoms we now take for granted were often at one time viewed as threatening or even criminal by the past power structure. Those changes might never have happened if the authorities had been able to achieve social control through surveillance.

This is one of the main reasons all of us should care about the emerging architecture of surveillance, even if we are not personally chilled by its existence. We suffer the effects because people around us will be less likely to proclaim new political or social ideas, or act out of the ordinary. If J. Edgar Hoover's surveillance of Martin Luther King Jr. had been successful in silencing him, it would have affected far more people than King and his family. Of course, many things that are illegal will rightly remain illegal forever: theft, murder, and so on. Taken to the extreme, though, perfect enforcement could have unforeseen repercussions. What does it mean for society if the police can track your car 24/7, and then mail you a bill at the end of the month itemizing every time you sped, ran a red light, made an illegal left turn, or followed the car in front of you too closely? Or if your township can use aerial surveillance to automatically fine you for failing to mow your lawn or shovel your walk regularly? Our legal systems are largely based on human judgment. And while there are risks associated with biased and prejudiced judgments, there are also risks associated with replacing that judgment with algorithmic efficiency. Ubiquitous surveillance could lead to the kind of society depicted in the 2002 Tom Cruise movie Minority Report, where people can become the subject of police investigations before they commit a crime. Already law enforcement agencies make use of predictive analytic tools to identify suspects and direct investigations. It's a short step from there to the world of Big Brother and thoughtcrime. This notion of making certain crimes impossible to get away with is new—a potential result of all this new technology—and it's something we need to think about carefully before we implement it. As law professor Yochai Benkler said, "Imperfection is a core dimension of freedom."

Surveillance is a means of social control—it creates a commodified subject that is forced to fit into a predetermined mold

McFarland 15 (Michael, "Why We Care about Privacy",
<http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Autonomy is part of the broader issue of human dignity, that is, the obligation to treat people not merely as means, to be bought and sold and used, but as valuable and worthy of respect in themselves. As the foregoing has made clear, personal information is an extension of the person. To have access to that information is to have access to the person in a particularly intimate way. When some personal information is taken and sold or distributed, especially against the person's will, whether it is a diary or personal letters, a record of buying habits, grades in school, a list of friends and associates or a psychological history, it is as if some part of the person has been alienated and turned into a commodity. In that way the person is treated merely as a thing, a means to be used for some other end.

Privacy and Power

Privacy is even more necessary as a safeguard of freedom in the relationships between individuals and groups. As Alan Westin has pointed out, surveillance and publicity are powerful instruments of social control.⁸ If individuals know that their actions and dispositions are constantly being observed, commented on and criticized, they find it much harder to do anything that deviates from accepted social behavior. There does not even have to be an explicit threat of retaliation. "Visibility itself provides a powerful method of enforcing norms."⁹ Most people are afraid to stand apart, to be different, if it means being subject to piercing scrutiny. The "deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."¹⁰ Under these circumstances they find it better simply to conform. This is the situation characterized in George Orwell's 1984 where the pervasive surveillance of "Big Brother" was enough to keep most citizens under rigid control.¹¹

Therefore privacy, as protection from excessive scrutiny, is necessary if individuals are to be free to be themselves. Everyone needs some room to break social norms, to engage in small "permissible deviations" that help define a person's individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves. As Brian Stelter wrote in the New York Times on the loss of anonymity in today's online world, "The collective intelligence of the Internet's two billion users, and the digital fingerprints that so many users leave on Web sites, combine to make it more and more likely that every embarrassing video, every intimate photo, and every indelicate e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view."¹²

Surveillance creates Social control.

Balkin 2008

Jack M., Knight Professor of Constitutional Law and the First Amendment, Yale Law School. "The Constitution in the National Surveillance State." Minnesota Law Review, Vol. 93, No. 1, 2008; Yale Law School, Public Law Working Paper No. 168. Available at SSRN: <http://ssrn.com/abstract=1141524>

Today's National Surveillance State goes beyond Foucault's Panoptic model. Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data. Much public and private surveillance occurs without any knowledge that one is watched. More to the point, data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes.⁵ Over time, these tools will only become more effective.

We leave traces of ourselves continually, including our location, our communications contacts, our consumption choices—even our DNA. Data mining allows inferences not only about the direct subjects of surveillance, but about other people with whom they live, work, and communicate.⁵⁴ Instead of spying on a particular person, data about other persons combined with public facts about a person can allow governments and private businesses to draw increasingly powerful inferences about that person's motives, desires, and behaviors.⁵⁵

The problem today is not that fear of surveillance will lead people to docile conformity, but rather that even the most innocent and seemingly unimportant behaviors can increase knowledge about both ourselves and others.⁵⁶ Normal behavior does not merely acquiesce to the state's power; it may actually amplify it, adding information to databases that makes inferences more powerful and effective. Our behavior may tell things about us that we may not even know about ourselves. In addition, knowledge about some people can generate knowledge about others who are not being directly watched. Individuals can no longer protect themselves simply by preventing the government from watching them, for the government may no longer need to watch them to gain knowledge that can be used against them.

Equally important, the rise of the National Surveillance State portends the death of amnesia. In practice, much privacy protection depends on forgetting. When people display unusual or embarrassing behavior, or participate in political protests in public places, their most effective protection may be that most people don't know who they are and will soon forget who did what at a certain time and place. But cameras, facial recognition systems, and location tracking systems let governments and businesses compile continuous records of what happens at particular locations, which can be collated with records of different times and places. The collation and analysis of events allows public and private actors to create locational and temporal profiles of people, making it easier to trace and predict their behaviors.⁵⁷ Older surveillance cameras featured imprecise, grainy images, and the recordings were quickly taped over. New digital systems offer ever greater fidelity and precision,⁵⁸ and the declining cost of digital storage means that records of events can be maintained indefinitely and copied and distributed widely to other surveillance systems around the country or even around the globe.⁵⁹ Ordinary citizens can no longer assume that what they do will be forgotten; rather, records will be stored and collated with other information collected at other times and places.⁶⁰ The greatest single protector of privacy amnesia—will soon be a thing of the past. As technology improves and storage costs decline, the National Surveillance State becomes the State that Never Forgets.⁶¹

The National Surveillance State poses three major dangers for our freedom. Because the National Surveillance State emphasizes ex ante prevention rather than ex post apprehension and prosecution, the first danger is that government will create a parallel track of preventative law enforcement that routes around the traditional guarantees of the Bill of Rights. The Bush administration's military detention practices and its NSA surveillance program are two examples. The administration justified detaining and interrogating people—including American citizens—in ways that would have violated traditional legal restraints on the grounds that it was not engaged in ordinary criminal law enforcement.ⁿ⁶² It sought intelligence that would prevent future attacks and wanted to prevent terrorists from returning to the battlefield.ⁿ⁶³ Similarly, the administration defended warrantless surveillance of people in the United States by arguing that the President was not engaged in criminal prosecutions but in collection of military intelligence designed to fight terrorism.ⁿ⁶⁴

[*16] The second danger posed by the National Surveillance State is that traditional law enforcement and social services will increasingly resemble the parallel track. Once governments have access to powerful surveillance and data mining technologies, there will be enormous political pressure to use them in everyday law enforcement and for delivery of government services. If data mining can help us locate terrorists, why not use it to find deadbeat dads, or even people who have not paid their parking tickets?ⁿ⁶⁵ If surveillance technologies signal that certain people are likely threats to public order, why not create a system of preventive detention outside the ordinary criminal justice system?ⁿ⁶⁶ Why not impose sanctions outside the criminal law, like denying people the right to board airplanes or use public facilities and transportation systems? And if DNA analysis can identify people who will likely impose high costs on public resources, why not identify them in advance and exclude them from public programs and other opportunities? The

more powerful and effective our technologies of surveillance and analysis become, the more pressure the government will feel to route around warrant requirements and other procedural hurdles so that it can catch potential troublemakers more effectively and efficiently before they have a chance to cause any harm.

Private power and public-private cooperation pose a third danger. Because the Constitution does not reach private parties, government has increasing incentives to rely on private [*17] enterprise to collect and generate information for it. n67 Corporate business models, in turn, lead companies to amass and analyze more and more information about people in order to target new customers and reject undesirable ones. As computing power increases and storage costs decline, companies will seek to know more and more about their customers and sell this valuable information to other companies and to the government.

If some form of the National Surveillance State is inevitable, how do we continue to protect individual rights and constitutional government? Today's challenge is similar to that faced during the first half of the twentieth century, when government transitioned into the Welfare State and the National Security State. Americans had to figure out how to tame these new forms of governance within constitutional boundaries. It is no accident that this period spawned both the New Deal - with its vast increase in government power - and the Civil Rights Revolution. The more power the state amasses, the more Americans need constitutional guarantees to keep governments honest and devoted to the public good.

Surveillance Bad – Dehumanization

Violations of privacy are dehumanizing.

Schneier, 2015

Bruce Schneier a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc., 3/2/15, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*,

The most common misconception about privacy is that it's about having something to hide. "If you aren't doing anything wrong, then you have nothing to hide," the saying goes, with the obvious implication that privacy only aids wrongdoers. If you think about it, though, this makes no sense. We do nothing wrong when we make love, go to the bathroom, or sing in the shower. We do nothing wrong when we search for a job without telling our current employer. We do nothing wrong when we seek out private places for reflection or conversation, when we choose not to talk about something emotional or personal, when we use envelopes for our mail, or when we confide in a friend and no one else. Moreover, even those who say that don't really believe it. In a 2009 interview, Google CEO Eric Schmidt put it this way: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." But in 2005, Schmidt banned employees from talking to reporters at CNET because a reporter disclosed personal details about Schmidt in an article. Facebook's Mark Zuckerberg declared in 2010 that privacy is no longer a "social norm," but bought the four houses abutting his Palo Alto home to help ensure his own privacy. There are few secrets we don't tell someone, and we continue to believe something is private even after we've told that person. We write intimate letters to lovers and friends, talk to our doctors about things we wouldn't tell anyone else, and say things in business meetings we wouldn't say in public. We use pseudonyms to separate our professional selves from our personal selves, or to safely try out something new. Facebook's CEO Mark Zuckerberg showed a remarkable naiveté when he stated, "You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly. Having two identities for yourself is an example of a lack of integrity." We're not the same to everyone we know and meet. We act differently when we're with our families, our friends, our work colleagues, and so on. We have different table manners at home and at a restaurant. We tell different stories to our children than to our drinking buddies. It's not necessarily that we're lying, although sometimes we do; it's that we reveal different facets of ourselves to different people. This is something innately human. Privacy is what allows us to act appropriately in whatever setting we find ourselves. In the privacy of our home or bedroom, we can relax in a way that we can't when someone else is around. Privacy is an inherent human right, and a requirement for about choice, and having the power to control how you present yourself to the world. Internet ethnographer danah boyd puts it this way: **"Privacy doesn't just depend on agency; being able to achieve privacy is an expression of agency."** When we lose privacy, we lose control of how we present ourselves. We lose control when something we say on Facebook to one group of people gets accidentally shared with another, and we lose complete control when our data is collected by the government. "How did he know that?" we ask. How did I lose control of who knows about my traumatic childhood, my penchant for tasteless humor, or my vacation to the Dominican Republic? You may know this feeling: you felt it when your mother friended you on Facebook, or on any other social networking site that used to be just you and your friends. Privacy violations are intrusions. There's a strong physiological basis for privacy. Biologist Peter Watts makes the point that a desire for privacy is innate: mammals in particular don't respond well to surveillance. We consider it a physical threat, because animals in the natural world are surveilled by predators. Surveillance makes us feel like prey, just as it makes the surveillors act like predators. Psychologists, sociologists, philosophers, novelists, and technologists have all written about the effects of constant surveillance, or even just the perception of constant surveillance. Studies show that we are less healthy, both physically and emotionally. We have feelings of low self-esteem, depression, and anxiety. **Surveillance strips us of our dignity. It threatens our very selves as individuals. It's a dehumanizing tactic employed in prisons and detention camps around the world.** Violations of privacy are not all equal. Context matters. There's a difference between a Transportation Security Administration (TSA) officer finding porn in your suitcase and your spouse finding it. There's a difference between the police learning about your drug use and your friends learning about it. **And violations of privacy aren't all equally damaging. Those of us in marginal socioeconomic situations—and marginalized racial, political, ethnic, and religious groups—are affected more.** Those of us in powerful positions who are subject to people's continued approval are affected more. The lives of some

of us depend on privacy. Our privacy is under assault from constant surveillance. Understanding how this occurs is critical to understanding what's at stake.

Surveillance Bad – Constitutionality

Metadata collection violates the first and fourth amendments

Price 15 — Michael W. Price, counsel for the Brennan Center's Liberty and National Security Program, which seeks to ensure that our government respects human rights and fundamental freedoms in conducting the fight against terrorism, 2015 ("Rethinking Privacy: Fourth Amendment "Papers" and the Third Party Doctrine," *Brennan Center for Justice*, June 29th.

Available online at <https://www.brennancenter.org/analysis/rethinking-privacy-fourth-amendment-papers-and-third-party-doctrine>, accessed on 7-17-15)

I specifically address communications metadata in Section IV. But suffice it to say here that metadata generally is quite capable of revealing information about one's political or religious associations, interests and dislikes, or habits and predilections that would otherwise be difficult to determine.¹⁹⁹ That is precisely why law enforcement and intelligence agencies are so eager to collect and analyze it.²⁰⁰ Analyzing a cache of metadata over time can be more telling than the content of the messages themselves. The metadata associated with a single email to a group of supporters could easily reveal the membership list of a political organization. It is possible to map entire social networks, identify influential members, or see who is on the outs.²⁰¹ It is likely to reveal relationships with lawyers, lovers, religious counselors, and political organizations.²⁰² What's more, the use of sophisticated computer algorithms to detect patterns and anomalies reduces this task to a few mouse clicks.²⁰³ This type of intrusion can implicate First Amendment freedom of expression and association with even greater force and ease than slogging through the actual content of communications.²⁰⁴ Thus, metadata associated with protected content should receive the same Fourth Amendment protection as the content itself. The same should hold true for the metadata generated by cloud computing.

Digital privacy is protected under the fourth amendment — Smith v. Maryland is outdated, data is not given voluntarily

Watzel 14 — Ryan Watzel, Law Clerk, U.S. Court of Appeals for the Second Circuit, JD from Yale Law School, BA from University of Miami, 2014 ("Riley's Implications for Fourth Amendment Protection in the Cloud," *Yale Law Journal*, Vol. 124, September 11th, Accessible online at <http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud>, accessed on 7-17-15)

Recently, however, some courts have distinguished Smith in the context of digital data by finding that such data is not "voluntarily" provided to third parties. For example, in United States v. Warshak, the Sixth Circuit found that email users have an expectation of privacy in emails saved by their internet service providers.¹⁰ Earlier this year, the Eleventh Circuit in United States v. Davis held that cell phone users have an expectation of privacy in cell site location data.¹¹ Most significantly, Justice Sotomayor stated in her concurrence in *United States v. Jones* that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."¹² Smith's approach, according to Justice Sotomayor, "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."¹³ Consequently, Justice Sotomayor advised that she "would not assume that all information voluntarily

disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”¹⁴ Although the Jones majority did not reconsider the third-party doctrine in that case, Justice Sotomayor’s concurrence questioning the doctrine’s applicability to digital data has become influential among judges,¹⁵ scholars,¹⁶ and even the Court itself.¹⁷

Digital privacy is protected under the fourth amendment — Smith v. Maryland is outdated, data is not given voluntarily

Watzel 14 — Ryan Watzel, Law Clerk, U.S. Court of Appeals for the Second Circuit, JD from Yale Law School, BA from University of Miami, 2014 (“Riley’s Implications for Fourth Amendment Protection in the Cloud,” *Yale Law Journal*, Vol. 124, September 11th, Accessible online at <http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud>, accessed on 7-17-15)

Recently, however, some courts have distinguished Smith in the context of digital data by finding that such data is not “voluntarily” provided to third parties. For example, in United States v. Warshak, the Sixth Circuit found that email users have an expectation of privacy in emails saved by their internet service providers.¹⁰ Earlier this year, the Eleventh Circuit in United States v. Davis held that cell phone users have an expectation of privacy in cell site location data.¹¹ Most significantly, Justice Sotomayor stated in her concurrence in *United States v. Jones* that “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”¹² Smith’s approach, according to Justice Sotomayor, “is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”¹³ Consequently, Justice Sotomayor advised that she “would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”¹⁴ Although the Jones majority did not reconsider the third-party doctrine in that case, Justice Sotomayor’s concurrence questioning the doctrine’s applicability to digital data has become influential among judges,¹⁵ scholars,¹⁶ and even the Court itself.¹⁷

Privacy is protected under the constitution

The University of Missouri

Kansas City is a public research university located in Kansas City, Missouri, USA.

It is a part of the University of Missouri System, **No date**

“The Right of Privacy” Online: “<http://law2.umkc.edu/faculty/projects/trials/conlaw/rightofprivacy.html>”

The U. S. Constitution contains no express right to privacy. The Bill of Rights, however, reflects the concern of James Madison and other framers for protecting specific aspects of privacy, such as the privacy of beliefs (1st Amendment), privacy of the home against demands that it be used to house soldiers (3rd Amendment), privacy of the person and possessions as against unreasonable searches (4th Amendment), and the 5th Amendment’s privilege against self-incrimination, which provides protection for the privacy of personal information. In addition, the Ninth Amendment states that the “enumeration of certain rights” in the Bill of Rights “shall not be construed to deny or disparage other rights retained by the people.” The meaning of the Ninth Amendment is elusive, but some persons (including Justice Goldberg in his *Griswold* concurrence) have interpreted the

Ninth Amendment as justification for broadly reading the Bill of Rights to protect privacy in ways not specifically provided in the first eight amendments.

Government has a moral obligation to follow the constitution — key to create fair, democratic, and moral laws.

Waldron 14 — Jeremy Waldron, professor of law and philosophy. He holds a professorship at the New York University School of Law and was formerly the Chichele Professor of Social and Political Theory at All Souls College, Oxford University. Waldron also holds an adjunct professorship at Victoria University of Wellington, studied at the University of Otago, New Zealand, where he graduated with a B.A. in 1974 and an LL.B. in 1978. Ph.D. at the University of Oxford, 2014 (“BOOK REVIEW: NEVER MIND THE CONSTITUTION: On Constitutional Disobedience,” *Harvard Law Review*, February, Available online to subscribing institutions via Lexis Nexis, Accessed on 7/14/15)

Instead, Seidman insists on saying that the existence of the Constitution is the problem and that, considering how things are done in other countries, we would be (or we would have been) better off without it. And that is not a satisfactory position. For the fact is that all modern countries, certainly all modern democracies, have written constitutional law in one form or another. In all of them, the people seem to have authority to establish and vary their systems of good government on the basis of reflection and choice; in the words of The Federalist, none of them seem “destined to depend for their political constitutions on accident and force.” Everywhere political systems are framed and defined by written constitutional law. And we consider it an important part of the rule of law that politicians and citizens take these provisions seriously and that, until they are repealed or amended, they have an obligation to modify their behavior accordingly.

Can it possibly be that Seidman thinks that this practice in itself is systematically a bad thing? Consider the spate of recent constitution-making. Over the past thirty or forty years, a number of new democracies have come into existence and, as far as I know, all of them have embarked on the task of defining their political system with a body of written law, often codified in a document called "the Constitution" of South Africa, or Poland, or East Timor, or wherever. Now [*1169] the arrangements they have made are more or less flexible, easier or more difficult to amend. But while they last, their provisions define the parameters of political activity in the country concerned. Moreover, they seldom consist of truisms and tautologies. Constitutional provisions are usually controversial; they could be imagined to be different, and they often attract proposals for emendation. These proposals are sometimes put forward in good faith by people who have no interest other than the abstract improvement of the constitution itself. But often they are put forward for strategic reasons or because the content of the constitutional provision in question is more or less congenial to the ideology of one of the parties or factions whose conflict and competition define the politics of the country. This means that, at any given time, obedience to a given constitutional requirement may seem inappropriate to one or more of those factions or parties. Someone formally obligated by such a requirement may therefore have to ask himself the question that Seidman repeatedly asks:

Why should I do this thing that I think is inappropriate for me (or anyone in my position) to do - which is, after all, why I think this provision should be changed - just because it is required by this piece of paper?

The answer is bound to be: because the constitution cannot do any of the work it is supposed to do in framing and defining a political system unless people are prepared to accept it, for the time being, as authoritative. The work that it has to do is to make politics possible among a people who disagree, often quite radically, about values, principles, rights, justice, and the common good. Even in the midst of their disagreements they need rules that can define a politics - a system of decisions and systems of debate and deliberation that can house the various parties and factions in their confrontations with one another. It seems to me that unless Seidman wishes to say that this work, done by constitutional arrangements, is unnecessary or unimportant, he cannot make a wholesale case against constitutional obedience.

The logic, I think, is irrefutable. Politics needs framing: there needs to be a defined political system, so at any given time there are rules constituting and regulating political interactions, rules that are accepted even by people whose political positions lead them to disagree with the content of the rules. In that sense the rules must have constitutional authority.

Surveillance Internal

Indiscriminate Mass Surveillance erodes privacy rights and violates the constitution

Sinha, 2014

G. Alex Sinha is an Aryeh Neier fellow with the US Program at Human Rights Watch and the Human Rights Program at the American Civil Liberties Union, July 2014 “With Liberty to Monitor All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy” Human Rights Watch, <http://www.hrw.org/node/127364>

The United States government today is implementing a wide variety of surveillance programs that, thanks to developments in its technological capacity, allow it to scoop up personal information and the content of personal communications on an unprecedented scale. Media reports based on revelations by former National Security Agency (NSA) contractor Edward Snowden have recently shed light on many of these programs. They have revealed, for example, that the US collects vast quantities of information—known as “metadata”—about phone calls made to, from, and within the US. It also routinely collects the content of international chats, emails, and voice calls. It has engaged in the large-scale collection of massive amounts of cell phone location data. Reports have also revealed a since-discontinued effort to track internet usage and email patterns in the US; the comprehensive interception of all of phone calls made within, into, and out of Afghanistan and the Bahamas; the daily collection of millions of images so the NSA can run facial recognition programs; the acquisition of hundreds of millions of email and chat contact lists around the world; and the NSA’s deliberate weakening of global encryption standards. In response to public concern over the programs’ intrusion on the privacy of millions of people in the US and around the world, the US government has at times acknowledged the need for reform. However, it has taken few meaningful steps in that direction.

On the contrary, the US—particularly the intelligence community—has forcefully defended the surveillance programs as essential to protecting US national security. In a world of constantly shifting global threats, officials argue that the US simply cannot know in advance which global communications may be relevant to its intelligence activities, and that as a result, it needs the authority to collect and monitor a broad swath of communications. In our interviews with them, US officials argued that the programs are effective, plugging operational gaps that used to exist, and providing the US with valuable intelligence. They also insisted the programs are lawful and subject to rigorous and multi-layered oversight, as well as rules about how the information obtained through them is used. The government has emphasized that it does not use the information gleaned from these programs for illegitimate purposes, such as persecuting political opponents.

The questions raised by surveillance are complex. The government has an obligation to protect national security, and in some cases, it is legitimate for government to restrict certain rights to that end. At the same time, international human rights and constitutional law set limits on the state’s authority to engage in activities like surveillance, which have the potential to undermine so many other rights. The current, large-scale, often indiscriminate US approach to surveillance carries enormous costs. It erodes global digital privacy and sets a terrible example for other countries like India, Pakistan, Ethiopia, and others that are in the process of expanding their surveillance capabilities. It also damages US credibility in advocating internationally for internet freedom, which the US has listed as an important foreign policy objective since at least 2010. As this report documents, US surveillance programs are also doing damage to some of the values the United States claims to hold most dear. These include freedoms of expression and association, press freedom, and the right to counsel, which are all protected by both international human rights law and the US Constitution.

And, these privacy violations are more dangerous than any risk of terrorism, which is magnified by the fact that surveillance fails to prevent attacks.

Schneier, 2014

Bruce Schneier a fellow at the Berkman Center for Internet and Society at Harvard Law School, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the CTO at Resilient Systems, Inc., 1-6-2014, "Essays: How the NSA Threatens National Security," Schneier On Security,
https://www.schneier.com/essays/archives/2014/01/how_the_nsa_threaten.html

We have no evidence that any of this surveillance makes us safer. NSA Director General Keith Alexander responded to these stories in June by claiming that he disrupted 54 terrorist plots. In October, he revised that number downward to 13, and then to "one or two." At this point, the only "plot" prevented was that of a San Diego man sending \$8,500 to support a Somali militant group. We have been repeatedly told that these surveillance programs would have been able to stop 9/11, yet the NSA didn't detect the Boston bombings— even though one of the two terrorists was on the watch list and the other had a sloppy social media trail. Bulk collection of data and metadata is an ineffective counterterrorism tool. Not only is ubiquitous surveillance ineffective, it is extraordinarily costly. I don't mean just the budgets, which will continue to skyrocket. Or the diplomatic costs, as country after country learns of our surveillance programs against their citizens. I'm also talking about the cost to our society. It breaks so much of what our society has built. It breaks our political systems, as Congress is unable to provide any meaningful oversight and citizens are kept in the dark about what government does. It breaks our legal systems, as laws are ignored or reinterpreted, and people are unable to challenge government actions in court. It breaks our commercial systems, as U.S. computer products and services are no longer trusted worldwide. It breaks our technical systems, as the very protocols of the Internet become untrusted. And it breaks our social systems; the loss of privacy, freedom, and liberty is much more damaging to our society than the occasional act of random violence. And finally, these systems are susceptible to abuse. This is not just a hypothetical problem. Recent history illustrates many episodes where this information was, or would have been, abused: Hoover and his FBI spying, McCarthy, Martin Luther King Jr. and the civil rights movement, anti-war Vietnam protesters, and—more recently—the Occupy movement. Outside the U.S., there are even more extreme examples. Building the surveillance state makes it too easy for people and organizations to slip over the line into abuse.

Rights based Advantage Impact/Framing

The impact is the loss of personal autonomy and agency. Privacy is a gateway right, it enables all of our other freedoms.

PoKempne 2014,

Dinah, General Counsel at Human Rights Watch, “The Right Whose Time Has Come (Again): Privacy in the Age of Surveillance” 1/21/14 <http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance>

Technology has invaded the sacred precincts of private life, and unwarranted exposure has imperiled our security, dignity, and most basic values. The law must rise to the occasion and protect our rights. Does this sound familiar? So argued Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article announcing “The Right to Privacy.” We are again at such a juncture. The technological developments they saw as menacing—photography and the rise of the mass circulation press—appear rather quaint to us now. But the harms to emotional, psychological, and even physical security from unwanted exposure seem just as vivid in our digital age. Our renewed sense of vulnerability comes as almost all aspects of daily social life migrate online. At the same time, corporations and governments have acquired frightening abilities to amass and search these endless digital records, giving them the power to “know” us in extraordinary detail. In a world where we share our lives on social media and trade immense amounts of personal information for the ease and convenience of online living, some have questioned whether privacy is a relevant concept. It is not just relevant, but crucial. Indeed, privacy is a gateway right that affects our ability to exercise almost every other right, not least our freedom to speak and associate with those we choose, make political choices, practice our religious beliefs, seek medical help, access education, figure out whom we love, and create our family life. It is nothing less than the shelter in which we work out what we think and who we are; a fulcrum of our autonomy as individuals. The importance of privacy, a right we often take for granted, was thrown into sharp relief in 2013 by the steady stream of revelations from United States government files released by former National Security Agency (NSA) contractor Edward Snowden, and published in the Guardian and other major newspapers around the world. These revelations, supported by highly classified documents, showed the US, the UK, and other governments engaged in global indiscriminate data interception, largely unchecked by any meaningful legal constraint or oversight, without regard for the rights of millions of people who were not suspected of wrongdoing.

The impact is Totalitarianism, the loss of autonomy due to surveillance enables “turnkey totalitarianism,” destroying democracy.

Haggerty, 2015

Kevin D. Professor of Criminology and Sociology at the University of Alberta, “What’s Wrong with Privacy Protections?” in A World Without Privacy: What Law Can and Should Do? Edited by Austin Sarat p. 230

Still others will say I am being alarmist. My emphasis on the threat of authoritarian forms of rule inherent in populations open to detailed institutional scrutiny will be portrayed as overblown and over dramatic, suggesting I veer towards the lunatic fringe of unhinged conspiracy theorists.⁶⁶ But one does not have to believe secret forces are operating behind the scenes to recognize that our declining private realm presents alarming dangers. Someone as conservative and deeply embedded in the security establishment as William Binney – a former NSA senior executive – says the security surveillance infrastructure he helped build now puts us on the verge of “turnkey totalitarianism.”⁶⁷ The contemporary expansion of surveillance, where monitoring becomes an ever-more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger of this situation is how our existing surveillance practices can be turned to oppressive uses. From this point forward our expanding surveillance infrastructure stands as a resource to be inherited by future generations of politicians, corporate actors, or even messianic leaders. Given sufficient political will this surveillance infrastructure can be re-purposed to monitor – in unparalleled detail – people who some might see as undesirable due to their political opinions, religion, skin color, gender, birthplace, physical abilities, medical history, or any number of an almost limitless list of factors used to pit people against one another. The twentieth century provides notorious examples of such repressive uses of surveillance. Crucially, those tyrannical states exercised fine-grained political control by relying on surveillance infrastructures that today seem laughably rudimentary, comprised as they were of paper files, index cards, and elementary telephone tapping.⁶⁸ It is no more alarmist to acknowledge such risks are germane to our own societies than it is to recognize the future will see wars, terrorist attacks, or environmental disasters – events that could themselves prompt surveillance structures to be re-calibrated towards more coercive ends. Those who think this massive surveillance infrastructure will not, in the fullness of time, be turned to repressive purposes are either innocent as to the realities of power, or whistling past a graveyard. But one does not have to dwell on the most extreme possibilities to be unnerved by how enhanced surveillance capabilities invest tremendous powers in organizations. Surveillance capacity gives organizations unprecedented abilities to manipulate human behaviors, desires, and subjectivities towards organizational ends – ends that are too often focused on profit, personal aggrandizement, and institutional self-interest rather than human betterment.

Freedom and dignity are ethically prior to security.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed. This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's

private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

FISA Probable Cause Requirements Fail

FISA probable cause standards do not require proof of a crime to search, only that one “may occur,” and courts will defer to the government in individual instances of determining whether or not probable cause is required

Gregory Birkenstock, 2002, Georgetown Law Journal, Gregory J.D., Georgetown University Law Center, 1992; B.S., Mount St. Mary's College, The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis, p. 843-4

There has always been a tension in the United States between the requirements for a democratic government, including openness and protection of individual freedom, and the need for governmental effectiveness, requiring occasional intrusions into individual freedom. The balance between these competing interests is not easy to strike, and all too often the rights of citizens have been neglected in the pursuit of national security. Electronic wiretapping, which law enforcement and national security agencies have practiced for almost as long as there have been wires to tap, is one area where the pursuit of national security has sometimes involved violations of the rights of individuals to be free from excessive governmental intrusions. Only within the past twenty-five years have courts been willing to apply Fourth Amendment protection to wiretapping at all, and even so the courts have generally excepted foreign intelligence wiretaps from the Warrant Clause requirements. Accordingly, the executive branch has long been unrestrained in gathering foreign intelligence information. Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978 to regulate the executive's previously unchecked discretion in conducting electronic surveillance to gather foreign intelligence information. The Act is essentially a compromise, protecting United States citizens from arbitrary invasions of privacy while granting the executive sufficient latitude to conduct foreign intelligence surveillance. The balance struck is unique because it limits the executive's authority to conduct foreign intelligence surveillance even though the Supreme Court has never addressed Fourth Amendment proscriptions in this area. Although generally regarded as an improvement from the days when executive discretion was essentially unlimited, the act is troubling in some respects. Specifically, there has been concern that FISA's probable cause standard fails to satisfy the Fourth Amendment. Unlike the probable cause standard for criminal warrants, FISA does not require any showing of criminal activity on the part of the target, unless the wiretap will intercept the communications of a "United States person." In that case, FISA still provides a low standard of probable cause, requiring only that the target be involved in activity which "may involve" a criminal violation. Several courts have held that surveillance authorized by FISA does not violate the Fourth Amendment. What is troubling is not that result, but the reasoning leading to it. Prior to the enactment of FISA, courts confronted with national security issues frequently evaded consideration of the difficult balance between freedom and security, deferring to the "unparalleled expertise" of the executive in areas of intelligence-gathering, noting that "the courts are unschooled in diplomacy and military affairs, a mastery of which would be essential to passing upon an executive branch request that a foreign intelligence wiretap be authorized." Accordingly, several courts have adopted a foreign intelligence exception to the Fourth Amendment's Warrant Clause.

Law enforcement can justify any surveillance action under the probable cause doctrine

Andrew Taslitz, 2013, Professor of Law, Washington College of Law, Journal of Criminal Law & Criminology, Cybersurveillance Without Restraint? The Meaning And Social Value Of The Probable Cause And Reasonable Suspicion Standards In Governmental Access To Third-Party Electronic Records,
<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7458&context=jclc>,
DOI: 7-29-15, p. 843-5

One member of the drafting committee, Professor Paul Ohm, has published an article rejecting Slobogin's premise that levels of justification matter and have practical significance in the area of electronic evidence in criminal cases. n18 Ohm argues that it is so easy to establish probable cause in most criminal investigations involving e-mail or the Internet that law enforcement objections have not been justified. Ohm argues, therefore, that there is no need for a sliding scale because probable cause will usually exist and that it alone provides too little protection in an electronic age. Although Ohm's view undercuts much of law enforcement's standard antijustification (whether probable cause or reasonable suspicion) position, Ohm does not clearly argue for increasing (or decreasing) the standard for probable cause, redefining it, or replacing it. Instead, he merely suggests at several points that probable cause in this area is so easy to prove and of so little value in restraining government and protecting privacy that law reform efforts should shift to other areas. Probable cause and reasonable suspicion can usually simply be ignored. But Ohm concedes that there are still instances - though he believes relatively few ones - in which Internet and e-mail investigations will be amenable to regulation by standards of justification like probable cause and reasonable suspicion. Whether these instances will in fact be as rare as Ohm argues is subject to dispute. Furthermore, the Standards themselves address some important situations, such as obtaining medical information or acting where First Amendment free speech concerns may be implicated, that merit high levels of protection even if they occur infrequently. Moreover, Ohm focuses on cybercrime investigations rather than investigations of ordinary crimes (e.g., murder, rape, robbery) that may nevertheless leave a digital trail - but he does not limit his claims to cybercrimes. Yet the latter sort of evidence should become increasingly important as technology advances. He simply underemphasizes the different issues ordinary crimes raise. But ordinary crimes leaving digital trails are often far less likely than cybercrimes to leave themselves open to easy proof of probable cause or even reasonable suspicion. Perhaps most importantly, however, Ohm does not explore in a more theoretical way the meaning and social value of the two main standards of justification - probable cause and reasonable suspicion. I agree with Ohm that many protections are required other than standards of justification. But standards of justification can still serve important social goals, even in Internet investigations, that should not be slighted. Moreover, the two major justification standard terms ("probable cause" and "reasonable suspicion") are rarely defined with any specificity. Part of the ease of meeting them may be the ambiguity in definition and the signals that these definitions send that they do not place much of a proof burden on law enforcement.

Many probable cause/warrant requirement exemptions under FISA, the plan doesn't change any of those

Gregory Birkenstock, 2002, Georgetown Law Journal, Gregory J.D., Georgetown University Law Center, 1992; B.S., Mount St. Mary's College, The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis, p. 849-50

FISA is a complex statute that reflects a multitude of compromises. The substantive provisions of FISA describe the procedural requirements for obtaining approval from the judiciary or the Attorney General to conduct "electronic surveillance." **Because of the statute's complex web of definitions, the application of those procedures will vary widely depending on the circumstances.** For example, **the Attorney General may authorize immediate surveillance in times of emergency.** **The Act authorizes the conducting of electronic surveillance without a warrant when the Attorney General certifies in writing and under oath** that (among other conditions) **the government will comply in statutory "minimization procedures," and that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a "United States person" is a party.**

Probable cause standards are vague [and individual suspicion is not required under FISA]

Gregory Birkenstock, 2002, Georgetown Law Journal, Gregory J.D., Georgetown University Law Center, 1992; B.S., Mount St. Mary's College, The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis, p. 853

FISA allows judges to issue search orders on the basis of information that would not constitute probable cause in the traditional criminal context. This makes the constitutional validity of the FISA search order doubtful in light of the Fourth Amendment's requirement that "no warrant shall issue, but upon probable cause." **Although there is general agreement that the Fourth Amendment was intended to prevent the sorts of abuses that had been common under British rule prior to the Revolution, the lines drawn by the Amendment are not clear.** **The Supreme Court has had great difficulty evaluating the precise meaning of the safeguards that the Fourth Amendment imposes on the government's ability to conduct searches, and its interpretation of those limits continues to evolve.** **Probable cause for a criminal search warrant exists only where "the facts and circumstances within [law enforcement officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed."** Unlike the criminal standard, **FISA does not require individualized suspicion of criminal activity.** The application for the search order merely must provide probable cause that the target is a foreign power, or an agent of a foreign power, and that the place to be searched is being used or will be used by that individual. **Thus, in many cases a FISA search order will issue without probable cause that a crime has been or will be committed.** If, however, the target of the search is a United States person, the Act does provide some apparent protection. In this case, FISA uses a quasi-criminal standard of probable cause, requiring the government to show probable cause that the target is engaging in activity which "may involve" a criminal violation. FISA also requires a demonstration that a United States person is knowingly engaged in or aiding a foreign power in intelligence or terrorist activities. Still, there need not be a current or imminent violation if there is probable cause that criminal acts *may* be committed. FISA orders are merely procedures that regulate the foreign intelligence exception to the Warrant Clause, and are not the substantive analogue of a warrant. **Congress intended the FISA probable cause standard to be less stringent than the criminal**

probable cause standard. **Courts have therefore interpreted the FISA standard loosely, often basing their holdings on Supreme Court statements that probable cause is not a static concept,** and referring to the more flexible approach the Court has recently taken to the Fourth Amendment. Courts have upheld the FISA probable cause definition as appropriate in the unique intelligence-gathering context. Still, **the lower standard of probable cause is troubling,** and poses difficult constitutional questions.

Vagueness makes it unenforceable -- courts will just defer to the government

Erica Goldberg, 2013, law professor, Penn State Dickinson School of Law, Lewis & Clark Law Review, Getting Beyond Intuition in the Probable Cause Inquiry,"

http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1033&context=fac_works, p. 789

Courts are proudly resigned to the fact that the probable cause inquiry is "nontechnical." In order to conduct a search or make an arrest, police need to satisfy **the probable cause standard,** which **the Supreme Court has deemed "incapable of precise definition** or quantification into percentages." **The flexibility of this elusive standard enables courts to defer to** police officers' **reasonable judgments and expert intuitions in unique situations.** **However, police officers are increasingly using investigative techniques that replace their own observational skills with test results from** some other source, such as drug sniffing dogs, **facial recognition technology, and DNA matching.** The reliability of such practices can and should be quantified, but **the vagueness of the probable cause standard renders it impossible for judges to determine which error rates are inconsistent with probable cause.**

Police lie on warrant affidavits

Erica Goldberg, 2013, law professor, Penn State Dickinson School of Law, Lewis & Clark Law Review, Getting Beyond Intuition in the Probable Cause Inquiry,"

http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1033&context=fac_works,

Although many scholars assume that most police officers would not abuse their power to establish probable cause, empirical evidence indicates a serious problem with perjury in warrant affidavits. See Stephen W. Gard, Bearing False Witness: Perjured Affidavits and the Fourth Amendment, *41 Suffolk U. L. Rev.* 445, 447-48 (2008). Clarifying the probable cause standard or applying a more stringent standard of review would not solve the problem of perjury, but it would impede police attempts to establish probable cause where none exists, which police might prefer to outright lying.

Protections don't apply to information obtained from third parties

Andrew Taslitz, 2013, Professor of Law, Washington College of Law, Journal of Criminal Law & Criminology, Cybersurveillance Without Restraint? The Meaning And Social Value Of The Probable Cause And Reasonable Suspicion Standards In Governmental Access To Third-Party Electronic Records,

<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7458&context=jclc>, DOA: 7-29-15, p. 849-50

Yet constitutional controls on the state are nonexistent when the state seeks private information held in the hands of third parties. As noted earlier, this is so because of the "third-party doctrine," holding that the Fourth Amendment's protection against unreasonable searches and seizures does not apply to information in the control of third parties. Although the Court has occasionally suggested limiting this doctrine,⁴ the doctrine is still a vibrant one. Yet, "[one] would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders." Disclosure is thus not truly "consensual" in any common understanding of that word. Third parties consequently hold records of our medical history, psychological condition, physical location, financial transactions, library visits, bookstore purchases, political activities, gifts, and media preferences. When the state seeks access to this mother lode of personal information, the Constitution is largely silent.

Courts allow probable cause to be shown after the fact

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, *37 Sw. U. L. Rev. 1091, 1124-31*, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15

Likewise, many courts rely increasingly on "constructive probable cause," finding probable cause in hindsight from combining the knowledge of several officers, none of whom individually had reasonable suspicion. Courts construct probable cause even absent case-specific proof that officers ever exchanged the information.⁵⁷ Similarly, the Court has recently found individualized probable cause based largely on guilt by association, while insisting it was doing no such thing.⁵⁸

Ext – Justify Any Surveillance Action

Police can always demonstrate probable cause for Internet surveillance

Andrew Taslitz, 2013, Professor of Law, Washington College of Law, Journal of Criminal Law & Criminology, Cybersurveillance Without Restraint? The Meaning And Social Value Of The Probable Cause And Reasonable Suspicion Standards In Governmental Access To Third-Party Electronic Records,
<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7458&context=jclc>,
DOA: 7-29-15, p. 896

Paul Ohm, in his article arguing that probable cause almost always exists in crimes involving the Internet, relies primarily on one subcategory, what I have here labeled "cybercrimes" - crimes committed via the Internet. n323 For many such crimes, he is right. For example, if a computer is used to hack another computer or fraud or threats are sent by e-mail, the combination of log files and Internet addresses usually readily traces to an IP address handled by an ISP. That creates probable cause to believe that the provider has information tying the threat or lie to a specific customer's computer. More investigation may be needed to link a specific person to the communication made using that computer at the relevant time. But probable cause to seek records from the ISP is established.

Ext – Vagueness Means Can't Define

Can't define probable cause, courts defer

Erica Goldberg, 2013, law professor, Penn State Dickinson School of Law, Lewis & Clark Law Review, Getting Beyond Intuition in the Probable Cause Inquiry,"
http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1033&context=fac_works, p. 790

Courts are proudly resigned to the fact that the probable cause inquiry is "nontechnical." To conduct a search or make an arrest, a police officer must establish probable cause based on the totality of the circumstances. This approach allows for great flexibility in the application of facts to the standard. Adding uncertainty to this flexibility, the actual legal standard of probable cause remains undefined. The Supreme Court has deemed probable cause "incapable of precise definition or quantification into percentages" and, just this year, overturned the Florida Supreme Court's efforts to add a more rigorous framework to the inquiry. Judges, prosecutors, and scholars display varying understandings as to the degree of suspicion that probable cause requires. n4 The deferential standard that reviewing courts apply to probable cause determinations further exacerbates the confusion. "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." The probable cause standard is so significant because it serves as the gatekeeper between individuals and these unwarranted intrusions. Yet, the standard has not been defined with sufficient precision. An examination of the role that probable cause plays in regulating governmental intrusions of various types is first necessary to understand why probable cause requires flexibility in applying the facts but greater precision in defining the legal standard. The standard's elusiveness is exacerbated by relatively recent decisions diminishing judicial review of probable cause determinations. Quantifying the standard is now a more urgently needed solution. Although the Supreme Court has held that the probable cause standard is incapable of quantification, courts already incorporate quantifiable evidence into the inquiry; they are just not doing so in a standardized way.

Courts defer in probable cause determinations

Erica Goldberg, 2013, law professor, Penn State Dickinson School of Law, Lewis & Clark Law Review, Getting Beyond Intuition in the Probable Cause Inquiry,"
http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1033&context=fac_works,

See *United States v. Allen*, 625 F.3d 830, 840 (5th Cir. 2010) ("A magistrate's determination of probable cause is entitled to great deference by reviewing courts.").

Vagueness of "probable cause" makes it meaningless

Andrew Taslitz,2013,Professor of Law, Washington College of Law, Journal of Criminal Law & Criminology, Cybersurveillance Without Restraint? The Meaning And Social Value Of The Probable Cause And Reasonable Suspicion Standards In Governmental Access To Third-Party Electronic Records,
<http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7458&context=jclc>,
DOA: 7-29-15, p. 856

There are, therefore, good reasons to guide important decisions implicating state power by establishing a specific standard of proof. **Probable cause** and reasonable suspicion authorize the state to use force against its citizens and thus likewise should require the articulation of an appropriate correlative standard of proof. **Yet the United States Supreme Court has never announced one**, much less two (in theory, one standard could govern probable cause, another reasonable suspicion). **The Court has repeatedly said that probable cause cannot be quantified**, and it has implied the same to be true of reasonable suspicion. In defining these terms - and it always does so vaguely - not once has it recited the relevant respective standard of proof. Indeed, **the outcomes of the Court's decisions suggest that the standard, if there is one, is elusive and ever-shifting, thus being no standard at all.**

Privacy Key To Dignity

Mass surveillance denies basic dignity. Privacy is necessary for individuals to be themselves.

Schneier 6 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, 2006 ("The Eternal Value of Privacy," *Wired*, May 18th, Available Online at <http://www.wired.com/news/columns/0,70886-0.html>, Accessed 05-22-2006)

The most common retort against privacy advocates -- by those in favor of ID checks, cameras, databases, data mining and other wholesale surveillance measures -- is this line: "If you aren't doing anything wrong, what do you have to hide?"

Some clever answers: "If I'm not doing anything wrong, then you have no cause to watch me." "Because the government gets to define what's wrong, and they keep changing the definition." "Because you might do something wrong with my information." My problem with quips like these -- as right as they are -- is that they accept the premise that privacy is about hiding a wrong. It's not. **Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect.**

Two proverbs say it best: *Quis custodiet custodes ipsos?* ("Who watches the watchers?") and "Absolute power corrupts absolutely."

Cardinal Richelieu understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged." Watch someone long enough, and you'll find something to arrest -- or just blackmail -- with. **Privacy is important because without it, surveillance information will be abused:** to peep, to sell to marketers and to spy on political enemies -- whoever they happen to be at the time.

Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.

We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need.

A future in which privacy would face constant assault was so alien to the framers of the Constitution that it never occurred to them to call out privacy as an explicit right. Privacy was inherent to the nobility of their being and their cause. Of course being watched in your own home was unreasonable. Watching at all was an act so unseemly as to be inconceivable among gentlemen in their day. You watched convicted criminals, not free citizens. You ruled your own home. **It's intrinsic to the concept of liberty.**

For **if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness.** We become children, fettered under watchful eyes, constantly fearful that – either now or in the uncertain future – patterns we leave

behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. **We lose our individuality, because everything we do is observable and recordable.**

How many of us have paused during conversation in the past four-and-a-half years, suddenly aware that we might be eavesdropped on? Probably it was a phone conversation, although maybe it was an e-mail or instant-message exchange or a conversation in a public place. Maybe the topic was terrorism, or politics, or Islam. We stop suddenly, momentarily afraid that our words might be taken out of context, then we laugh at our paranoia and go on. But our demeanor has changed, and our words are subtly altered.

This is the loss of freedom we face when our privacy is taken from us. **This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives.**

Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is **the very definition of a police state.** And that's why we should champion privacy even when we have nothing to hide.

This is the most important impact. Respect for dignity is a baseline requirement of ethical conduct.

Kaczor 12 — Christopher Kaczor, Professor of Philosophy at Loyola Marymount University, holds a Ph.D. in Philosophy from the University of Notre Dame, 2012 (“The Importance of Dignity: A Reply to Steven Pinker,” *Public Discourse*—a publication of The Witherspoon Institute, January 31st, Available Online at <http://www.thepublicdiscourse.com/2012/01/4540/>, Accessed 06-17-2015)

Even if we can successfully disambiguate the term, why is dignity important? The concept of dignity does a better job than autonomy in describing and accounting for the intrinsic value of every human being. **We are valuable not simply because of our choices, and still less do we have value only while we are exercising our autonomy.** We have value even when we are not choosing or cannot choose. In his 2009 Tanner Lectures at UC Berkeley, “Dignity, Rank, and Rights,” Jeremy Waldron pointed out that in ancient times dignity was accorded in particular to persons regarded as royalty or nobility. Noble persons were accorded rights, privileges, and immunities that accorded with their elevated rank. Contemporary society at its best does not reduce the noble but elevates the commoner, making every single human person equal in rank to the Duke or Lady. Although these ideals are often imperfectly realized in our society, still Waldron has a point when he writes, “we are not like a society which has eschewed all talk of caste; we are like a caste society with just one caste (and a very high caste at that): every man a Brahmin. Every man a duke, every woman a queen, everyone entitled to the sort of deference and consideration, everyone’s person and body sacrosanct, in the way that nobles were entitled to deference or in the way that an assault upon the body or the person of a king was regarded as a sacrilege.” The term dignity better captures than most, if not all, other terms the elevated status of the human person.

Do we have any reason for ascribing to all human beings such intrinsic dignity? In an earlier essay, I suggested that there are a number of ways to argue for the proposition that all human beings are endowed with intrinsic dignity and certain inalienable rights. The first is that our dignity should be based on who we are, the kind of being that we are, rather than on how we are functioning in the moment. Dignity should be based on our membership in the human family, rather than on any particular performative activity in which we could engage. Our functioning, whether it be understood in terms of our ability to experience pleasure and pain, or our consciousness, or our intelligence, comes in many degrees. If we think that our value as persons is based on a degreed characteristic, an accident in terms of Aristotelian metaphysics, then we cannot secure equal basic dignity and equal basic rights for all persons. We should therefore base our fundamental ethical judgments on the substantial identity of who we are rather than on any accidental degreed quality. Since all human beings are endowed with the same nature, members of the same kind—*homo sapiens*—they all share equally basic rights and dignity.

Privacy Key To Identity Formation

The breathing room provided by privacy is an end in itself. We can't be "ourselves" without it.

Sadowski 13 — Jathan Sadowski, Doctoral Candidate in Human and Social Dimensions of Science and Technology in the Consortium for Science, Policy and Outcomes at Arizona State University, holds an M.A. in Applied Ethics and the Professions from Arizona State University and a B.S. in Philosophy from the Rochester Institute of Technology, 2013 ("Why Does Privacy Matter? One Scholar's Answer," *The Atlantic*, February 26th, Available Online at <http://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/>, Accessed 04-16-2015)

Even though the practices of many companies such as Facebook are legal, there is something disconcerting about them. Privacy should have a deeper purpose than the one ascribed to it by those who treat it as a currency to be traded for innovation, which in many circumstances seems to actually mean corporate interests. To protect our privacy, we need a better understanding of its purpose and why it is valuable.

That's where Georgetown University law professor Julie E. Cohen comes in. In a forthcoming article for the Harvard Law Review, she lays out a strong argument that addresses the titular concern "What Privacy Is For." Her approach is fresh, and as technology critic Evgeny Morozov rightly tweeted, she wrote "the best paper on privacy theory you'll get to read this year." (He was referring to 2012.)

At bottom, Cohen's argument criticizes the dominant position held by theorists and legislators who treat privacy as just an instrument used to advance some other principle or value, such as liberty, inaccessibility, or control. Framed this way, privacy is relegated to one of many defenses we have from things like another person's prying eyes, or Facebook's recent attempts to ramp up its use of facial-recognition software and collect further data about us without our explicit consent. As long as the principle in question can be protected through some other method, or if privacy gets in the way of a different desirable goal like innovation, it is no longer useful and can be disregarded.

Cohen doesn't think we should treat privacy as a dispensable instrument. To the contrary, she argues privacy is irreducible to a "fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic. Privacy is shorthand for breathing room to engage in the process of ... self-development."

What Cohen means is that since life and contexts are always changing, privacy cannot be reductively conceived as one specific type of thing. It is better understood as an important buffer that gives us space to develop an identity that is somewhat separate from the surveillance, judgment, and values of our society and culture. Privacy is crucial for helping us manage all of these pressures -- pressures that shape the type of person we are -- and for "creating spaces for play and the work of self-[development]." Cohen argues that this self-development allows us to discover what type of society we want and what we should do to get there, both factors that are key to living a fulfilled life.

Woodrow Hartzog and Evan Selinger make similar arguments in a recent article on the value of "obscurity." When structural constraints prevent unwanted parties from getting to your data,

obscurity protections are in play. These protections go beyond preventing companies from exploiting our information for their financial gain. They safeguard democratic societies by furthering "autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power."

In light of these considerations, what's really at stake in a feature like Facebook's rumored location-tracking app? You might think it is a good idea to willfully hand over your data in exchange for personalized coupons or promotions, or to broadcast your location to friends. But consumption -- perusing a store and buying stuff -- and quiet, alone time are both important parts of how we define ourselves. If how we do that becomes subject to ever-present monitoring it can, if even unconsciously, change our behaviors and self-perception.

In this sense, we will be developing an identity that is absent of privacy and subject to surveillance; we must decide if we really want to live in a society that treats every action as a data point to be analyzed and traded like currency. The more we allow for constant tracking, the more difficult it becomes to change the way that technologies are used to encroach on our lives.

Privacy is not just something we enjoy. It is something that is necessary for us to: develop who we are; form an identity that is not dictated by the social conditions that directly or indirectly influence our thinking, decisions, and behaviors; and decide what type of society we want to live in. Whether we like it or not constant data collection about everything we do -- like the kind conducted by Facebook and an increasing number of other companies -- shapes and produces our actions. We are different people when under surveillance than we are when enjoying some privacy. And Cohen's argument illuminates how the breathing room provided by privacy is essential to being a complete, fulfilled person.

Privacy provides an “interior zone” that’s necessary for full and free personal development.

Brooks 15 — David Brooks, Columnist for the *New York Times*, Commentator for PBS *NewsHour*, holds an A.B. in History from the University of Chicago, 2015 (“The Lost Language of Privacy,” *New York Times*, April 14th, Available Online at <http://www.nytimes.com/2015/04/14/opinion/david-brooks-the-lost-language-of-privacy.html>, Accessed 05-15-2015)

Privacy is important to the development of full individuals because there has to be an interior zone within each person that other people don't see. There has to be a zone where half-formed thoughts and delicate emotions can grow and evolve, without being exposed to the harsh glare of public judgment. There has to be a place where you can be free to develop ideas and convictions away from the pressure to conform. There has to be a spot where you are only yourself and can define yourself.

Privacy is important to families and friendships because there has to be a zone where you can be fully known. There has to be a private space where you can share your doubts and secrets and expose your weaknesses with the expectation that you will still be loved and forgiven and supported.

Privacy is important for communities because there has to be a space where people with common affiliations can develop bonds of affection and trust. There has to be a boundary between us and

them. Within that boundary, you look out for each other; you rally to support each other; you cut each other some slack; you share fierce common loyalties.

All these concentric circles of privacy depend on some level of shrouding. They depend on some level of secrecy and awareness of the distinction between the inner privileged space and the outer exposed space. They depend on the understanding that what happens between us stays between us.

Mass Surveillance Not Needed to Fight Terrorism

Little of the collected data is terrorism related

Rebecca Abrahams, 10-21, 13, "What's Behind the Spying?" CCO, SVP Ziklag Systems, a mobile security technology company, http://www.huffingtonpost.com/rebecca-abrahams/whats-behind-the-spying_b_4136079.html

The NSA "cover story" is that extensive spying is necessary to stop terrorism. But NSA has been hard pressed to demonstrate that its phone and Internet spying has actually helped stop terrorism, and targeting the President of Mexico or key government and industrial leaders in France, Germany and many other countries, is absolutely divorced from having any linkage to terrorism. In fact, the United States has been carrying out political and economic spying. Terrorism probably accounts for only a small portion of what the mighty NSA collection apparatus sweeps up.

Most of the surveillance is for economic espionage, not terror prevention

Li Jingjing, Global Times (China), June 24, 2014

'No Place to Hide'

Although the US government has tried to use the prevention of terrorism as an excuse to justify its programs, based on the documents Snowden revealed, most of the intelligence collected had less to do with anti-terrorism and more to do with economic espionage. No matter if it was Brazilian oil giant Petrobras, Russian gas company Gazprom, Russian airline Aeroflot or the organizations and leaders of other countries, all fell under the purview of this intelligence collection. During a presentation at the TED conference in March, Snowden stated, "Terrorism has always been what we in the intelligence world would call a cover for action. Terrorism is something that provokes an emotional response that allows people to rationalize authorizing powers and programs that they wouldn't give otherwise."

Information didn't prevent the Boston attacks

Bergen, et al, September 2013, Jihadist Terrorism: A Threat Assessment, http://bipartisanpolicy.org/sites/default/files/Jihadist%20Terrorism-A%20Threat%20Assesment_0.pdf

Peter Bergen is the author of four books about al-Qaeda, three of which were *New York Times* best sellers. The books have been translated into 20 languages. He is the director of the National Security Program at the New America Foundation in Washington, D.C.; a fellow at Fordham University's Center on National Security; and CNN's national security analyst. He has held teaching positions at the Kennedy School of Government at Harvard University and at the School of Advanced International Studies at Johns Hopkins University.[¶] Bruce Hoffman is a professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where he is also the director of both the Center for Security Studies and the Security Studies Program. He previously held the corporate chair in counterterrorism and counterinsurgency at the RAND Corporation and was the scholar-in-residence for counterterrorism at the CIA between 2004 and 2006.[¶] Michael Hurley is the president of Team 3i LLC, an international strategy company, and advises the Bipartisan Policy Center's Homeland Security Project. He led the 9/11 Commission's counterterrorism policy investigation, as well as CIA personnel in Afghanistan immediately after the 9/11 attacks. He retired from the CIA following a 25-year career and has served as director on the National Security Council staff.[¶] Erroll Southers is the associate director of research transition at the Department of Homeland Security's National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California, where

he is an adjunct professor in the Sol Price School^[1] of Public Policy. He is a former FBI special agent and was President Barack Obama's nominee for the Transportation Security Administration, as well as Governor Arnold Schwarzenegger's deputy director for the California Office of Homeland Security and the chief of homeland security and intelligence for the LAX Police Department. He is the author of *Homegrown Violent Extremism*.)

A final question is: how were the Tsarnaevs able to^[1] avoid tipping off local and federal intelligence and law enforcement agencies, either through contact with an informant or from tips by the community? Russian officials had flagged Tamerlan Tsarnaev as a potential threat in 2011, though whether the quality of their evidence was sufficient to justify actions other than those taken is unclear.²⁰ The FBI opened an investigation into Tamerlan, but closed it when they found no evidence of criminal or terrorist activity.²¹ Boston's Police Commissioner Edward Davis told the House Homeland Security Committee at the first congressional hearing on the bombings, on May 9, 2013, that the Boston Police Department did not receive information regarding the Russian tip.²² In a statement later that same day, the FBI noted that several Boston police officers were part of the squad that investigated Tamerlan^[1] in 2011, and they also had access to the Joint Terrorism Task Force database that included information on him.²³ The statement also acknowledged, though, that the Boston Joint Terrorism Task Force (JTTF) conducted about 1,000 assessments in 2011, making it impossible for every officer to give each case close attention. The lack of a direct mechanism to share terrorism-related information between law enforcement agencies, along with the sheer amount of data that a JTTF in a major city has to sort through, are two issues that should be addressed in light of these attacks.

CIA uses other means to disrupt terrorists

Washington Post, 10-16, 13, http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story_1.html

The documents do not explain how the Ghul e-mail was obtained or whether it was intercepted using legal authorities that have emerged as a source of controversy in recent months and enable the NSA to compel technology giants including Microsoft and Google to turn over information about their users. Nor is there a reference to another NSA program facing scrutiny after Snowden's leaks, its metadata collection of numbers dialed by nearly every person in the United States. To the contrary, the records indicate that the agency depends heavily on highly targeted network penetrations to gather information that wouldn't otherwise be trapped in surveillance nets that it has set at key Internet gateways.^[1] The new documents are self-congratulatory in tone, drafted to tout the NSA's counterterrorism capabilities. One is titled "CT MAC Hassan Gul Success." The files make no mention of other agencies' roles in a drone program that escalated dramatically in 2009 and 2010 before tapering off in recent years.

NSA surveillance has not stopped 54 terror attacks

Gizmodo, June 2, 2014, <http://gizmodo.com/the-five-dumbest-ways-that-people-defend-nsa-spying-1585242095>

1. The NSA has Stopped 54 Terrorist Attacks with Mass Spying

The discredited claim: NSA defenders have thrown out many claims about how NSA surveillance has protected us from terrorists, including repeatedly declaring that it has thwarted 54 plots. Rep. Mike Rogers says it often. Only weeks after the first Snowden leak, US President Barack Obama claimed: "We know of at least 50 threats that have been averted" because of the NSA's spy powers. Former NSA Director Gen. Keith Alexander also repeatedly claimed that those programs thwarted 54 different attacks.

Others, including former Vice President Dick Cheney have claimed that had the bulk spying programs in place, the government could have stopped the 9/11 bombings, specifically noting that the government needed the program to locate Khalid al Mihdhar, a hijacker who was living in San Diego.

Why it's not credible: These claims have been thoroughly debunked. First, the claim that the information stopped 54 terrorist plots fell completely apart. In dramatic Congressional testimony, Sen. Leahy forced a formal retraction from NSA Director Alexander in October, 2013:

"Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S.?" Leahy said at the hearing. "Would you agree with that, yes or no?"

"Yes," Alexander replied, without elaborating.

But that didn't stop the apologists. We keep hearing the "54 plots" line to this day.

As for 9/11, sadly, the same is true. The government did not need additional mass collection capabilities, like the mass phone records programs, to find al Mihdhar in San Diego. As ProPublica noted, quoting Bob Graham, the former chair of the Senate Intelligence Committee:

U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al Mihdhar, long before 9/11 and had the ability find him, but they failed to do so.

"There were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar," says former Senator Bob Graham, the Florida Democrat who extensively investigated 9/11 as chairman of the Senate's intelligence committee.

Moreover, Peter Bergen and a team at the New America Foundation dug into the government's claims about plots in America, including studying over 225 individuals recruited by al Qaeda and similar groups in the United States and charged with terrorism, and concluded:

Our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading...

When backed into a corner, the government's apologists cite the capture of Zazi, the so-called New York subway bomber. However, in that case, the Associated Press reported that the government could have

easily stopped the plot without the NSA program, under authorities that comply with the Constitution. Sens. Ron Wyden and Mark Udall have been saying this for a long time.

Both of the President's hand-picked advisors on mass surveillance concur about the telephone records collection. The President's Review Board issued a report in which it stated "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks," The Privacy and Civil Liberties Oversight Board (PCLOB) also issued a report in which it stated, "we have not identified a single instance involving a threat to the United States in which [bulk collection under Section 215 of the Patriot Act] made a concrete difference in the outcome of a counterterrorism investigation."

And in an amicus brief in EFF's case First Unitarian Church of Los Angeles v. the NSA case, Sens. Ron Wyden, Mark Udall, and Martin Heinrich stated that, while the administration has claimed that bulk collection is necessary to prevent terrorism, they "have reviewed the bulk-collection program extensively, and none of the claims appears to hold up to scrutiny."

Even former top NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US and at most, helped catch one guy who shipped about \$8,000 to a Somalian group that the US has designated as a terrorist group but that has never even remotely been involved in any attacks aimed at the US.

Evidence that surveillance has prevented terrorism is wrong

Peter Bergen et al, New America Foundation, January 13, 2014, "Do NSA's Bulk Surveillance Programs stop terrorists?"

On June 5, 2013, the Guardian broke the first story in what would become a flood of revelations regarding the extent and nature of the NSA's surveillance programs. Facing an uproar over the threat such programs posed to privacy, the Obama administration scrambled to defend them as legal and essential to U.S. national security and counterterrorism. Two weeks after the first leaks by former NSA contractor Edward Snowden were published, President Obama defended the NSA surveillance programs during a visit to Berlin, saying: "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved." Gen. Keith Alexander, the director of the NSA, testified before Congress that: "the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world." Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that "54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives."

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted

intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.

Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it's unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government's investigations of these cases: <http://natsec.newamerica.net/nsa/analysis>).

Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided \$8,500 to al-Shabaab, al-Qaeda's affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to "connect the dots" faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA's phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it's unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin's calls, despite official statements that the bureau had Moalin's phone number and had identified him. This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues.

Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange.

In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been

initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used.

We have also identified three additional plots that the government has not publicly claimed as NSA successes, but in which court records and public reporting suggest the NSA had a role. However, it is not clear whether any of those three cases involved bulk surveillance programs.

Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

NSA doesn't aid in detection efforts – surveillance has a negligible impact

Benkler 13 -- Yochai Benkler is a law professor and director of the Berkman Center for Internet & Society at Harvard University. "Fact: the NSA gets negligible intel from Americans' metadata. So end collection" <http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence>

Congress may be on the verge of prohibiting the NSA from continuing its bulk telephony metadata collection program. Two weeks ago, the Senate national security dissenters: Wyden, Udall, Paul, and Blumenthal proposed prohibition. Last week, the move received a major boost from a bipartisan proposal by core establishment figures: Senator Patrick Leahy, and Representatives Jim Sensenbrenner and John Conyers. It's a prohibition whose time has come. Dragnet surveillance, or bulk collection, goes to the heart of what is wrong with the turn the NSA has taken since 2001. It implements a perpetual "state of emergency" mentality that inverts the basic model outlined by the fourth amendment: that there are vast domains of private action about which the state should remain ignorant unless it provides clear prior justification. And all public evidence suggests that, from its inception in 2001 to this day, bulk collection has never made more than a marginal contribution to securing Americans from terrorism, despite its costs. In a 2 October hearing of the Senate judiciary committee, Senator Leahy challenged the NSA chief, General Keith Alexander. Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and that of the 54 only 13 had some nexus to the US? Would you agree with that, yes or no? Alexander responded: Yes. Leahy then demanded that Alexander confirm what his deputy, Christopher Inglis, had said in the prior week's testimony: that there is only one example where collection of bulk data is what stopped a terrorist activity. Alexander responded that Inglis might have said two, not one. Advertisement In fact, what Inglis had said the week before was that there was one case "that comes close to a but-for example and that's the case of Basaaly Moalin". So who is Moalin, on whose fate the NSA places the entire burden of justifying its metadata collection program? Did his capture foil a second 9/11? A cabby from San Diego, Moalin had immigrated as a teenager from Somalia. In February, he was convicted of providing material assistance to a terrorist organization: he had transferred \$8,500 to al-Shabaab in Somalia. After the Westgate Mall attack in Nairobi, few would argue that al-Shabaab is not a terrorist organization. But al-Shabaab is involved in a local war, and is not invested in attacking the US homeland. The indictment against Moalin explicitly stated that al-Shabaab's enemies were the present Somali government and "its Ethiopian and African Union supporters". Perhaps, it makes sense for prosecutors to pursue Somali Americans for doing essentially what some Irish Americans did to help the IRA; perhaps not. But this single successful prosecution, under

a vague criminal statute, which stopped a few thousand dollars from reaching one side in a local conflict in the Horn of Africa, is the sole success story for the NSA bulk domestic surveillance program.

At the hearing, perhaps trying to bolster Alexander's feeble defense of the program's effectiveness, Director of National Intelligence James Clapper complained that "plots foiled" should not be the metric. He said: There's another metric I would use; let's call it the "peace of mind metric". In the case of the Boston Marathon bomber, we were able to use these tools to determine whether there was, or was not, a subsequent plot in NYC. Clapper actually used the clearest example that his program offers Americans little real security – its failure to pick up the Tsarnaev brothers before they attacked – as a way of persuading us that we should use an amorphous and unmeasurable "peace of mind" metric; peace of mind we should gain from knowing that the same system that failed to detect the Boston bombers also detected no bombers in New York. One is left picturing Inspector Clouseau: I did not know the bank was being robbed because I was engaged in my sworn duty as a police officer. The admissions Leahy forced out of the NSA heads and DNI Clapper that they have been systematically overstating the effectiveness of bulk collection are consistent with the only other official assessments of bulk collection. The sole publicly available FISC opinion (pdf) that assesses the impact of bulk collection from 2006 to 2009 was unimpressed that: [T]he government's submission cites three examples in which the FBI opened three new preliminary investigations of persons in the US based on tips from the BR metadata program. Judge Walton wrote that this achievement "does not seem particularly significant". Perhaps most damning are the results of the consensus report authored by the five inspectors general of the Departments of Defense and Justice and the CIA, NSA, and Office of DNI, mandated by Congress as part of the Fisa Amendments Act of 2008. That report provides the most detailed official assessment of the effectiveness of bulk collection, from inception as the President's Surveillance Program (PSP) in the fall of 2001 until 2007. It is revealing about both the NSA and its bulk

collection program. The NSA's inspector general only reported the agency's top brass beliefs; his report merely quoted then NSA Director Michael Hayden in his view that there were "no communications more important to NSA efforts to defend the nation". Other inspectors general were more skeptical. The Department of Justice "concluded that although PSP-derived information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts. The CIA reported: [W]orking-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP reporting. Officials also stated that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP. The inspector general of the DNI reported that "National Counterterrorism Center analysts characterized the PSP information as being a useful tool, but noted that the information was only one of several valuable sources of information available to them", and "not of greater value than other sources of intelligence". It is hardly surprising that supporters of bulk collection fervently believe it is critical to national security. No psychologically well-balanced person could permit herself to support a program that compromises the privacy of tens of millions of Americans, costs billions of dollars, and imposes direct and articulable harm to cyber security by undermining the security of commercial products and public standards without holding such a belief truly and honestly. But the honest faith of insiders that their bureaucratic mission is true and critical is no substitute for credible evidence. A dozen years of experience has produced many public overstatements and much hype from insiders, but nothing to support the proposition that the program works at all, much less that its marginal contribution is significant enough to justify its enormous costs in money, freedom, and destabilization of internet security. No rational cost-benefit analysis could justify such a leap of faith. If the NSA cannot show real, measurable evidence of its effectiveness, evidence that doesn't collapse as soon as it is examined and isn't a vague appeal to amorphous, measurement-free "peace of mind", its bulk collection program has to go.

NSA ineffective – info-overload

Puiu 15 – Tibi, ZME Science "The NSA is gathering so much data, it's become swamped and ironically ineffective at preventing terrorism" <http://www.zmescience.com/research/technology/nsa-overwhelmed-data-53354/>

One of the most famous NSA whistleblowers (or the 'original NSA whistleblower'), William Binney, said the agency is collecting stupendous amounts of data – so much that it's actually hampering intelligence operations. Binney worked for three decades for the intelligence agency, but left shortly after the 9/11 attacks. A program he had developed was scrapped and replaced with a system he said was more expensive and more intrusive, which made him feel he worked for an incompetent employer. Plans to enact the now controversial Patriot Act was the last straw, so he quit. Since then, Binney has frequently criticized the agency and revealed some of its operations hazards and weaknesses. Among these, he alleges: The NSA buried key intelligence that could have prevented 9/11; The agency's bulk data collection from internet and telephone communications is unconstitutional and illegal in the US; Electronic intelligence gathering is being used for covert law enforcement, political control and industrial espionage, both in and beyond the US; Edward Snowden's leaks could have been prevented. Ironically, Snowden cites Binney as an inspiration. His greatest insights however is that the NSA is ineffective at preventing terrorism because analysts are too swamped with information under its bulk collection programme. Considering Binney's impeccable track record – he was co-founder and director of the World Geopolitical & Military Analysis at the Signals Intelligence Automation Research Center (SARC), a branch with 6,000 employees – I can only presume he knows what he's talking about. The Patriot Act is a U.S. law passed in the wake of the September 11, 2001 terrorist attacks. Its goals are to strengthen domestic security and broaden the powers of law-enforcement agencies with regards to identifying and stopping terrorists. In effect, the law laxes the restrictions authorities have to search telephone, e-mail

communications, medical, financial, and other records. Because a lot of people use web services whose servers are located in the US, this means that the records of people not located or doing business in the US are also spied upon by the NSA. All this information, however, comes at a price: overload. According to the Guardian, the NSA buffers a whooping 21 petabytes a day! In this flood of information, an NSA analyst will quickly find himself overwhelmed. Queering keywords like "bomb" or "drugs" might prove a nightmare for the analyst in question. It's impossible not to, considering four billion people — around two-thirds of the world's population — are under the NSA and partner agencies' watchful eyes, according to Binney. "That's why they couldn't stop the Boston bombing, or the Paris shootings, because the data was all there," said Binney for ZDnet.

Info isn't used or shared properly

Eddington 15 -- Patrick Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute. He was formerly a senior policy advisor to Rep. Rush Holt (D-N.J.) and a military imagery analyst at the CIA's National Photographic Interpretation Center. "No, Mass

Surveillance Won't Stop Terrorist Attacks" <http://reason.com/archives/2015/01/27/mass-surveillance-and-terrorism#.0wxmih:U8Io>

The recent terrorist attack on the office of French satirical magazine Charlie Hebdo generated a now-familiar meme: Another terrorist attack means we need more surveillance. Sen. Bob Corker (R-Tenn.) said that while "Congress having oversight certainly is important ... what is more important relative to these types of events is ensuring we don't overly hamstring the NSA's ability to collect this kind of information in advance and keep these kinds of activities from occurring." Similarly, Sen. Lindsey Graham (R-S.C.) spoke of his "fear" that "our intelligence capabilities, those designed to prevent such an attack from taking place on our shores, are quickly eroding," adding that the government surveillance "designed to prevent these types of attacks from occurring is under siege." A recent poll demonstrates that their sentiments are widely shared in the wake of the attack. But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the answer: 2009: Umar Farouk Abdulmutallab—i.e., the "underwear bomber"—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community(IC) failed "to connect, integrate, and fully understand the intelligence" it had collected. 2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation. 2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency (NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS. 2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine. No, mass surveillance does not prevent terrorist attacks. It's worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally-dubious ones—were premised on the belief that bin Laden's hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data. Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government's hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination. That malady perfectly describes every intelligence failure from Pearl Harbor to the present day. The Office of the Director of National Intelligence (created by Congress in 2004) was supposed to be the answer to the "failure-to-connect-the-dots" problem. Ten years on, the problem remains, the IC bureaucracy is bigger than ever, and our government is continuing to rely on mass surveillance programs that have failed time and again to stop terrorists while simultaneously undermining the civil liberties and personal privacy of every American. The quest to "collect it all," to borrow a phrase from NSA Director Keith Alexander, only leads to the accumulation of masses of useless information, making it harder to find real threats and costing billions to store. A recent Guardian editorial noted that such mass-surveillance myopia is spreading among European political leaders as well, despite the fact that "terrorists, from 9/11 to the Woolwich jihadists and the neo-Nazi Anders Breivik, have almost always come to the authorities' attention before murdering." Mass surveillance is not only destructive of our liberties, its continued use is a virtual guarantee of more lethal intelligence failures. And our continued will to disbelieve those facts is a mental dodge we engage in at our peril.

Government statements about NSA surveillance preventing attacks have been thoroughly debunked.

Cindy Cohn and Nadia Kayyali, **6/2/2014**. Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel; and member of EFF's activism team. Nadia's work focuses on surveillance, national security policy, and the intersection of criminal justice, racial justice, and digital civil liberties issues. "The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible," Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible>.

Over the past year, as the Snowden revelations have rolled out, the government and its apologists have developed a set of talking points about mass spying that the public has now heard over and over again. From the President, to Hilary Clinton to Rep. Mike Rogers, Sen. Dianne Feinstein and many others, the arguments are often eerily similar.

But as we approach the one year anniversary, it's time to call out the key claims that have been thoroughly debunked and insist that the NSA apologists retire them.

So if you hear any one of these in the future, you can tell yourself straight up: "this person isn't credible," and look elsewhere for current information about the NSA spying. And if these are still in your talking points (you know who you are) it's time to retire them if you want to remain credible. And next time, the talking points should stand the test of time.

1. The NSA has Stopped 54 Terrorist Attacks with Mass Spying

The discredited claim

NSA defenders have thrown out many claims about how NSA surveillance has protected us from terrorists, including repeatedly declaring that it has thwarted 54 plots. Rep. Mike Rogers says it often. Only weeks after the first Snowden leak, US President Barack Obama claimed: "We know of at least 50 threats that have been averted" because of the NSA's spy powers. Former NSA Director Gen. Keith Alexander also repeatedly claimed that those programs thwarted 54 different attacks.

Others, including former Vice President Dick Cheney have claimed that had the bulk spying programs in place, the government could have stopped the 9/11 bombings, specifically noting that the government needed the program to locate Khalid al Mihdhar, a hijacker who was living in San Diego.

Why it's not credible:

These claims have been thoroughly debunked. First, the claim that the information stopped 54 terrorist plots fell completely apart. In dramatic Congressional testimony, Sen. Leahy forced a formal retraction from NSA Director Alexander in October, 2013:

"Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S.?" Leahy said at the hearing. "Would you agree with that, yes or no?"

"Yes," Alexander replied, without elaborating.

But that didn't stop the apologists. We keep hearing the "54 plots" line to this day.

As for 9/11, sadly, the same is true. The government did not need additional mass collection capabilities, like the mass phone records programs, to find al Mihdhar in San Diego. As ProPublica noted, quoting Bob Graham, the former chair of the Senate Intelligence Committee:

U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al Mihdhar, long before 9/11 and had the ability find him, but they failed to do so.

"There were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar," says former Senator Bob Graham, the Florida Democrat who extensively investigated 9/11 as chairman of the Senate's intelligence committee.

Moreover, Peter Bergen and a team at the New America Foundation dug into the government's claims about plots in America, including studying over 225 individuals recruited by al Qaeda and similar groups in the United States and charged with terrorism, and concluded:

Our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading...

When backed into a corner, the government's apologists cite the capture of Zazi, the so-called New York subway bomber. However, in that case, the Associated Press reported that the government could have easily stopped the plot without the NSA program, under authorities that comply with the Constitution. Sens. Ron Wyden and Mark Udall have been saying this for a long time.

Both of the President's hand-picked advisors on mass surveillance concur about the telephone records collection. The President's Review Board issued a report in which it stated "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks," The Privacy and Civil Liberties Oversight Board (PCLOB) also issued a report in which it stated, "we have not identified a single instance involving a threat to the United States in which [bulk collection under Section 215 of the Patriot Act] made a concrete difference in the outcome of a counterterrorism investigation."

And in an amicus brief in EFF's case First Unitarian Church of Los Angeles v. the NSA case, Sens. Ron Wyden, Mark Udall, and Martin Heinrich stated that, while the administration has claimed that bulk collection is necessary to prevent terrorism, they "have reviewed the bulk-collection program extensively, and none of the claims appears to hold up to scrutiny."

Even former top NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US and at most, helped catch one guy who shipped about \$8,000 to a Somalian group that the US has designated as a terrorist group but that has never even remotely been involved in any attacks aimed at the US.

Mass surveillance fails --- numerous empirical examples prove we are never able to effectively act on intelligence.

Patrick Eddington, 1/27/2015. Policy analyst in homeland security and civil liberties at the Cato Institute. "No, Mass Surveillance Won't Stop Terrorist Attacks," Reason, <http://reason.com/archives/2015/01/27/mass-surveillance-and-terrorism>.

But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the answer:

2009: Umar Farouk Abdulmutallab—i.e., the "underwear bomber"—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community(IC) failed "to connect, integrate, and fully understand the intelligence" it had collected.

2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation.

2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency (NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from

Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS.

2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine.

No, mass surveillance does not prevent terrorist attacks.

It's worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally-dubious ones—were premised on the belief that bin Laden's hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data. Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government's hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination. That malady perfectly describes every intelligence failure from Pearl Harbor to the present day.

The Office of the Director of National Intelligence (created by Congress in 2004) was supposed to be the answer to the "failure-to-connect-the-dots" problem. Ten years on, the problem remains, the IC bureaucracy is bigger than ever, and our government is continuing to rely on mass surveillance programs that have failed time and again to stop terrorists while simultaneously undermining the civil liberties and personal privacy of every American. The quest to "collect it all," to borrow a phrase from NSA Director Keith Alexander, only leads to the accumulation of masses of useless information, making it harder to find real threats and costing billions to store.

A recent Guardian editorial noted that such mass-surveillance myopia is spreading among European political leaders as well, despite the fact that "terrorists, from 9/11 to the Woolwich jihadists and the neo-Nazi Anders Breivik, have almost always come to the authorities' attention before murdering."

Mass surveillance is not only destructive of our liberties, its continued use is a virtual guarantee of more lethal intelligence failures. And our continued will to disbelieve those facts is a mental dodge we engage in at our peril.

Applications of network theory are helpful for preventing fraud but not terrorism --- mass surveillance just generates over-saturation of information.

Patrick Radden Keefe, 3/12/2006. Century Foundation fellow, is the author of "Chatter: Dispatches from the Secret World of Global Eavesdropping." "Can Network Theory Thwart Terrorists?" New York Times, <http://www.trecento.com/lfriedl/tmp/forwiki/nwks.html>.

Recent debates about the National Security Agency's warrantless-eavesdropping program have produced two very different pictures of the operation. Whereas administration officials describe a carefully aimed "terrorist surveillance program," press reports depict a pervasive electronic net ensnaring thousands of innocent people and few actual terrorists. Could it be that both the administration and its critics are right? One way to reconcile these divergent accounts — and explain the administration's decision not to seek warrants for the surveillance — is to examine a new conceptual paradigm that is changing how America's spies pursue terrorists: network theory.

During the last decade, mathematicians, physicists and sociologists have advanced the scientific study of networks, identifying surprising commonalities among the ways airlines route their flights, people interact at cocktail parties and crickets synchronize their chirps. In the increasingly popular language of network theory, individuals are "nodes," and

relationships and interactions form the "links" binding them together; by mapping those connections, network scientists try to expose patterns that might not otherwise be apparent. Researchers are applying newly devised algorithms to vast databases — one academic team recently examined the e-mail traffic of 43,000 people at a large university and mapped their social ties. Given the difficulty of identifying elusive terror cells, it was only a matter of time before this new science was discovered by America's spies.

In its simplest form, network theory is about connecting the dots. Stanley Milgram's finding that any two Americans are connected by a mere six intermediaries — or "degrees of separation" — is one of the animating ideas behind the science of networks; the Notre Dame physicist Albert-Laszlo Barabasi studied one obvious network — the Internet — and found that any two unrelated Web pages are separated by only 19 links. After Sept. 11, Valdis Krebs, a Cleveland consultant who produces social network "maps" for corporate and nonprofit clients, decided to map the hijackers. He started with two of the plotters, Khalid al-Midhar and Nawaf Alhazmi, and, using press accounts, produced a chart of the interconnections — shared addresses, telephone numbers, even frequent-flier numbers — within the group. All of the 19 hijackers were tied to one another by just a few links, and a disproportionate number of links converged on the leader, Mohamed Atta. Shortly after posting his map online, Krebs was invited to Washington to brief intelligence contractors.

Announced in 2002, Adm. John Poindexter's controversial Total Information Awareness program was an early effort to mine large volumes of data for hidden connections. But even before 9/11, an Army project called Able Danger sought to map Al Qaeda by "identifying linkages and patterns in large volumes of data," and may have succeeded in identifying Atta as a suspect. As if to underline the project's social-network principles, Able Danger analysts called it "the Kevin Bacon game."

Given that the N.S.A. intercepts some 650 million communications worldwide every day, it's not surprising that its analysts focus on a question well suited to network theory: whom should we listen to in the first place? Russell Tice, a former N.S.A. employee who worked on highly classified Special Access Programs, says that analysts start with a suspect and "spider-web" outward, looking at everyone he contacts, and everyone those people contact, until the list includes thousands of names. Officials familiar with the program have said that before individuals are actually wiretapped, computers sort through flows of metadata — information about who is contacting whom by phone or e-mail. An unclassified National Science Foundation report says that one tool analysts use to sort through all that data is link analysis.

The use of such network-based analysis may explain the administration's decision, shortly after 9/11, to circumvent the Foreign Intelligence Surveillance Court. The court grants warrants on a case-by-case basis, authorizing comprehensive surveillance of specific individuals. The N.S.A. program, which enjoys backdoor access to America's major communications switches, appears to do just the opposite: the surveillance is typically much less intrusive than what a FISA warrant would permit, but it involves vast numbers of people.

In some ways, this is much less alarming than old-fashioned wiretapping. A computer that monitors the metadata of your phone calls and e-mail to see if you talk to terrorists will learn less about you than a government agent listening in to the words you speak. The problem is that most of us are connected by two degrees of separation to thousands of people, and by three degrees to hundreds of thousands. This explains reports that the overwhelming number of leads generated by the N.S.A. program have been false positives — innocent civilians implicated in an ever-expanding associational web.

This has troubling implications for civil liberties. But it also points to a practical obstacle for using link analysis to discover terror networks: information overload. The National Counterterrorism Center's database of suspected terrorists contains 325,000 names; the Congressional Research Service recently found that the N.S.A. is at risk of being drowned in information. Able Danger analysts produced link charts identifying suspected Qaeda figures, but some charts were 20 feet long and covered in small print. If Atta's name was on one of those

network maps, it could just as easily illustrate their ineffectiveness as it could their value, because nobody pursued him at the time.

One way to make sense of these volumes of information is to look for network hubs. When Barabasi mapped the Internet, he found that sites like Google and Yahoo operate as hubs — much like an airline hub at Newark or O'Hare — maintaining exponentially more links than the average. The question is how to identify the hubs in an endless flow of records and intercepted communications. Scientists are using algorithms that can determine the "role structure" within a network: what are the logistical and hierarchical relationships, who are the hubs? The process involves more than just tallying links. If you examined the metadata for all e-mail traffic at a university, for instance, you might find an individual who e-mailed almost everyone else every day. But rather than being an especially connected or charismatic leader, this individual could turn out to be an administrator in charge of distributing announcements. Another important concept in network theory is the "strength of weak ties": the most valuable information may be exchanged by actors from otherwise unrelated social networks.

Network academics caution that the field is still in its infancy and should not be regarded as a panacea. Duncan Watts of Columbia University points out that it's much easier to trace a network when you can already identify some of its members. But much social-network research involves simply trawling large databases for telltale behaviors or activities that might be typical of a terrorist. In this case the links among people are not based on actual relationships at all, but on an "affiliation network," in which individuals are connected by virtue of taking part in a similar activity. This sort of approach has been effective for corporations in detecting fraud. A credit-card company knows that when someone uses a card to purchase \$2 of gas at a gas station, and then 20 minutes later makes an expensive purchase at an electronics store, there's a high probability that the card has been stolen. Marc Sageman, a former C.I.A. case officer who wrote a book on terror networks, notes that correlating certain signature behaviors could be one way of tracking terrorists: jihadist groups in Virginia and Australia exercised at paint-ball courses, so analysts could look for Muslim militants who play paint ball, he suggests. But whereas there is a long history of signature behaviors that indicate fraud, jihadist terror networks are a relatively new phenomena and offer fewer reliable patterns.

There is also some doubt that identifying hubs will do much good. Networks are by their very nature robust and resistant to attack. After all, while numerous high ranking Qaeda leaders have been captured or killed in the years since Sept. 11, the network still appears to be functioning. "If you shoot the C.E.O., they'll hire another one," Duncan Watts says. "The job will still get done."

All Attacks Were Committed by known Terrorists – Don't Need Excess Data

Matthias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Almost every major terrorist attack on Western soil in the past fifteen years has been committed by people who were already known to law enforcement. One of the gunmen in the attack on Charlie Hebdo, in Paris, had been sent to prison for recruiting jihadist fighters. The other had reportedly studied in Yemen with Umar Farouk Abdulmutallab, the underwear bomber, who was arrested and interrogated by the F.B.I. in 2009. The leader of the 7/7 London suicide bombings, in 2005, had been observed by British intelligence meeting with a suspected terrorist, though MI5 later said that the bombers were "not on our radar." The men who planned the Mumbai attacks, in 2008, were under electronic surveillance by the United States, the United Kingdom, and India, and one had been an informant for the Drug Enforcement Administration. One of the brothers accused of bombing the Boston Marathon was the subject of an F.B.I. threat assessment and a warning from Russian intelligence. In each of these cases, the authorities were not wanting for data. What they failed to do was appreciate the significance of the data they already had. Nevertheless, since 9/11, the National Security Agency has sought to acquire every possible scrap of digital information—what General Keith Alexander, the agency's former head, has called "the whole haystack." The size of the haystack was revealed in June, 2013, by Edward Snowden. The N.S.A.

vacuums up Internet searches, social-media content, and, most controversially, the records (known as metadata) of United States phone calls—who called whom, for how long, and from where. The agency stores the metadata for five years, possibly longer.

Majority of Data is junk and unrelated to Terror

Rebecca Abrahams, 10-21, 13, "What's Behind the Spying?" CCO, SVP Ziklag Systems, a mobile security technology company, http://www.huffingtonpost.com/rebecca-abrahams/whats-behind-the-spying_b_4136079.html

The NSA "cover story" is that extensive spying is necessary to stop terrorism. But NSA has been hard pressed to demonstrate that its phone and Internet spying has actually helped stop terrorism, and targeting the President of Mexico or key government and industrial leaders in France, Germany and many other countries, is absolutely divorced from having any linkage to terrorism. In fact, the United States has been carrying out political and economic spying. Terrorism probably accounts for only a small portion of what the mighty NSA collection apparatus sweeps up.

Most of the surveillance is for economic espionage, not terror prevention

Li Jingjing, Global Times (China), June 24, 2014

'No Place to Hide' Although the US government has tried to use the prevention of terrorism as an excuse to justify its programs, based on the documents Snowden revealed, most of the intelligence collected had less to do with anti-terrorism and more to do with economic espionage. No matter if it was Brazilian oil giant Petrobras, Russian gas company Gazprom, Russian airline Aeroflot or the organizations and leaders of other countries, all fell under the purview of this intelligence collection. During a presentation at the TED conference in March, Snowden stated, "Terrorism has always been what we in the intelligence world would call a cover for action. Terrorism is something that provokes an emotional response that allows people to rationalize authorizing powers and programs that they wouldn't give otherwise."

Surveillance doesn't solve

Mass Surveillance Won't Stop Terrorism – because bulk collection does nothing to prevent terrorism

Macri, 3-16-2015 (Giuseppe Macri, writer, 3-16-2015, "Edward Snowden Says Mass Surveillance Won't Stop Terrorism," Daily Caller, <http://dailycaller.com/2015/03/16/edward-snowden-says-mass-surveillance-doesnt-stop-terrorism/>)

National Security Agency whistleblower Edward Snowden spent the weekend popping up at tech conferences across the globe, accusing governments of falsely equating terrorism with mass surveillance and calling on Silicon Valley to take action against them. While speaking virtually at FutureFest London on Saturday, the former NSA contractor called on the U.S., UK and Australia to stop masking mass surveillance underneath sugar-coated terms such as “bulk collection,” which he said does nothing to prevent terrorism. “They’re not going to stop the next attacks either,” Snowden said, referencing the recent terror attacks in Sydney and against the satirical magazine Charlie Hebdo in Paris, which were perpetrated by assailants already known to their governments. “Because they’re not public safety programs. They’re spying programs.” “But the question that we as a society have to ask, are our collective rights worth a small advantage in our ability to spy.”

Snowden said according to news.com.au. Snowden spoke via video to “roughly two dozen people from across the technology and policy world” during a closed door meeting at SXSW Sunday, The Verge reports, which one attendee described as a “call to arms” encouraging tech companies to build better tools to combat spying. With government reform stalled in Congress and the White House, Snowden suggested companies take more aggressive approaches to securing data, calling in particular for the widespread implementation of end-to-end encryption, which keeps even companies themselves from accessing data. “

Mass surveillance doesn't catch terrorists – France and UK proves

Corrigan 15 Ray Corrigan (Ray Corrigan is a senior lecturer in mathematics, computing, and technology at the Open University, U.K.), “Mass Surveillance Will Not Stop Terrorism” Jan. 25, 2015, http://www.slate.com/articles/health_and_science/new_scientist/2015/01/mass_surveillance_against_terrorism_gathering_intelligence_on_all_is_statistically.html

In response to the terrorist attacks in Paris, the U.K. government is redoubling its efforts to engage in mass surveillance. Prime Minister David Cameron wants to reintroduce the so-called snoopers’ charter—properly, the Communications Data Bill—which would compel telecom companies to keep records of all Internet, email, and cellphone activity. He also wants to ban encrypted communications services. Cameron seems to believe terrorist attacks can be prevented if only mass surveillance, by the U.K.’s intelligence-gathering center GCHQ and the U.S. National Security Agency, reaches the degree of perfection portrayed in his favorite TV dramas, where computers magically pinpoint the bad guys. Computers don’t work this way in real life and neither does mass surveillance. Brothers Said and Cherif Kouachi and Amedy Coulibaly, who murdered 17 people, were known to the French security services and considered a serious threat. France has blanket electronic surveillance. It didn’t avert what happened. Police, intelligence, and security systems are imperfect. They process vast amounts of imperfect intelligence data and do not have the resources to monitor all known suspects 24/7. The French authorities lost track of these extremists long enough for them to carry out their murderous acts. You cannot fix any of this by treating the entire population as suspects and then engaging in suspicionless, blanket collection and processing of personal data. Mass data collectors can dig deeply into anyone’s digital persona but don’t have the resources to do so with everyone. Surveillance of the entire population, the vast majority of whom are innocent, leads to the diversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle-in-a-haystack problem. You don’t make it easier by throwing more needless hay on the stack. It is statistically impossible for total population surveillance to be an effective tool for catching terrorists. Even if your magic terrorist-catching machine has a false positive rate of 1 in 1,000—and no security technology comes anywhere near this—every time you asked it for suspects in the U.K. it would flag 60,000 innocent people. Law enforcement and security services need to be able to move with the times, using modern digital technologies intelligently and through targeted data preservation—not a mass surveillance regime—to engage in court-supervised technological surveillance of individuals whom they have reasonable cause to suspect. That is not, however, the same as building an infrastructure of mass surveillance. Mass surveillance makes the job of the security services more difficult and the rest of us less secure.

Mass surveillance does not stop terrorism – Aff answer to DA

Corrigan in 2015 (Ray Corrigan; a senior lecturer in mathematics, computing, and technology at the Open University, U.K., “Mass Surveillance Will Not Stop Terrorism”, 01/25/15 New Scientist, Website, http://www.slate.com/articles/health_and_science/new_scientist/2015/01/mass_surveillance_against_terrorism_gathering_intelligence_on_all_is_statistically.html)

Some U.K. politicians are trying once again to pass mass surveillance laws after the Paris attacks. It's a misguided approach, says a computing researcher. In response to the terrorist attacks in Paris, the U.K. government is redoubling its efforts to engage in mass surveillance. Prime Minister David Cameron wants to reintroduce the so-called snoopers' charter—properly, the Communications Data Bill—which would compel telecom companies to keep records of all Internet, email, and cellphone activity. He also wants to ban encrypted communications services. Cameron seems to believe terrorist attacks can be prevented if only mass surveillance, by the U.K.'s intelligence-gathering center GCHQ and the U.S. National Security Agency, reaches the degree of perfection portrayed in his favorite TV dramas, where computers magically pinpoint the bad guys. Computers don't work this way in real life and neither does mass surveillance. Brothers Said and Cherif Kouachi and Amedy Coulibaly, who murdered 17 people, were known to the French security services and considered a serious threat. France has blanket electronic surveillance. It didn't avert what happened. Police, intelligence, and security systems are imperfect. They process vast amounts of imperfect intelligence data and do not have the resources to monitor all known suspects 24/7. The French authorities lost track of these extremists long enough for them to carry out their murderous acts. You cannot fix any of this by treating the entire population as suspects and then engaging in suspicionless, blanket collection and processing of personal data. Mass data collectors can dig deeply into anyone's digital persona but don't have the resources to do so with everyone. Surveillance of the entire population, the vast majority of whom are innocent, leads to the diversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle-in-a-haystack problem. You don't make it easier by throwing more needless hay on the stack. It is statistically impossible for total population surveillance to be an effective tool for catching terrorists. Even if your magic terrorist-catching machine has a false positive rate of 1 in 1,000—and no security technology comes anywhere near this—every time you asked it for suspects in the U.K. it would flag 60,000 innocent people. Law enforcement and security services need to be able to move with the times, using modern digital technologies intelligently and through targeted data preservation—not a mass surveillance regime—to engage in court-supervised technological surveillance of individuals whom they have reasonable cause to suspect. That is not, however, the same as building an infrastructure of mass surveillance. Mass surveillance makes the job of the security services more difficult and the rest of us less secure.

Increasing surveillance does nothing – little evidence proving it to stop terrorist threats

Tuccille '15 (J.D. Tuccille Managing Editor for reason.com, 1/14/15, “What's a Terrorist Attack If Not An Excuse for More Domestic Spying?” <http://reason.com/blog/2015/01/14/whats-a-terrorist-attack-if-not-an-excuse>)

Following on last week's terrorist attacks in France, the British government has dusted off a long-sought "snooper's charter"—better known as the Data Communications Bill—to ease the power of officials to track people's private communications. "It is too soon to say for certain, but it is highly probable that communications data was used in the Paris attacks to locate the suspects and establish the links between the two attacks," Home Secretary Theresa May told Parliament. "Quite simply, if we want the police and the security services to protect the public and save lives, they need this capability. You get that? There's no evidence that the bill would have prevented the Charlie Hebdo attack, but that incident is why you should pass the bill. Prime Minister David Cameron even says that messaging services that can't be intercepted should be banned. Using the latest outrage to inject new life into old security-state legislation isn't a British specialty. When the Patriot Act was introduced in 2001, then-Senator Joseph Biden boasted, "I drafted a terrorism bill after the Oklahoma City bombing. And the bill John Ashcroft sent up was my bill." This is a game in which politicians everywhere can participate. Never mind that, as Reason's Ron Bailey pointed out

in November, "there is very little evidence that the Internet is making terrorism easier to do." But pretending otherwise, and passing legislation that empowers security services, lets government officials accumulate power and give the appearance of doing something when the public is frightened. Added Bailey: As [David Benson, a political scientist at the University of Chicago] argues, exaggerating the Internet's usefulness to terrorism has "egregious costs." Some officials, for example, have been calling for a "kill switch" that would allow the government to shut down the Internet in an emergency. Noting how much Americans depend upon the Net for commerce, communication, medical care, and so forth, Benson points out that "It is difficult to imagine a terrorist attack being as costly as turning off the Internet would be." Terrorism also gives officials an excuse to tighten censorship—especially in jurisdictions, including many democratic countries in Europe, where the whole free speech thing has relatively shallow roots. So get ready for the ride. Driven by a need to appear proactive, and a preexisting taste for accumulating power, government officials once again exploit a murderous incident to increase their authority over us. Which escalates the ongoing cold war between people who want to be left alone, and the governments that seek to control them.

Mass surveillance doesn't prevent terrorism – Impractical mass surveillance reduces effectiveness

Corrigan, 1-13-2015 (Ray Corrigan, is Senior Lecturer in Technology at The Open University, 1-13-2015, "Mass surveillance will never be able to stop all known terrorists," Conversation, <http://theconversation.com/mass-surveillance-will-never-be-able-to-stop-all-known-terrorists-36177>)

The French intelligence and security services could not keep track of the Kouachi brothers, known extremists, to a sufficient degree to prevent the Charlie Hebdo attacks. Likewise Amedy Coulibaly who murdered a police officer on the street and four others in a supermarket. France has blanket electronic surveillance and armed police. It even has the ID cards so beloved (and so tantalisingly out of reach) of Tony Blair and his succession of home secretaries. It has an inquisitorial justice system, the purveyors of the Counter Terrorism and Security Bill's "prevent duty" seem to be hankering after. It arguably also has a constitution that mass surveillance, at least, offends against. None of it was enough to stop the Kouachis and Coulibaly. Absolute security and guaranteed prevention of these kinds of extreme acts is impossible. Mass surveillance cannot and will not move us any closer to that goal. Counterintuitively, it actually makes us all less secure. Diverting limited intelligence resources from pursuing truly dangerous suspects, in order to watch everyone, is a really bad idea. If it takes a conservative 20 intelligence and security staff to monitor a suspect 24/7, the state would need to figure out how to muster the 1.2 billion staff and associated resources to keep tabs on the UK's 60m-plus people. In case you'd forgotten. whatleydude via Flickr, CC BY And if it can't monitor all of us 24/7, the government will need ways to decide who and how many to watch, in addition to the known dangerous individuals it's already unable to keep track of.

Mass surveillance hinders finding terrorist- makes rest of us less secure- turns impact

Corrigan 1/25/15 (Roy Corrigan, teacher at Open University, U.K., 1/25/15, "Mass Surveillance Will Not Stop Terrorism", http://www.slate.com/articles/health_and_science/new_scientist/2015/01/mass_surveillance_against_terrorism_gathering_intelligence_on_all_is_statistically.html, 7/1/15)

Cameron seems to believe terrorist attacks can be prevented if only mass surveillance, by the U.K.'s intelligence-gathering center GCHQ and the U.S. National Security Agency, reaches the degree of perfection portrayed in his favorite TV dramas, where computers magically pinpoint the bad guys. Computers don't work this way in real life and neither does mass surveillance. Brothers Said and Cherif Kouachi and Amedy Coulibaly, who murdered 17 people, were known to the French security services and considered a serious threat. France has blanket electronic

surveillance. It didn't avert what happened. **Police, intelligence, and security systems are imperfect.** They process vast amounts of imperfect intelligence data and do not have the resources to monitor all known suspects 24/7. The French authorities lost track of these extremists long enough for them to carry out their murderous acts. You cannot fix any of this by treating the entire population as suspects and then engaging in suspicionless, blanket collection and processing of personal data. Mass data collectors can dig deeply into anyone's digital persona but don't have the resources to do so with everyone. Surveillance of the entire population, the vast majority of whom are innocent, leads to the diversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle-in-a-haystack problem. You don't make it easier by throwing more needless hay on the stack. It is statistically impossible for total population surveillance to be an effective tool for catching terrorists. Even if your magic terrorist-catching machine has a false positive rate of 1 in 1,000—and no security technology comes anywhere near this—every time you asked it for suspects in the U.K. it would flag 60,000 innocent people. Top Comment . The most permanent thing in the world is a temporary government bureau. More... -Formerly Pepin the Short 68 CommentsJoin In Law enforcement and security services need to be able to move with the times, using modern digital technologies intelligently and through targeted data preservation—not a mass surveillance regime—to engage in court-supervised technological surveillance of individuals whom they have reasonable cause to suspect. That is not, however, the same as building an infrastructure of mass surveillance. Mass surveillance makes the job of the security services more difficult and the rest of us less secure.

NSLs Specific

National Security Letters are not needed- time is not an issue

Baker and Sanger on May 1st, 2015 (Peter Baker and Peter Sanger, Political writer and chief Washington correspondent, “Why the N.S.A. Isn’t Howling Over Restrictions”, May 1st 2015, <http://www.nytimes.com/2015/05/02/us/politics/giving-in-a-little-on-national-security-agency-data-collection.html>, 6/29/15) DPC

“N.S.A. believes that on at least a few occasions, information derived” had “contributed to its efforts to prevent possible terrorist attacks, either in the United States or somewhere else in the world,” the report said. But the panel concluded that its review showed that the information collected under the program “was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional” court orders. The panel recommended legislation that “terminates the storage of bulk telephony metadata by the government” and that, it be held instead by telecommunications companies or some other third party, ensuring that the government gained access only when the Foreign Intelligence Surveillance Court issued an order. Although the government said nothing at the time, General Alexander, then in his last months as the head of the N.S.A., told Mr. Obama that it would be preferable if legislation were passed that moved the program to private hands.

President’s closest advisors say that the National Security Letter does not help with terrorism- This shows that it is ineffective

Ross in 13 (Brian Ross, ABC News Chief Investigative Correspondent, “President Obama’s Own Experts Recommend End to NSA Phone Data Spying”, December 18th 2013, <http://abcnews.go.com/Blotter/nsa-surveillance-obamas-experts-recommend-end-nsa-phone/story?id=21265133>, 6/29/15) DPC

In calling for sweeping curbs on the NSA, the panel said stressed the need for increased transparency and less secrecy. “Americans must never make the mistake of wholly ‘trusting’ our public officials,” the report concluded. The NSA declined to comment on the report today. The President’s review group, which had access to top-secret information, concluded the bulk collection of American citizens’ phone records served little useful purpose in combatting terrorism, producing only 12 tips to the FBI in 2012. “There are very few pieces of data that have been collected in this program that have been useful,” Clarke said. The NSA has maintained the program is essential in the efforts to stop terror attacks. In response to the panel report, Leahy, Chairman of the Senate Judiciary Committee, praised the recommendations. “The message to the NSA is now coming from every branch of government and from every corner of our nation: You have gone too far,” he said. “This momentous report from the President’s closest advisers is a vindication of the efforts of a bipartisan group of legislators that has been working for years to protect Americans’ privacy by reining in these intelligence authorities. I welcome the report and call on the President to immediately consider implementing the recommendations that can be achieved without legislation.”

Drones

Drones are inefficient mechanism to solve terrorism

Rothfuss 2014 (Ian F [George Mason School of Law]; Student Comment: An Economic Perspective on the Privacy Implications of Domestic Drone Surveillance; 10 J.L. Econ. & Pol'y 441; kdf)

Conclusion

U.S. citizens want to be safe from terrorist attacks and other threats, but not at the expense of their privacy rights. Therefore, a delicate balance must be achieved between privacy and security interests. Drones represent a surveillance technology advancement that threatens to dramatically alter the balance between these interests. As discussed in this comment, the current legal framework does not adequately protect privacy from the widespread surveillance that will likely result from the unrestricted domestic use of drones. Therefore, prompt legislative action is necessary to address the fundamental privacy challenges presented by the use of drones. Such legislation should allow for constructive use of drones within a framework that contains restrictions to protect individual privacy rights. While widespread general surveillance could make the nation safer from crime and terrorism, such extensive surveillance will ultimately be inefficient. The surveillance that could result from the domestic use of drones would detract from individual privacy and cause individuals to reduce productive activities and invest in countermeasures. Such "privacy disutility" will outweigh the societal benefits unless domestic drone surveillance is restricted. Therefore, [*462] without legislative action we may soon live in a world where "every time we walk out of our front door we have to look up and wonder whether some invisible eye in the sky is monitoring us." n175

Drones – Link Turn

Turn —warrantless use of drones ensures a perpetual state of psychological terrorism— only the aff solves

Greenwald 13 — ex-constitutional lawyer, former columnist on civil liberties and US national security issues for the Guardian

(Glenn Greenwald, 3-29-2013, "Domestic drones and their unique dangers,"
<http://www.theguardian.com/commentisfree/2013/mar/29/domestic-drones-unique-dangers>, Date Accessed: 6-23-2015) //NM

What is most often ignored by drone proponents, or those who scoff at anti-drone activism, are the unique features of drones: the way they enable more warfare, more aggression, and more surveillance. Drones make war more likely precisely because they entail so little risk to the war-making country. Similarly, while the propensity of drones to kill innocent people receives the bulk of media attention, the way in which drones psychologically terrorize the population - simply by constantly hovering over them: unseen but heard - is usually ignored, because it's not happening in the US, so few people care (see this AP report from yesterday on how the increasing use of drone attacks in Afghanistan is truly terrorizing local villagers). It remains to be seen how Americans will react to drones constantly hovering over their homes and their childrens' schools, though by that point, their presence will be so institutionalized that it will be likely be too late to stop. Notably, this may be one area where an actual bipartisan/trans-partisan alliance can meaningfully emerge, as most advocates working on these issues with whom I've spoken say that libertarian-minded GOP state legislators have been as responsive as more left-wing Democratic ones in working to impose some limits. One bill now pending in Congress would prohibit the use of surveillance drones on US soil in the absence of a specific search warrant, and has bipartisan support. Only the most authoritarian among us will be incapable of understanding the multiple dangers posed by a domestic drone regime (particularly when their party is in control of the government and they are incapable of perceiving threats from increased state police power). But the proliferation of domestic drones affords a real opportunity to forge an enduring coalition in defense of core privacy and other rights that transcends partisan allegiance, by working toward meaningful limits on their use. Making people aware of exactly what these unique threats are from a domestic drone regime is the key first step in constructing that coalition.

Airport Security

TSA fails 95 percent of the time—heightens security risk

Campbell 6/1 — Huffington Post

(Andy, 6-1-2015, "TSA Fails 95 Percent Of Undercover Security Tests: Report," http://www.huffingtonpost.com/2015/06/01/tsa-fails-95-percent-tests-homeland-security_n_7485558.html, Date Accessed: 6-22-2015) //NM

As thorough as the Transportation Security Administration screeners may be as they rifle through your belongings, the agency isn't performing where it counts. In a series of trials, the Department of Homeland Security was able to smuggle fake explosives, weapons and other contraband past airport screeners in major cities across the country, according to ABC News. Officials briefed on the Homeland Security Inspector General's investigation told the station that the TSA failed 67 out of 70 tests conducted by the department's Red Teams -- undercover passengers tasked with identifying weaknesses in the screening process, NJ.com reports. During the tests, DHS agents each tried to bring a banned item past TSA screeners. They succeeded 95 percent of the time. The internal investigation was designed to find the TSA's most egregious vulnerabilities. The TSA has said Red Team agents are "super terrorists" who "push the boundaries of our people, processes, and technology," but DHS officials told ABC the test results were frustrating at the very least. ABC reports: In one test an undercover agent was stopped after setting off an alarm at a magnetometer, but TSA screeners failed to detect a fake explosive device that was taped to his back during a follow-on pat down. Officials would not divulge the exact time period of the testing other than to say it concluded recently. Homeland Security Secretary Jeh Johnson was apparently so frustrated by the findings he sought a detailed briefing on them last week at TSA headquarters in Arlington, Virginia, according to sources. U.S. officials insisted changes have already been made at airports to address vulnerabilities identified by the latest tests. The TSA referred all questions to the DHS. A DHS spokesman told The Huffington Post that "Red Team testing of the aviation security network has been part of TSA's mission advancement for 13 years."

And, the TSA fails at screening their own employees

Jansen 6/16 — USA Today

(Bart Jansen, 6-16-2015, "TSA finds no threat from 73 workers who fell through screening loophole," <http://www.usatoday.com/story/news/nation/2015/06/16/tsa-aviation-worker-background-checks-inspector-general/28807021/>, Date Accessed: 6-22-2015) //NM

WASHINGTON – The Transportation Security Administration found no threat from 73 aviation workers cited as possible security risks after they fell through a screening loophole, a House panel heard Tuesday. Stacey Fitzmaurice, TSA's deputy assistant administrator for the Office of Intelligence and Analysis, told the Homeland Security subcommittee on transportation that TSA re-checked the workers cited in an inspector general's report for having possible links to terrorism and found no threats. "To be clear, these individuals are not considered to be known or suspected terrorists," Fitzmaurice said. "The individuals do not pose a threat to transportation security." Even so, lawmakers urged TSA to gain access to the broader government intelligence database that includes people with alleged links to terrorism. TSA expects access by the end of the year. TSA is not responding in a timely manner to seemingly very important issues," said Rep. John Katko, R-N.Y., the committee's chairman. "We cannot have a bureaucratic morass in charge of guarding our airports." TSA screens 2 million workers who operate behind security checkpoints in jobs from mechanics to shop clerks. But the inspector general for the Department of Homeland Security revealed last week that while TSA checks names against an FBI terrorist watch list, it does not have access to a broader database maintained by the National Counterterrorism Center (NCTC). While the FBI's watch list contains "reasonable"

suspicions against people, the NCTC list includes rawer intelligence that doesn't meet that standard, Fitzmaurice said. The former head of TSA asked for access to the broader NCTC list in May 2014. The agency expects to obtain access by the end of 2015. Fitzmaurice said the intelligence-related data may provide a benefit in evaluating security risks. Inspector General John Roth told lawmakers it took 18 months for his office to jump the legal hurdles to allow it to run the names of aviation workers against the different databases for its report. But he said the task of checking the 900,000 names is relatively simple. "Legally and bureaucratically, it was a huge lift," Roth said. "It was not that big a task to match one set of data against another set of data."

TSA measures cant identify people flagged as terrorists

Gass 15— degree in convergence journalism (Nick, “Report: TSA missed 73 terrorism-flagged airline workers,” Politico, 6/8/15, <http://www.politico.com/story/2015/06/tsa-missed-73-terrorism-flagged-airline-workers-report-118738.html>). WM

The Transportation Security Administration failed to identify at least 73 people employed in the airline industry flagged under terrorism-related activity codes, according to a recent report by its inspector general. These people, including employees of major airlines, airport vendors and other employers, were all cleared to access secure airport areas despite being watch-listed. The reason for this, according to the TSA, is in part because the agency “is not authorized to receive all terrorism-related information under current interagency watchlisting policy.” Rather than conducting criminal-history and work-authorization checks itself, the TSA generally delegated individual airports to do these tasks, though it had limited oversight. “Thus, TSA lacked assurance that it properly vetted all credential applicants,” the report says. Additionally, thousands of records used to vet these workers had incomplete or inaccurate data, the report says. The agency “risks credentialing and providing unescorted access to secure airport areas for workers with potential to harm the nation’s air transportation system,” it concludes. The latest news comes a week after interim TSA chief Melvin Carraway was reassigned the same day a bombshell report surfaced, finding that officials failed to stop undercover TSA agents from smuggling banned weapons or fake explosives through airport security.

TSA programs are scientifically proven infective

KONSTANTINIDES 15— reporter (Anetta, “How to spot a terrorist: TSA's checklist reveals the behavior they look out for, including a 'strong body odor', 'whistling' and a 'cold penetrating stare,'” Daily Mail, 28 March 2015, <http://www.dailymail.co.uk/news/article-3015970/TSA-s-SPOT-checklist-reveals-behavioral-trait-agents-look-spot-terrorist.html>). WM

A behavioral checklist that the Transportation Security Administration uses to help identify airport travelers they believe could be potential terrorists has been revealed. The Screening of Passengers by Observation Techniques system, nicknamed SPOT, breaks down body language and demeanor the TSA believes indicates either 'stress' or 'deception'. Mannerisms are assigned points based on their severity and are assessed by trained 'Behavior Detection Officers', who observe passengers as they go through the security checkpoint. Behaviors are given points based on their perceived severity. If you walk through security with a 'face pale from recent shaving of beard' or happen to be yawning or whistling, you can be assigned one point. A strong body odor, sweaty palms and a bobbing Adam's apple can also get you one point, according to the checklist obtained by The Intercept. Having 'widely open eyes' will get you two points, as will showing 'unusual' interest in a security officer's work routine or having 'identical luggage or dress' to an individual who does not seem related to you. Appearing to be in disguise will get you three points. But you can also get points shaved off. If you appear to be a member of a family or part of

a married couple, you get two points deducted from your score. Being a female over 55, or a male over 65, gets you a one point reduction. The checklist includes a list of items and behaviors to look out for if a passenger is pulled aside for inspection. 'Suspicious' items range from blueprints to liquids 'in excess of 3.4oz'. Further signs of deception include excessive yawning or perspiration and lacking details about the purpose of one's trip. The SPOT program, which has cost more than \$800million since its inception in 2007, was deemed ineffective by both the Department of Homeland Security and the Government Accountability Office last year. The GAO found that there was no scientific evidence to support the SPOT's claim that terrorists can be picked out via 'behavioral indicators', and said the human's ability to 'accurately identify' suspicious behavior is 'slightly better than chance'.

The Department of Homeland Security report said that the TSA had not assessed the effectiveness of the SPOT program or designed a 'comprehensive training program' for it.

It concluded that the TSA could not 'ensure that passengers at United States airports are screened objectively' with SPOT and did not believe the administration could 'justify the program's expansion'.

PRISM

Terrorists adapting—metadata collection is obsolete

Eli Lake, 15 "The Phony Surveillance Debate", BloombergView 6-1-

2015 <http://www.bloombergview.com/articles/2015-06-01/the-phony-surveillance-debate>

If any terrorists are reading this column, now would be a good time to turn on C-Span 2. For the next few days, you guys got it made. Section 215 of the Patriot Act has expired and the Senate has only just started debating the bill that would renew and tailor these authorities. So if you suspect you might be under investigation, go ahead and switch burner phones. No more roving wiretaps. Feel free to contact any compatriots inside the United States on a landline. No more bulk collection of telephone metadata. Gather ye rosebuds. Carpe diem. This at least is what the White House and others would have you believe. Speaking on "Face the Nation" on Sunday, CIA Director John Brennan warned that terrorists are monitoring the Congressional debate carefully "looking for the seams to operate within." President Obama himself warned on Saturday that terrorists like al Qaeda and the Islamic State "aren't suddenly going to stop plotting against us at midnight tomorrow. And we shouldn't surrender the tools that help keep us safe." What happened to the Barack Obama of 2008, who warned voters about the politics of fear? Well, in this case it's more "politics" than "fear." It's true that part of the Patriot Act has expired, including the piece that the government interpreted as giving it the authority for bulk collection of telephone meta-data. And it's not coming back. The Senate is likely to pass the USA Freedom Act, which will require the NSA to search out connections between suspicious phone numbers using data stored by the telecom companies, rather than data banked by the NSA itself. The Patriot Act's "lone wolf" and roving wiretap powers will be restored in the USA Freedom Act. But what about these vulnerable days in the meantime? The reality is they're not very vulnerable. There are probably workarounds that let the government continue its surveillance of bad guys, citing authorities other than the lapsed provisions of the Patriot Act or even relying on some "fuzziness" in the Patriot Act, to use Senator Bob Corker's term from Sunday night. There is Section 702 of the FISA Amendments Act, which gives the NSA the authority to monitor electronic communications of non-citizens. Given the interconnectedness of electronic communications, this provides an important tool for snooping on terrorists dumb enough to still use email. The worst terrorist group these days does a lot of its business in public. The Islamic State recruits and signals its followers on Twitter. This gives all of us the opportunity to play NSA and monitor communications from the group with cutting edge technology like Tweetdeck. This is not to say that terrorists do not also have more clandestine ways of communicating. Al Qaeda, for example, developed an encrypted Internet-based communications system. U.S. officials have also warned that terrorists have changed how they communicate since some of the disclosures by former NSA contractor Edward Snowden

Their stats are untrue – PRISM has had a minimal effect if any on preventing terrorism

Sterman ET. AL, program associate at New America, 14 (David Sterman, Bailey Cahall, Emily Schneider, Peter Bergen, master's degree from Georgetown's Center for Security Studies, worked at the Institute for National Security and Counterterrorism, a joint research center at Syracuse University's Maxwell School and College of Law, "Do NSA's bulk surveillance programs stop terrorists?", <https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/>)

On June 5, 2013, the Guardian broke the first story in what would become a flood of revelations regarding the extent and nature of the NSA's surveillance programs. Facing an uproar over the threat such programs posed to privacy, the Obama administration scrambled to defend them as legal and essential to U.S. national security and counterterrorism. Two weeks after the first leaks by former NSA contractor Edward Snowden were published, President Obama defended the NSA surveillance programs during a visit to Berlin, saying: "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved." Gen. Keith Alexander, the director of the NSA, testified before Congress that: "the information gathered from

these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world.” Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that “54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives.” However, our review of the government’s claims about the role that NSA “bulk” surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda’s ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA’s bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined. Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it’s unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government’s investigations of these cases: <http://natsec.newamerica.net/nsa/analysis>). Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens’ telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided \$8,500 to al-Shabaab, al-Qaeda’s affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to “connect the dots” faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA’s phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it’s unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin’s calls, despite official statements that the bureau had Moalin’s phone number and had identified him. This undercuts the government’s theory that the database of Americans’ telephone metadata is necessary to expedite the investigative process, since it clearly didn’t expedite the process in the single case the government uses to extol its virtues. Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange. In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used. We have also identified three additional plots that the government has not publicly claimed as NSA successes, but in which court records and public reporting suggest the NSA had a role. However, it is not clear whether any of those three cases involved bulk surveillance programs. Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don’t sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

CVE fails

CVE reinforces Islamaphobia – can't solve terror

Ackerman 2/13 --- Spencer Ackerman is national security editor for Guardian US. A former senior writer for Wired, he won the 2012 National Magazine Award for Digital Reporting (Spencer Ackerman, 2-13-2015, "Anti-terrorism summit reinforces 'fear and hate' towards Muslims, critics warn," Guardian, <http://www.theguardian.com/us-news/2015/feb/13/muslim-anti-terrorism-summit-white-house-critics>//A-Sharma)

As Barack Obama prepares to host a summit on preventing homegrown terrorism, he faces a backlash from those he says he wants to empower: American Muslim community leaders, who warn that the summit risks stigmatizing and even endangering them. Hanging over the “countering violent extremism” (CVE) summit, to be held Tuesday through Thursday at the White House and State Department, is Wednesday’s brutal murder of three Muslim students in North Carolina. In the wake of the killings, Muslim leaders, some of whom met with Obama recently, say that whatever the summit’s intentions, it will reinforce a message that American Muslims are to be hated and feared, a spark in what they consider to be a powder-keg of Islamophobia in the media and online. The killing of Deah Barakat, 23, his wife Yusor Mohammad Abu-Salha, 21, and her sister Razan Mohammad Abu-Salha, 19, “really underscores how dangerous it is for the US government, including the White House, to focus its countering violent extremism initiatives primarily on American Muslims”, said Farhana Khera, the executive director of civil rights law firm Muslim Advocates. “We’ve long said to the administration, to those in government, that directing the bulk of CVE resources to US Muslims undermines the safety of all of us and endangers US Muslims, because it sends the message our community is to be viewed with fear, suspicion and even hate.” Without community support, the CVE initiative, a favorite of the Obama administration, is in critical danger. The idea behind CVE is to forge closer ties between communities deemed to be at risk of incubating terrorism – though the White House prefers the term “violent extremism” – and law enforcement. First unveiled by the administration in 2010, CVE has attempted to avoid stating that it singles out Muslim communities, but the emphasis in practice from US attorneys and Department of Homeland Security officials, has disproportionately been on them. Similarly, while the administration talks about CVE meaning “comprehensive” government interlocution, to include greater social services, American Muslims see the face of their government to be police, prosecutors and other elements of the security services. “There is a very real concern in American Muslim community that even one of our community members being pulled into violent extremism is too many, but there's a significant distrust of government-led CVE efforts.” said Corey Saylor of the Council on American Islamic Relations. “That’s because too often in the past you've had this hand reached out in friendship while the other is behind their back with handcuffs in it.” The timing of recent government CVE efforts has struck some as suspect as well. In September, the attorney general, Eric Holder, announced new CVE pilot programs in Boston, Los Angeles and Minneapolis to “develop comprehensive local strategies” – shortly after the Islamic State beheadings of American journalists Steven Sotloff and James Foley. The forthcoming summit was delayed last fall without explanation, only to reappear on the White House agenda after the Charlie Hebdo attack in Paris. A US official, speaking on background ahead of the summit, said next week’s CVE summit will also unveil some new initiatives, though the official declined to specify. Obama will speak personally, but the full agenda, including invitees, has yet to be announced. Foreign delegations will attend at the ministerial level, the official confirmed, which has raised concerns from some in civil-rights circles that the US is “asking other governments to do what is, at the least, constitutionally suspect domestically”, said Hina Shamsi of the ACLU, to include greater intelligence gathering on US Muslims outside the bounds of US law. “This is not an intelligence gathering summit, this is not an Interpol summit,” the US official said. Last week, several Muslim community leaders gathered at the White House ahead of the summit, meeting with senior aides Valerie Jarrett and Ben Rhodes, as well as Obama himself. Khera, the director of Muslim Advocates, was in attendance. While ground rules forbade her from discussing what Obama said, she told the Guardian that she called on Obama to address “an uptick in ferocity of anti-Muslim vitriol from everyday Americans”, including “public officials who should know better”, like a state representative in Oklahoma, an Iraq and Afghanistan veteran, who called Islam a “cancer in our nation that needs to be cut out”, Muslim leaders fear tensions, accelerating

after the release of the film American Sniper and the Paris attacks, have reached a bloody crescendo with the North Carolina shooting. Though local police have said they believe Craig Steven Hicks killed the three over a parking dispute, the family has rejected that explanation, suspecting an Islamophobic motive. The Muslim Public Affairs Council has launched a campaign for Obama, Holder and congressional leaders to address the killings. The FBI has opened a federal inquiry into the shooting deaths. In a statement on Friday, Obama welcomed the FBI inquiry into the “brutal and outrageous murders” in North Carolina. “No one in the United States of America should ever be targeted because of who they are, what they look like, or how they worship,” the president said, offering his condolences to the families of the slain. Though community leaders have noted that CVE programs do not target white supremacists or call atheist organizations in for dialogue, Ned Price, a spokesman for the National Security Council, said next week’s summit will not single out Muslims. “While the summit will address contemporary challenges, it will not focus on any particular religion, ideology, or political movement and will, instead, seek to draw lessons that are applicable to the full spectrum of violent extremists,” Price said.

CVE doesn’t solve for terror – flawed theories of radicalization

German 2/19 --- Michael German is a fellow with the Brennan Center for Justice’s Liberty and National Security Program, which seeks to ensure that our government respects human rights and fundamental freedoms in conducting the fight against terrorism. (Michael German, 2-19-2015, "Counterterrorism Efforts Should Be Based on Facts, Not Flawed Theories," Brennan Center, <https://www.brennancenter.org/analysis/counterterrorism-efforts-should-be-based-facts-not-flawed-theories>//A-Sharma

This week, the White House held a three-day summit to discuss a recently announced domestic counterterrorism program, dubbed “Countering Violent Extremism” (CVE). These programs, which are slated to launch in Boston, Minneapolis, and Los Angeles in the months ahead, aim to help communities identify violent extremists in the United States. The summit is part of the Administration’s renewed effort to position its outreach programs to Muslim American communities as part of a larger anti-terrorism campaign. But if these programs are anything like past iterations, they are likely to create more problems than they solve. One major problem is that although the 2011 White House CVE strategy recognizes that violent extremists come from many ideological backgrounds, which we saw last year in Las Vegas and Kansas City, the actual programs tend to target only Muslim Americans. This solitary focus tends to stigmatize, rather than empower Muslim communities. I spoke with NYU professor Arun Kundnani, author of The Muslims are Coming! Islamophobia, Extremism, and the Domestic War on Terror, who has studied CVE programs in both Britain and the U.S. He explains how tying outreach programs to an anti-terrorism purpose tends to reinforce the perception that the government views Muslim communities primarily as a potential security threat, rather than a constituency government is obligated to serve in a fair and equal manner: The Brennan Center and the American Civil Liberties Union have uncovered ample evidence that the government has previously viewed its community outreach programs to Muslim groups as an opportunity to secretly gather intelligence. A 2014 National Counterterrorism Center document published by The Intercept suggests it plans to use CVE programs to evaluate communities, families, and individuals for their potential to become terrorists. The document, a CVE guide for practitioners and analysts, includes a five-page checklist for police officers, public health workers, educators, and social service departments to rate “risk and resilience factors” of the public they serve on a five-point scale. The risk factors NCTC suggests include whether there was empathetic parent-child bonding and whether family members trust each other, experienced loss, or perceive being treated unjustly. Communities are to be rated on whether they face discrimination by or show trust in law enforcement. There’s little evidentiary basis to believe these factors are relevant to whether a person becomes violent, let alone that lay persons could accurately rate them on a five-point scale. But it is also ironic that individuals and communities that already face discrimination are considered a higher risk, which could potentially lead to their further targeting for disparate treatment from law enforcement and intelligence agencies. There’s no question that innocent American Muslims have suffered from over-aggressive surveillance, unjustified interference with their religious and political activities, and unnecessary impediments to their travel. Hina Shamsi, Director of the ACLU’s National Security Project, talked to me about the impact this misplaced scrutiny has on Muslim communities: This highlights one glaring disconnect in the government’s CVE strategy. The flawed theories of terrorist radicalization the CVE programs rely on tend to identify individual or community grievances as a primary indicators or drivers of

violence. A recent White House CVE strategy memo, however, recognizes that government activities themselves can generate grievances: ... We must remember that just as our words and deeds can either fuel or counter violent ideologies abroad, so too can they here at home. Actions and statements that cast suspicion toward entire communities, promote hatred and division, and send messages to certain Americans that they are somehow less American because of their faith or how they look, reinforce violent extremist propaganda and feed the sense of disenchantment and disenfranchisement that may spur violent extremist radicalization. But rather than implement a strategy that evaluates the relative legitimacy of these grievances so the government can take action to mitigate them as appropriate, the government's CVE programs attempt to suppress this debate by recruiting community leaders willing to promote pro-government messaging. Identifying past discrimination against these communities as one more reason to continue discriminating against them isn't the answer. Treating terrorism as the spread of an ideological infection within a vulnerable community also allows the government to put aside difficult questions about the role US foreign and national security policies play in generating anti-American grievances, which the Defense Department raised in a 2004 report. Studies supporting government-favored radicalization theories rarely mention U.S. military actions in Muslim countries, lethal drone strikes, torture, or the Guantanamo Bay prison as radicalizing influences, though many terrorists reference them in attempting to justify their actions. The intelligence agencies should be leading the government in fact-based research on national security issues. Peddling debunked radicalization theories that spread unnecessary fear and confusion will only lead to more discrimination and distrust of government. This would be an unfortunate outcome, whether you believe it leads to more terrorism or not.

Hacking encryption turn

Encryption cracking opens access to unintended consequences, terrorism, loss of soft power, and stops tech company innovation

Weitzner July 7th,

(Daniel Weitzner is the Director of the MIT CSAIL Decentralized Information Group and teaches Internet public policy in MIT's Computer Science Department. His research includes development of accountable systems architectures to enable the Web to be more responsive to policy requirements, former US Deputy Chief Technology Officer for Internet Policy in the White House. led initiatives on privacy, cybersecurity, Internet copyright, and trade policies promoting the free flow of information, "Encryption 'backdoors' will open for criminals as well as governments: experts", <http://www.timeslive.co.za/scitech/2015/07/07/Encryption-backdoors-will-open-for-criminals-as-well-as-governments-experts>, TMP)

A research report published by the Massachusetts Institute of Technology challenges claims from US and British authorities that such access is the policy response needed to fight crime and terrorism. Providing this kind of access "will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend," said the report by 13 scientists. The paper was released a day after FBI Director James Comey called for public debate on the use of encrypted communications, saying Americans may not realize how radical groups and criminals are using the technology. Comey argued in a blog post that Islamic State militants are among those using encryption to avoid detection. The New York Times, which reported earlier on the study, said Comey was expected to renew a call at a congressional hearing for better access to encrypted communications to avoid "going dark." The computer scientists said, however, that any effort to build in access for law enforcement could be exceedingly complex and lead to "unintended consequences," such as stifling innovation and creating hostility toward new tech products. "The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict," the report said. "The costs to developed countries' soft power and to our moral authority would also be considerable." In the 1990s, there was a similar debate on the "clipper chip" proposal to allow "a trusted third party" to have access to encrypted messages that could be granted under a legal process. The clipper chip idea was abandoned, but the authors said that if it had been widely adopted, "it is doubtful that companies like Facebook and Twitter would even exist." The computer scientists said the idea of special access would create numerous technical and legal challenges, leaving unclear who would have access and who would set standards. "The greatest impediment to exceptional access may be jurisdiction," the report said. "Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it." The British government is considering legislation to compel communications service providers, including US-based corporations, to grant access to British law enforcement agencies. "China has already intimated that it may require exceptional access," the report said. "If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement?" Among the report's authors are Daniel Weitzner, director of the MIT Computer Science and Artificial Intelligence Laboratory, and well-known MIT cryptographer Ronald Rivest.

Privacy Key To Free Speech

Intellectual privacy is essential to free speech and free expression.

Richards 8 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2008 (“Intellectual Privacy,” *Texas Law Review* (87 Tex. L. Rev. 387), December, Available Online to Subscribing Institutions via Lexis-Nexis)

It is unfortunate that the principal theories of the First Amendment have failed to treat intellectual privacy as an important First Amendment value. This deficiency is a critical one, because meaningful freedom of speech requires meaningful intellectual privacy. To illustrate this point, imagine a system of free speech law that is deeply protective of the act of speaking, but which has little protection for the act of thinking. Under a system like this, people could speak freely on a whole host of controversial issues, and could engage in widespread obscene, racist, libelous, or inciting speech. Current theory would consider such a regime to be deeply speech-protective. n95 But if this system had little protection for intellectual privacy, the government would be free to secretly monitor phone calls, Internet usage, and the movements and associations of individuals. Private industry would also be relatively unconstrained in its ability to participate in a market for the same information. Such a world would have plenty of speech but little privacy; indeed, some observers have predicted that this is the future of our online world and, by extension, the expressive topography of our society as a whole. n96

A regime that protected speech but not thoughts would be deeply problematic, to say the least. In a world of widespread public and private scrutiny, novel but unpopular ideas would have little room to breathe. Much could be said, but it would rarely be new, because original ideas would have no refuge in which to develop, save perhaps in the minds of hermits. Such a world has in the past been the domain of writers of speculative and science fiction, n97 but it should be no less familiar as a result. Indeed, the word "Orwellian" strikes with deep resonance in this context. n98 Moreover, as many scholars have argued, surveillance has a deep effect on the actions of the subject. n99 The knowledge that others are watching (or may be watching) tends the preference of the individual towards the bland and the [*404] mainstream. n100 Thoroughgoing surveillance, whether by public or private actors, has a normalizing and stifling effect. n101

Intellectual privacy creates a screen against such surveillance. As the English philosopher Timothy Macklem has argued, "The isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and subversive." n102 When there is protection from surveillance, new ideas can be entertained, even when they might be deeply subversive or threatening to conventional or orthodox views. If we value a pluralistic society or the cognitive processes that produce new ideas, then some measure of intellectual privacy, some respite from cognitive surveillance, is essential. Any meaningful freedom of speech requires an underlying culture of vibrant intellectual innovation. Intellectual privacy nurtures that innovation, protecting the engine of expression - the imagination of the human mind. n103 To the extent that orthodox First Amendment theory is underprotective of intellectual privacy, we must rehabilitate it to take account of these vital norms.

Privacy Key To Other Rights

Intellectual privacy is the basis for all other political and religious rights.

Richards 8 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2008 (“Intellectual Privacy,” *Texas Law Review* (87 Tex. L. Rev. 387), December, Available Online to Subscribing Institutions via Lexis-Nexis)

The core of intellectual privacy is the freedom of thought and belief. The freedom to think and to believe as we want is arguably the defining characteristic of a free society and our most cherished civil liberty. n118 This right encompasses the range of thoughts and beliefs that a person might hold or develop, dealing with matters that are trivial and important, secular and profane. And it protects the individual's thoughts from scrutiny or unwilling disclosure by anyone, whether a government official or a private actor such as an employer, a friend, or a spouse. At the level of law, if there is any constitutional right that is absolute, it is this one, which is the precondition for all other political and religious rights guaranteed by the Western tradition.

Surveillance Bad - Liberty

Government Surveillance risks total invasion of liberty.

Schneier 2015

Bruce Schneier a fellow at the Berkman Center for Internet and Society at Harvard Law School, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the CTO at Resilient Systems, 3/2/15, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, p, 90

Government surveillance is costly. Most obviously, it's extraordinarily expensive: \$72 billion a year in the US. But it's also costly to our society, both domestically and internationally. Harvard law professor Yochai Benkler likens NSA surveillance to an autoimmune disease, because it attacks all of our other systems. It's a good analogy. The biggest cost is liberty, and the risk is real enough that people across political ideologies are objecting to the sheer invasiveness and pervasiveness of the surveillance system. Even the politically conservative and probusiness Economist magazine argued, in a 2013 editorial about video surveillance, that it had gone too far: "This is where one of this newspaper's strongly held beliefs that technological progress should generally be welcomed, not feared, runs up against an even deeper impulse, in favour of liberty. Freedom has to include some right to privacy: if every move you make is being chronicled, liberty is curtailed." ACCUSATION BY DATA In the 17th century, the French statesman Cardinal Richelieu famously said, "Show me six lines written by the most honest man in the world, and I will find enough therein to hang him. Lavrentiy Beria, head of Joseph Stalin's secret police in the old Soviet Union, declared, "Show me the man, and I'll show you the crime." Both were saying the same thing: if you have enough data about someone, you can find sufficient evidence to find him guilty of something. It's the reason many countries' courts prohibit the police from engaging in "fishing expeditions." It's the reason the US Constitution specifically prohibits general warrants documents that basically allow the police to search for anything. General warrants can be extremely abusive; they were used by the British in colonial America as a form of social control. Ubiquitous surveillance means that anyone could be convicted of lawbreaking, once the police set their minds to it. It is incredibly dangerous to live in a world where everything you do can be stored and brought forward as evidence against you at some later date. There is significant danger in allowing the police to dig into these large data sets and find "evidence" of wrongdoing, especially in a country like the US with so many vague and punitive laws, which give prosecutors discretion over whom to charge with what, and with overly broad material witness laws. This is especially true given the expansion of the legally loaded terms "terrorism," to include conventional criminals, and "weapons of mass destruction," to include almost anything, including a sawed-off shotgun. The US terminology is so broad that someone who donates \$10 to Hamas's humanitarian arm could be considered a terrorist. Surveillance puts us at risk of abuses by those in power, even if we're doing nothing wrong at the time of surveillance. The definition of "wrong" is often arbitrary, and can quickly change. For example, in the US in the 1930s, being a Communist or Socialist was a bit of an intellectual fad, and not considered wrong among the educated classes. In the 1950s, that changed dramatically with the witch-hunts of Senator Joseph McCarthy, when many intelligent, principled American citizens found their careers destroyed once their political history was publicly disclosed. Is someone's reading of Occupy, Tea Party, animal rights, or gun rights websites going to become evidence of subversion in five to ten years?

Surveillance threatens human freedom and dignity.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed. This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

Lack of privacy destroys liberty — important to preserve rights

Schell, 2013

Jonathan Schell, Lannan Fellow at The Nation Institute and Instructor at Yale, 6-19-2013,
"America's Surveillance Net," The Nation, <http://www.thenation.com/article/174889/americas-surveillance-net>

A school of fish swims peacefully in the ocean. Out of sight, a net is spread beneath it. At the edges of the net is a circle of fishing boats. Suddenly, the fishermen yank up the edges of the net, and in an instant the calm, open ocean becomes a boiling caldron, an exitless, rapidly shrinking prison in which the fish thrash in vain for freedom and life. Increasingly, the American people are like this school of fish in the moments before the net is pulled up. The net in question is of course the Internet and associated instruments of data collection, and the fishermen are corporations and the government. That is, to use the more common metaphor, we have come to live alongside the machinery of a turnkey tyranny. As we now know, thanks to the courageous whistleblower Edward Snowden, the National Security Agency has been secretly ordering Verizon to sweep up and hand over all the metadata from the phone calls of millions of its customers: phone numbers, duration of calls, routing information and sometimes the location of the callers. Thanks to Snowden, we also know that unknown volumes of like information are being extracted from Internet and computer companies, including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The first thing to note about these data is that a mere generation ago, they did not exist. They are a new power in our midst, flowing from new technology, waiting to be picked up; and power, as always, creates temptation, especially for the already powerful. Our cellphones track our whereabouts. Our communications pass through centralized servers and are saved and kept for a potential eternity in storage banks, from which they can be recovered and examined. Our purchases and contacts and illnesses and entertainments are tracked and agglomerated. If we are arrested, even our DNA can be taken and stored by the state. Today, alongside each one of us, there exists a second, electronic self, created in part by us, in part by others. This other self has become de facto public property, owned chiefly by immense data-crunching corporations, which use it for commercial purposes. Now government is reaching its hand into those corporations for its own purposes, creating a brand-new domain of the state-corporate complex. Surveillance of people on this scale turns basic liberties—above all the Fourth Amendment, which protects citizens against unreasonable search and seizure—into a dead letter. Government officials, it is true, assure us that they will never pull the edges of the net tight. They tell us that although they could know everything about us, they won't decide to. They'll let the

information sit unexamined in the electronic vaults. But history, whether of our country or others, teaches that only a fool would place faith in such assurances. What one president refrains from doing the next will do; what is left undone in peacetime is done when a crisis comes.

Privacy good - Autonomy

Privacy links rational agency and moral autonomy.

Magi, 2011

Trina J. Librarian, University of Vermont, Burlington. "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature1." *The Library* 81.2 (2011).

Gavison admits that there have always been some autonomous individuals in totalitarian societies, and therefore privacy may not be necessary for autonomy. But she says the fact that most people require privacy is enough to justify it as a value, because "we are not all giants, and societies should enable all, not only the exceptional, to seek moral autonomy" [16, p. 450]. Charles Fried describes a "most basic" form of complete privacy in which privacy serves not to protect things we will share only with friends but to protect certain thoughts from the whole world. Although the sharing of certain thoughts with a lover or friend, he says, would be a "hostile act," the thinking of those thoughts is completely consistent with friendship and love because "these thoughts, prior to being given expression, are mere unratified possibilities for action" [29, p. 485]. Only when we express thoughts do we adopt them and choose to make them part of ourselves, he says, and this is why privacy is essential to the freedom to define ourselves. Julie Inness also talks about privacy providing a sphere of autonomy in which a person can develop a self-concept as an originator of love, liking, and care [30, p. 107]. In their theory of privacy as a fundamental moral right, Alfino and Mayes contend that a person requires personal space in order to reason about his/her choices, that reasoning activity is what links rational agency and moral autonomy, and that to deprive a person of her ability to reason is to fundamentally interfere with a person's capacity for self-government. According to this framework, privacy is "the condition of having secured one's personal space, by which we mean the right to exercise our practical reason without undue interference from others" [18]

Privacy is critical to personal moral autonomy.

Corlett, 2002

J. Angelo. Professor Corlett is a philosopher specializing in ethics and epistemology at San Diego State University "The nature and value of the moral right to privacy." *Public Affairs Quarterly* (2002): 329-350.

Privacy, moreover, can insulate one from being treated as a mere means to the end of, say, social utility, where private objectives tend to be devalued. It is based on the Kantian principle of respect for persons.⁴⁵ Privacy enables us to pursue our projects because they are ours, because they have value for us. Construed in this way, the moral right to privacy may be seen as a concern for moral autonomy.⁴⁶ Furthermore, privacy is necessary for persons to create, develop, and sustain intimacy with others.⁴⁷ It is connected to basic ends and relations such as respect, love, friendship, and trust.⁴⁸ As Thomas Nagel argues, "The boundary between what we reveal and what we do not, and some control over that boundary, are among the most important attributes of our humanity."⁴⁹ And as Frederick Schauer argues, not even public figures, elected or otherwise, ought to be expected to forgo their essential privacy.⁵⁰ To argue thusly is to insist on the essential moral (though non-absolute) right to privacy, a right which is only the moral agent's to waive as she sees fit. To the extent that the balance of reason secures the importance of these factors for human life, these factors serve as moral grounds for the need to respect privacy by moral right. Indeed, among other things, a well-ordered society ought to foster a reasonable culture of privacy. But this is possible only where there is a clear idea, not only of the nature and value of privacy as a moral right, but also of the scope of that right.

Privacy good - Individuality

Violations of privacy eliminate autonomy and individuality.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

To say that one has a moral right to privacy means that one has a morally justified claim or interest that others not gain access to one's personal information without one's informed consent; and this right can be said to be violated or abridged when others manage to gain such access. Further, the moral right to privacy derives from a more general right of self-determination, that is, the liberty or freedom to choose for oneself in matters concerning what is one's own, such as one's personal possessions or property, or one's own life—provided, of course, one is a competent adult. Thus, one has such a right to dispose of personal information in any way one sees fit inasmuch as such information is one's own. This general moral right of self-determination also has legal standing pursuant to the US Constitution. It is enshrined in the Fourteenth Amendment, which holds that no state shall "deprive any person of life, liberty, or property, without due process of law," and the same language is repeated in the Fifth Amendment. The First Amendment holds that "Congress shall make no law ... abridging the freedom of speech, or of the press ..." But, clearly, without a sphere of privacy in which to speak freely without the government listening, or of the press to gather news without the government eavesdropping on its sources, there can be no protected legal right to free speech, or a free press. Again, the Fourth Amendment recognizes "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures ..." Here is where the Constitution makes clear that the government will, in no case, violate one's personal space without a warrant based on probable cause. In *Olmstead v. U.S.* (1928), Justice Brandeis famously expressed, The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality—the right to be left alone—the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.¹ The "privacies of life" are, in Justice Brandeis' words, at the core of "man's spiritual nature, his feelings, and his intellect." Foreclose this area of protected freedom or autonomy to be oneself in the privacy of one's home, or to dispose of one's personal information as one sees fit, and one's very personhood and individuality—one's unique spiritual nature, feelings, and intellect—is chilled off. The quality of human dignity lies in the respect owed to persons by virtue of their ability to navigate their own ship of life. Dismantle this private sphere of freedom by refusing to leave people alone and an essential condition of their dignity—the ability to freely think and act—is also imperiled.

Privacy is central to personal liberty and individuality, violations turn individuals into statistics, the courts have an obligation to solve

Mills 08 — Jon L. Mills, B.A. from Stetson University in 1969. He went on to the University Of Florida College Of Law where he graduated second overall in 1972. While at the Levin College of Law he served on the Florida Law Review, and was a member of Florida Blue Key. Before Mills became the Dean (education) of the Levin College of Law he served as a Professor at the University of Florida in 1995, 2008 (*Privacy: The Lost Right*, ISBN: 978-0195367355, Oxford University Press, Accessed On 7-16-15, pg. 305-306)

Privacy, as a central part of personal liberty and individuality, is a touchstone of American democracy and a generally accepted, yet amorphous, global right. A combination of forces from the government, an intrusive society, commercial interests, and segments of the press are, in effect, crushing the individual's right to be let alone. If they were concerned about an intrusive world in 1890, what might Warren and Brandeis think today? In 2008, the

law is ill equipped to protect citizens from the private and public assault on their privacy. This onslaught is not the result of some grand conspiracy. No conspiracy could work so well. In fact, the government, the information industry, and the press are, at least on the surface, doing what the public demands: they are providing security, needed information, and the news and gossip that the public wants. The status of our collective privacy is unpredictable, inconsistent and changing continually—a reflection of a society with changing mores and changing technology. The confluence of technology and the motivations of data brokers are causing the individual to be treated more and more as a statistic. The threshold question is, do we care? Well, we do when we are hurt. We care when the government dictates that a loved one must die painfully. We care when we are crime victims scrutinized by the press. We care when we do not get a job because of inaccurate criminal records. As part of today's culture and society, no individual is immune. As suggested in the introduction, there are very few private aspects of a "day in the life" of a modern citizen. Further, as this book has made clear, the legal solutions are piecemeal and incremental, requiring the public to demand remedies for violations of their right to privacy. The impact is so vast and comprehensive that no one ethnic, religious, or other group is singled out. We are all part of the privacy interest group. So far, most of us are underinformed as to what is happening to us and are largely unaware of any effective legal remedies. However, there are legal remedies for privacy violations. And, if the privacy right is important, the courts have an obligation to fashion effective options from the myriad remedies. There will be no single sweeping reform that will bestow privacy on each of us. The forces and policies that support intrusions on individual privacy are too substantial and in some cases, are supported by most of the public. For example, most of the public supports warrantless searches and constant camera surveillance to counter violence and terrorism. Likewise, most of the public shows a voyeuristic interest in tabloids and disaster journalism, at least until someone in their own family becomes an unwilling subject. This most individual of rights requires our personal commitment to protect ourselves through our personal choices and actions and our advocacy. The central lessons of a study of privacy today are as follows: • No universal agreement exists on the scope of privacy because of inherent moral, political, and perceptual differences. • Privacy is a broad concept affecting multiple facets of human existence that individuals and governments value as a general principle. • A single policy is not probable or practical to protect privacy across the globe or even across the country. • A broader understanding of the scope of privacy (i.e., recognizing which issues are important to individual liberty) is a prerequisite for protecting individual privacy.

Privacy is akin to liberty — it is important in our daily lives and it is essential for the government to preserve it

Gavison 12 — Ruth E. Gavison, Professor of Human Rights Law at Hebrew University Law Faculty. Born in Jerusalem. Received an LLB (cum laude) in 1969, LLM (summa cum laude) in 1971, and BA in economics and philosophy (1970), all from Hebrew University. Law clerk at the Israel Supreme Court (Justice Benjamin Halevi). Admitted to the Israeli bar in 1971. In 1975 she received a D.Phil. in legal philosophy from Oxford University, 2012 ("Privacy and the Limits of Law," *Yale Law Journal*, Vol 28 No. 3, Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957, Accessed on 7-15-15)

In positive terms, the case for an explicit commitment to privacy is made by pointing out the distinctive functions of privacy in our lives. Privacy has as much coherence and attractiveness as other values to which we have made a clear commitment, such as liberty. Arguments for liberty, when examined carefully, are vulnerable to objections similar to the arguments we have examined for privacy, yet this vulnerability has never been considered a reason not to acknowledge the importance of liberty, or not to express this importance by an explicit commitment so that any loss will be more likely to be noticed and taken into consideration. Privacy deserves no less. Further insight about the need for an explicit commitment to privacy comes from study of the arguments made against this approach. First, it may be argued that the American legal system has already made this commitment, and that we should concentrate on answering questions of the scope of legal protection rather than spend time arguing for commitments that have already been made. Questions of scope are no doubt important, and had a commitment to privacy been made and its implications internalized, there would indeed be no further need for an explicit affirmation. But the reductionist literature is at least as influential as that which affirms the distinctness and importance of privacy, and although it is true that some parts of the legal system are informed by an

affirmation of privacy, it is equally clear that others are not. For the latter, an explicit commitment to privacy could make an important difference.

Privacy good – Self Determination

Privacy critical for personal agency.

Richards, 2015, Neil M., Professor of Law, Washington University. “Four Privacy Myths” Revised form, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2427808>

A second reason why the “Nothing to Hide” argument is misleading is that it reduces privacy to an individual’s right to hide big secrets. Such a crude reduction of the issue ignores both the complexity of privacy, as well as the social value that comes from living in a society that not everything about us is publicly available all of the time. This is the insight of legal scholar Daniel Solove in his book “Nothing to Hide.” Solove shows how thinking of privacy as the hiding of discreditable secrets by individuals is a mistake because privacy is about more than hiding secrets, and can mean a wide variety of things. Moreover, he notes that “privacy is “often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone.”⁶⁴ Privacy, in this view, is a social value rather than merely an individual one. Rather than thinking about privacy as merely the individual right to hide bad deeds, we should think more broadly about the kind of society we want to live in. A society in which everyone knew everything about everyone else would be oppressive because it would place us all under the glare of publicity all the time; there would be no “free zones for individuals to flourish.”⁶⁵ Legal scholar Julie Cohen goes further, arguing that privacy is necessary for humans to be able to decide who they are. In Cohen’s account, our selves are fluid, constantly being built and changed by our activities, thoughts, and interactions with other people. Privacy, in her view, shelters the development of our dynamic selves “from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable.” Privacy protects our ability to manage boundaries between ourselves and others so that self-determination is possible.⁶⁶ It helps us avoid the calculating, quantifying tyranny of the majority. Privacy is thus essential for individuality and self-determination, with substantial benefits for society.

Privacy Good – Democracy

Privacy is a prerequisite to democracy

Michael **McFarland**, [a computer scientist with extensive liberal arts teaching experience and a special interest in the intersection of technology and ethics, served as the 31st president of the College of the Holy Cross.], June **2012**

"Why We Care about Privacy", Online:

<http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Privacy is even more necessary as a safeguard of freedom in the relationships between individuals and groups. As Alan Westin has pointed out, surveillance and publicity are powerful instruments of social control.⁸ If individuals know that their actions and dispositions are constantly being observed, commented on and criticized, they find it much harder to do anything that deviates from accepted social behavior. There does not even have to be an explicit threat of retaliation. "Visibility itself provides a powerful method of enforcing norms."⁹ Most people are afraid to stand apart, to be different, if it means being subject to piercing scrutiny. The "deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."¹⁰ Under these circumstances they find it better simply to conform. This is the situation characterized in George Orwell's 1984 where the pervasive surveillance of "Big Brother" was enough to keep most citizens under rigid control.¹¹ Therefore privacy, as protection from excessive scrutiny, is necessary if individuals are to be free to be themselves. Everyone needs some room to break social norms, to engage in small "permissible deviations" that help define a person's individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves. As Brian Stelter wrote in the New York Times on the loss of anonymity in today's online world, "The collective intelligence of the Internet's two billion users, and the digital fingerprints that so many users leave on Web sites, combine to make it more and more likely that every embarrassing video, every intimate photo, and every indecent e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view."¹² This ability to develop one's unique individuality is especially important in a democracy, which values and depends on creativity, nonconformism and the free interchange of diverse ideas. That is where a democracy gets its vitality. Thus, as Westin has observed, "Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life."¹³ When Brandeis and Warren wrote their seminal article on privacy over one hundred years ago, their primary concern was with the social pressure caused by excessive exposure to public scrutiny of the private affairs of individuals. The problem for them was the popular press, which represented the "monolithic, impersonal and value-free forces of modern society,"¹⁴ undermining the traditional values of rural society, which had been nurtured and protected by local institutions such as family, church and other associations. The exposure of the affairs of the well-bred to the curiosity of the masses, Brandeis and Warren feared, had a leveling effect which undermined what was noble and virtuous in society, replacing it with the base and the trivial. Even apparently harmless gossip, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.... Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.¹⁵ For Brandeis and Warren, privacy was a means of protecting the freedom of the virtuous to maintain their values against the corrupting influence of the mass media that catered to people's basest instincts. Although the degrading effect of the mass media is still a problem, today a more serious threat to

freedom comes from governments and other large institutions. Over the last century, governments have developed sophisticated methods of surveillance as a means of controlling their subjects. This is especially true of totalitarian states, as the passage from Westin quoted above indicates. The Soviet Union, Communist China, Nazi Germany, Fascist Italy and white-run South Africa all used covert and overt observation, interrogation, eavesdropping, reporting by neighbors and other means of data collection to convince their subjects that independent, "antisocial" thought, speech and behavior was unacceptable. In many cases the mere presence of the surveillance was enough to keep people in line. Where it was not, the data collected was used to identify, round up and punish elements of the population that were deemed dangerous. For example, Ignazio Silone, in his book Bread and Wine, described the use of surveillance in Fascist Italy in this way: It is well-known [says Minorca] that the police have their informers in every section of every big factory, in every bank, in every big office. In every block of flats the porter is, by law, a stool pigeon for the police.... This state of affairs spreads suspicion and distrust throughout all classes of the population. On this degradation of man into a frightened animal, who quivers with fear and hates his neighbor in his fear, and watches him, betrays him, sells him, and then lives in fear of discovery, the dictatorship is based. The real organization on which the system in this country is based is the secret manipulation of fear. 16 While totalitarian regimes may not seem as powerful or as sinister as they did 50 years ago, surveillance is still used in many places as an instrument of oppression. For example Philip Zimmerman, the author of the PGP (Pretty Good Privacy) data encryption program, reports receiving a letter from a human rights activist in the former Yugoslavia that contained the following testimonial: We are part of a network of not-for-profit agencies, working among other things for human rights in the Balkans. Our various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and our office in Romania has a constant wiretap. Last year in Zagreb, the security police raided our office and confiscated our computers in the hope of retrieving information about the identity of people who had complained about their activities. Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients. 17 More recently social media and the Internet played major roles in the "Arab Spring" uprisings in the Middle East, causing Egypt and Libya to shut down the Internet in their countries in an attempt to stifle dissent. 18 In China there has been an ongoing battle between the government and activist groups over government monitoring and censorship of the Internet. 19 Even in a democracy, there is always the danger that surveillance can be used as a means of control. In the United States, for example, where freedom is such an important part of the national ethos, the FBI, the CIA, the National Security Agency (NSA) and the armed forces have frequently kept dossiers on dissidents. The NSA from 1952 to 1974 kept files on about 75,000 Americans, including civil rights and antiwar activists, and even members of Congress. During the Vietnam war, the CIA's Operation Chaos collected data on over 300,000 Americans. 20 Since then the NSA has had an ongoing program to monitor electronic communications, both in the U.S. and abroad, which has led to constant battles with individuals and groups who have sought to protect the privacy of those communications through encryption and other technologies. 21 Some of the most famous incidents of surveillance of dissidents, of course, occurred during the Nixon administration in the early 1970s. For example, when Daniel Ellsberg was suspected of leaking the Pentagon Papers, an internal critique of government conduct of the Vietnam war, Nixon's agents broke into the office of Ellsberg's psychiatrist and stole his records. 22 And it was a bungled attempt at surveillance of Nixon's political opposition, as well as illegal use of tax returns from the IRS, that ultimately brought down the Nixon administration. 23 More recently, during the 1996 presidential campaign, it was revealed that the Clinton White House had access to the FBI investigative records of over 300 Republicans who had served in the Reagan and Bush administrations. The Clinton administration claimed it was all a mistake caused by using an out-of-date list of White House staff, while the challenger Bob Dole accused them of compiling an "enemies list." >sup>24 Whatever the motivation, the head of the FBI termed the use of the files "egregious violations of privacy." 25 Since the 9/11 terrorist attacks in 2001, there has been even greater urgency in the government's efforts to monitor the activities and communications of people, both foreigners and its own citizens, in order to identify and prevent terrorist threats. The Patriot Act, passed less than two months after 9/11, greatly expanded the government's authority to intercept electronic communications, such as emails and phone calls, including those of U.S. citizens. As a result government agencies have been building the technological and organizational capabilities to monitor the activities and communications of their own citizens. For example, Wired magazine revealed in a recent report how the National Security Agency has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created. In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it's all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever. 26 The FBI, the Drug Enforcement Agency and the Department of Homeland Security also have many programs to monitor citizens in general, not just those who are under suspicion. These efforts include sifting through media references, 27 tracking chatter on social networks, 28 and monitoring peoples' movements through license plate scanners 29 and video cameras. 30 The mere knowledge that American citizens could be the subjects of surveillance can in itself have a chilling effect on political freedom. "Now it is much more difficult than it once was to dismiss the possibility that one's phone is being tapped, or that one's tax returns may be used for unfriendly political purposes, or that one's life has become

the subject of a CIA file. The realization that these activities might take place, whether they really do or not in any particular instance, has potentially destructive effects on the openness of social systems to innovation and dissent." 31 At times the government in the United States has gone beyond surveillance and intimidation and has used the data gathered as a basis for overt oppression. One of the most blatant examples is the internment of over 100,000 Japanese Americans, most of them American citizens, during World War II. The Justice Department used data from the Census Bureau to identify residential areas where there were large concentrations of Japanese Americans, and the army was sent in to round them up. They were taken away from their homes and held in concentration camps for the duration of the war. 32 Governments do need information, including personal information, to govern effectively and to protect the security of their citizens. But citizens also need protection from the overzealous or malicious use of that information, especially by governments that, in this age, have enormous bureaucratic and technological power to gather and use the information.

Privacy key to democracy, creates autonomous subjects.

Maras, 2012

Marie-Helen. Criminal Justice, State University of New York, "The social consequences of a mass surveillance measure: What happens when we become the 'others'?" International Journal of Law, Crime and Justice 40.2 (2012): 65-81.

The very foundation of a democratic society depends on citizens who are able to formulate plans for their lives, take actions and make their decisions free from coercion (Loader and Walker, 2007: 225–226). Indeed, the justification for the majority rule and the right to vote in a democratic society is based on the assumption that the individual from their own judgement can express their own preferences (free from coercion) while participating in political decisions (Gavison, 1980: 455). Therefore, individuals' autonomy should not be considered the antithesis of political power but key factors in its exercise since subjects play an important part in its operations (Rose and Miller, 1992: 174). Privacy is thus essential to a democratic government because it fosters and encourages the autonomy of its citizens, which itself is a central requirement for democracy (Gavison, 1980: 455). Constant observation transforms the self from a subject to an object and the uncertainty of this mass surveillance makes the development of the self nearly impossible because the self "cannot develop its individual subjectivity...without insulation from the gaze of pervasive surveillance" (Rosen, 2001: 220). Individuals who are constantly subjected to scrutiny will lose their uniqueness, autonomy, and their sense of self; in short, they will lose their individual personality (Schoeman, 1984: 19). Accordingly, with individuals under constant surveillance, their "opinions, being public, tend never to be different" and their "aspirations, being known, tend always to be conventionally accepted ones"; such a being, however, is not an individual (Bloustein, 1984: 189). Goffman (1959: 63) similarly observes that if everyone is constantly censoring their thought processes, the result will be socially acceptable behaviour (whatever this may be) "which nevertheless in no way approximates an accumulation of the kinds of behaviour which come most naturally". What occurs as a result is the replacement of the 'I' with the 'me'; thus preventing the development of the individual subjective self.

Privacy key to autonomy and democratic collaboration

Schwartz, 99- Professor of Law at Brooklyn Law School, (Paul, "Privacy and Democracy in Cyberspace", 52 Vand. Law Review, Vol 52: 1609, 1999, PDF, page 1652-1655)//AP

Beyond democratic deliberation, information use in cyberspace poses an important threat to a second value necessary for life in a democracy. Here, one must go beyond existing civic republican thought, which is largely focused on the group, and consider the individual. Decision making in a democracy takes place not only within a given community, but also within individuals who, at any time, are anchored in a variety of social settings.²⁷⁴ The health of a democratic society depends both on the group-oriented process of democratic deliberation and the functioning of each person's capacity for selfgovernance.²⁷⁵ This Article will therefore supplement the idea of democratic deliberation by elaborating a principle of individual self-determination. It will first define this concept and then explore the threat to it posed by current information processing in cyberspace. The argument is that without the right kind of privacy rules, the potential of cyberspace for promoting self-governance will be lost. The fashion in which society and law insulate certain acts and places from data collection affects the process of development of identity. The need is to insulate an individual's reflective facilities from certain forms of manipulation and coercion. Privacy rules for cyberspace must set aside areas of limited access to personal data in order to allow individuals, alone and in association with others, to deliberate about how to live their lives. This Article will therefore supplement the idea of democratic deliberation by elaborating a principle of individual self-determination. It will first define this concept and then explore the threat to it posed by current information processing in cyberspace. The argument is that without the right kind of privacy rules, the potential of cyberspace for promoting self-governance will be lost. The fashion in which society and law insulate certain acts and places from data collection affects the process of development of identity. The need is to insulate an individual's reflective facilities from certain forms of manipulation and coercion. Privacy rules for cyberspace must set aside areas of limited access to personal data in order to allow individuals, alone and in association with others, to deliberate about how to live their lives. This Section begins by returning again, briefly, to civic republicanism. Although civil republican theory does not elaborate a detailed concept of individual self-determination, this Article's attention to autonomy is compatible with this strain of political thought. For example, Michael Sandel has noted that self-government today requires development of a capacity to participate in politics in a multiplicity of settings.²⁷⁶ He argues, “[t]he civic virtue distinctive to our time is the capacity to negotiate our way among the sometimes overlapping, sometimes conflicting obligations that claim us, and to live with the tension to which multiple loyalties give rise.”²⁷⁷ Despite Sandel's insight on this point, neither he nor other civic republicans identify the precise ability needed to fulfill these negotiations and the external programmatic structure essential to nurture this ability.²⁷⁸ This absence represents a considerable flaw in the civic republican project. Civic republicanism must undergird its existing concept of democratic deliberation with a foundation based on an individual's capacity for critical reflection. Outside of this movement, an important corrective attempt is already underway. James E. Fleming has argued, for example, that democracy in general and constitutional law in particular must secure the preconditions for “citizens to apply their capacity for a conception of the good to deliberat[ions] about . . . how to live their own lives.”²⁷⁹ His call is for a deliberative autonomy that is the locus of moral agency, responsibility, and independence. This quality involves both decisionmaking internal to the individual and a person's consulting with others, taking their views into account, and associating with them. From this perspective, democracy requires more than group deliberation at a town square located either in Real Space or in cyberspace. It requires individuals with an underlying capacity to form and act on their notions of the good in deciding how to live their lives. This anti-totalitarian principle stands as a bulwark against any coercive standardization of the individual.²⁸⁰ Yet, a considerable difficulty arises in identifying the kinds of government or group behavior that raises a threat to personal self-governance. Part of the problem is that autonomy is a notoriously slippery concept.²⁸¹ Even more to the point, however, communal life requires something beyond isolated decisionmaking—self-governance takes place in individuals who are not located on discrete behavioral islands, but are tied to others and necessarily open to influence through outside persuasion.²⁸² Social life's give-and-take is not merely compatible with individual autonomy, but an essential factor in it because life is lived among others. Prior and ongoing commitments make a difference in the choices we make and in the hierarchy of our goals.²⁸³ As a result, we must comprehend autonomous people as being only partially the authors of their lives. As Joseph Raz has proposed, “[t]he ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives.”²⁸⁴ Individuals who exercise self-determination, therefore, should be defined as people who, as part authors of their lives, substantially shape their existence through the choices they make. Self-determination is a capacity that is embodied and developed through social forms and practices. The threat to this quality arises when private or government action interferes with a person's control of her reasoning process. To understand the harm of this manipulation, consider David Strauss's examination of different kinds of manipulation in the speech context.²⁸⁵ In that setting, coercion occurs when one compels another to pursue the speaker's objectives instead of the victim's own

objectives.²⁸⁹ Such coercion can take place through simple use of physical force or through inducements that interject false facts into the thought processes of the listeners.²⁹⁰ Drawing on Strauss's work, we can state that a coercive influence on decision making is that which takes over, or colonizes, a person's thinking processes.²⁹¹

Privacy good – Serial Policy Failure

Privacy is a necessary right – otherwise that ensures serial policy failure

Brand 15 (Jeffrey S. Brand, Dean and Professor Emeritus and Chairman of the Center for Law and Global Justice, “Eavesdropping on Our Founding Fathers: How a Return to the Republic’s Core Democratic Values Can Help Us Resolve the Surveillance Crisis”, February 2015, <http://harvardnsj.org/wp-content/uploads/2015/02/Brand.pdf>) //mL

Those who voted for and even those who voted against FISA in the 95th Congress deserve high marks for articulating the fundamental values at stake. In fact, well before FISA’s passage in 1978, members of Congress had invoked the fundamental values of American democracy in trying to come to grips with the Watergate crisis and how America should handle the balance between the nation’s legitimate security needs and the rights of its citizens. Thus, on June 29, 1972, just twelve days after the White House “plumbers” bungled their Watergate break-in, the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee held hearings. Senator Kennedy gavelled the hearing to order and intoned the words of Justice Lewis Powell in Keith, which he characterized as “one of the most stirring judicial statements of our times.”⁸⁵ He stated: The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public disclosure is essential to our free society.⁸⁶ Kennedy’s linking of Justice Powell’s comments to the purpose of the hearing was equally stirring: Our goal here today is to relieve all Americans of that “dread of unchecked surveillance power” and that “fear of unauthorized official eavesdropping. . . .” We are here to see that the constitutional promise is kept, that our right to be let alone, our right to privacy, our right to speak freely in public and in private, our right to have different views, and the other rights which keep our lives free from unwarranted government intrusion, are vindicated rather than evaded, preserved and not avoided, enhanced instead of circumvented.⁸⁷ Indeed, at the June 29 hearing, there was a definite sense of dread of unchecked power and outright fear about where the Republic was headed.

Senator Edmond Muskie (D-ME) expressed the views of many: “George Orwell may prove to have been right 10 years ahead of his time if we cannot bring under control whom Big Brother is watching and when.”⁸⁸ The urgency was laced with a sense of betrayal. Again, Senator Muskie captured the feeling: “As reasonable men we had put our faith in the reasonable use of power. That faith has been abused and we offer this legislation to check the unreasonable power now vested in the President to order actions in the name of national security.”⁸⁹ Former Attorney General Ramsey Clark echoed these comments when he testified at the same hearing: “Unfortunately, our ignorance exceeds our knowledge in such subjects [the history of wiretapping and electronic surveillance], because we practice government by secrecy, which in my opinion is wholly incompatible with a free society.”⁹⁰ That sense of urgency and concern was exacerbated by the findings of the Church Committee two years later. The Committee report, often cited during the FISA debates, was blunt in its analysis: Since the early 1930’s, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a U.S. Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam war protest group.⁹¹ The Church Committee’s findings, coupled with the findings of the Senate Select Watergate Committee which he chaired, led the self-described “simple country lawyer” from North Carolina, Senator Sam Ervin (D-NC), to opine in 1974 at a hearing on one of the bills that was the precursor to FISA: “The problem, as I see it, is to legislate controls over the practice of warrantless wiretapping which would protect the constitutional rights of all citizens. . . .”⁹² It is fair to say, that these comments reflected a deep concern that time might have run out and that it might be too late to act. It was in that context that on March 23, 1976, President Gerald Ford, who had inherited his office from a disgraced Richard Nixon who had resigned eighteen months earlier, formally forwarded the first version of a bill that would morph into FISA to the Speaker of the House, Carl Albert (D-OK). Ford’s letter accompanying the legislation lacked the inspirational tones of Senator Kennedy but stated the same goal that Senator Ervin had articulated two years earlier: The enactment of this bill will ensure that the government will be able to collect necessary foreign intelligence. At the same time, it will provide major assurance to the public that electronic surveillance for foreign intelligence purposes can and will occur only when reasonably justified in circumstances demonstrating an overriding national interest, and that they will be conducted according to standards and procedures that protect against possibilities of abuse.⁹³ Thus, by 1976, when the FISA bill was being debated, there were multiple statements by Democrats and Republicans arguing that the current state of affairs was inconsistent with the foundation on which the country was built and affirming the underlying values of the Republic. Senator Mathias’s statement on October 10, 1978, that FISA was a “milestone in our nation’s history” and a “ringing affirmation of a commitment to fundamental liberties,”⁹⁴ mirrored the comments of Senator Bayh, who staked out the moral high ground and the underlying values of the nation in support of the legislation: The bill also sends a message around the world . . . [that] in the United States we like to feel that we establish a higher standard, and

we feel a high degree of sensitivity about the rights of all human beings . . . I believe the American people can take pride in this legislation. It represents all that we stand for as a nation with a living constitution that can be adapted to new problems without sacrificing its fundamental values.⁹⁵ In addition, the country's roots in the rule of law became a common theme throughout the debate. In the House, Representative Robert Kastenmeier (D-WI) hailed the bill as a return to the "rule of law,"⁹⁶ as did Senator Kennedy upon his introduction of S. 1566 on May 18, 1977: "Mr. President, today I am introducing legislation—endorsed and supported by this administration—which would at long last place foreign intelligence electronic surveillance under the rule of law."⁹⁷ Kennedy had offered the same rationale when he introduced S. 3197 the previous year: "It is a recognition, long overdue, that the rule of law must prevail in the area of foreign intelligence surveillance."⁹⁸ Even stalwart opponents of FISA echoed the need to be vigilant about the fundamental values upon which American democracy rests. Listen to Senator Malcolm Wallop (R-WY), a vocal Republican opponent of FISA, who nonetheless understood the core values that were at stake: "In order to be lawful . . . the power of electronic surveillance, like all other powers, must be exercised only for the purpose for which it was intended. Each exercise of power must be reasonably and proportionally related to the end for which the power exists."⁹⁹ It was Senator John Tunney (D-CA), however, the lone wolf to vote against S3197 (the precursor to S1566) in the Senate Judiciary Committee, who best and most presciently articulated why the fate of the Republic hung in the balance: Technological developments are arriving so rapidly and are changing the nature of our society so fundamentally that we are in danger of losing the capacity to shape our own destiny. This danger is particularly ominous when the new technology is designed for surveillance purposes, for in this case the tight relationship between technology and power is most obvious. Control over the technology of surveillance conveys effective control over our privacy, our freedom, and our dignity—in short, control over the most meaningful aspects of our lives as free human beings.¹⁰⁰

Privacy good – Check State Power

Private is good for citizens but private government opens the door to corruption

Truthout, 13- nonprofit organization dedicated to revealing systemic injustices and providing a platform for transformative ideas, (“Without Privacy There Can Be No Democracy”, Truthout, September 24th 2013, <http://www.truth-out.org/opinion/item/19039-without-privacy-there-can-be-no-democracy>)//AP

The president of Brazil, Dilma Rousseff, spoke this morning at the United Nations and delivered a powerful indictment of spying by the NSA on behalf of the United States. She said, "Without respect for a nation's sovereignty, there is no basis for proper relations among nations," adding that "Brazil knows how to protect itself. Brazil ... does not provide shelter to terrorist groups. We are a democratic country." The Brazilian president is so outraged at American spying, both on her country and on her personal emails and her personal life, that she canceled a state dinner with President Obama. While most Americans see this as a rift between Brazil in the United States over the issue of our spying on them, President Rousseff highlighted the most important point of all elsewhere in her speech this morning. She said, "Without the right of privacy, there is no real freedom of speech or freedom of opinion, and so there is no actual democracy." This is not just true of international relations.

It's also true here within the United States. Back before the Kennedy administration largely put an end to it, J Edgar Hoover was infamous in political circles in Washington DC for his spying on and blackmailing of both American politicians and activists like Martin Luther King. He even sent King tapes of an extramarital affair and suggested that King should consider committing suicide. That was a shameful period in American history, and most Americans think it is behind us. But the NSA, other intelligence agencies, and even local police departments have put the practice of spying on average citizens in America on steroids. As Brazil's President points out, without privacy there can be no democracy. Democracy requires opposing voices; it requires a certain level of reasonable political conflict. And it requires that government misdeeds be exposed. That can only be done when whistleblowers and people committing acts of journalism can do so without being spied upon. Perhaps a larger problem is that well over half – some estimates run as high as 70% – of the NSA's budget has been outsourced to private corporations. These private corporations maintain an army of lobbyists in Washington DC who constantly push for more spying and, thus, more money for their clients. With the privatization of intelligence operations, the normal system of checks and balances that would keep government snooping under control has broken down. We need a new Church Commission to investigate the nature and scope of our government spying both on our citizens and on our allies. But even more than that we need to go back to the advice that President Dwight Eisenhower gave us as he left the presidency in 1961. Eisenhower warned about the rise of a military-industrial complex, suggesting that private forces might, in their search for profits, override the protective mechanisms that keep government answerable to its people. That military-industrial complex has become the military-industrial-spying-private-prison complex, and it is far greater a threat to democracy than probably was envisioned by Eisenhower. Government is the protector of the commons. Government is of by and for we the people. Government must be answerable to the people. When the functions of government are privatized, all of that breaks down and Government becomes answerable to profit. It's time to reestablish the clear dividing lines between government functions and corporate functions, between the public space and the private space. A critically important place to start that is by ending the privatization within our national investigative and spying agencies.

Intellectual Privacy key 1st Amend

Intellectual Privacy is protected under the first amendment of the constitution

Neil M. Richards, Professor of Law, Washington University School of Law, 05-20-13

{Harvard Law Review: Volume 126, Number 7 - May 2013: The Dangers of Surveillance} Pgs. 1949-1950

A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the “First Pillar” of First Amendment law — the “[e]xtraordinary [p]rotection against [c]ensorship.”⁸⁵ Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the “chilling effect.” This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspicion by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, New York Times Co. v. Sullivan,⁸⁶ the importance of uninhibited public debate means that, although “erroneous statement is inevitable in free debate, . . . it must be protected if the freedoms of expression are to have the ‘breathing space’ that they ‘need . . . to survive.’⁸⁷ As Professor Frederick Schauer explains, “the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech.”⁸⁸ Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments,⁸⁹ such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech’s undesirable consequences.

Fear Magnifies Privacy Loss

Fear and perception magnify privacy loss.

Heymann 2015,

Philip B, Professor of Law, Harvard Law School “An Essay On Domestic Surveillance” Lawfare Research Paper Series Vol 3.2, <http://www.lawfareblog.com/wp-content/uploads/2013/08/Lawfare-Philip-Heymann-SURVEILLANCE-for-publ-10-May-2015.pdf>

The Independent Significance Of Fear Of Loss Of Privacy To Secret Governmental Surveillance: The capacity to collect, process, and use massive amounts of information on great numbers of citizens does not necessarily mean that the information is actually used in a way threatening to a citizen's privacy. Phone metadata, images from street cameras, and the product of a secretly placed global positioning device, could simply be stored until some form of predicate, such as probable cause, gave reason to pull it out of the inventory for view and study. And perhaps I need not worry about cameras or global positioning devices or cell phones collecting information on where I have been and what I have done, so long as there must be probable cause or some lesser predicate (e.g., “reasonable suspicion”) for the government to access what it has collected. In fact, on this theory, a huge inventory of government metadata on phone use is stored by the NSA where it is readily available to be searched – but only on an internal governmental determination of “reasonable suspicion” that it involves a terrorist plan. The inventory may not be searched without that internal determination. So, in both examples I have chosen, concern about adverse effects of lost privacy turns on the effect on citizens' attitudes and behavior of knowing that records of what they are doing will be held by the government and could, perhaps improperly, be viewed at a later date without a judicial warrant -- with no more than a bureaucratic determination of “reasonable suspicion” that the record bears on a national security threat. The presence of fear, even unreasonable fear, has important effects on the confident and free social and political life on which democracy depends. Fear of discovery alone could easily affect with whom I associate, for example, or what use I make of psychiatrists or drugs. The fear is far deeper and more lasting if a warrant from a judge is not required. Internal agency processes are not an adequate substitute. The deep suspicions that are valuable in an agency charged with preventing terrorism or preventing crime have a dark side; they will infect its judgment of when there is a genuine need to see the required information. Important consequences turn on the citizens' trust that data the government has acquired will not be used without there being a “real” need for its use. Much of the population would not trust any such assurance by the NSA or the FBI alone. Perceptions of government prying do matter. Whether a dramatic growth in the capacity for, and fruits of, government surveillance would be experienced as harmful to individual freedom, civil society and democratic institutions depend on more than how the information would, in fact, be used. Fear also depends on what other potential uses citizens would suspect; the exercise of individual liberty and autonomy additionally depend on what citizens suspect might happen with that information and the precautionary steps – curtailment of entirely lawful activities, for example – citizens might take. Attitudes toward government and one's freedoms also depend upon a number of broader contextual factors: the extent of the perceived danger sought to be prevented; the current level of suspicion or trust in the government; the history and culture of privacy in the society; and much else. Some few would argue that the loss of privacy might not be a concern at all. After all, most people do not harbor a crime or a scandal that they must hide behind claims to privacy; their lives are too proper for that. But those voices are a small minority; for most people, the value of privacy is to protect the possibility of association and, particularly, intimacy with others, irrespective of whether one has anything to hide in the way of crime or scandal. One fact is clear. The fear and the prospect of rapidly expanding government surveillance in the United States are plainly there on the near horizon. The children of the Snowden age take it for granted that they are being monitored and they fear the social effects of that monitoring.

Privacy Outweighs w/Util

Even within a utilitarian framework, privacy outweighs for two reasons:
First – Structural bias. Their link inflates the security risk and their impact's an epistemologically wrong.

Solove '8 Daniel Solove is an Associate Professor at George Washington University Law School and holds a J.D. from Yale Law School. He is one of the world's leading expert in information privacy law and is well known for his academic work on privacy and for popular books on how privacy relates with information technology. He has written 9 books and more than 50 law review articles – From the Article: "Data Mining and the Security-Liberty Debate" - University of Chicago Law Review, Vol. 74, p. 343, 2008 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030

Data mining is one issue in a larger debate about security and privacy. Proponents of data mining justify it as an essential tool to protect our security. For example, Judge Richard Posner argues that "[i]n an era of global terrorism and proliferation of weapons of mass destruction, the government has a compelling need to gather, pool, sift, and search vast quantities of information, much of it personal."⁹ Moreover, proponents of security measures argue that we must provide the executive branch with the discretion it needs to protect us. We cannot second guess every decision made by government officials, and excessive meddling into issues of national security by judges and others lacking expertise will prove detrimental. For example, William Stuntz contends that "effective, active government—government that innovates, that protects people who need protecting, that acts aggressively when action is needed—is dying. Privacy and transparency are the diseases. We need to find a vaccine, and soon."¹⁰ Stuntz concludes that "[i]n an age of terrorism, privacy rules are not simply unaffordable. They are perverse."¹¹ We live in an "age of balancing," and the prevailing view is that most rights and civil liberties are not absolute.¹² Thus, liberty must be balanced against security. But there are systematic problems with how the balancing occurs that inflate the importance of the security interests and diminish the value of the liberty interests. In this essay, I examine some common difficulties in the way that liberty is balanced against security in the context of data mining. Countless discussions about the tradeoffs between security and liberty begin by taking a security proposal and then weighing it against what it would cost our civil liberties. Often, the liberty interests are cast as individual rights and balanced against the security interests, which are cast in terms of the safety of society as a whole. Courts and commentators defer to the government's assertions about the effectiveness of the security interest. In the context of data mining, the liberty interest is limited by narrow understandings of privacy that neglect to account for many privacy problems. As a result, the balancing concludes with a victory in favor of the security interest. But, as I will argue, important dimensions of data mining's security benefits require more scrutiny, and the privacy concerns are significantly greater than currently acknowledged. These problems have undermined the balancing process and skewed the results toward the security side of the scale.

Debates about data mining begin with the assumption that it is an essential tool in protecting our security. Terrorists lurk among us, and ferreting them out can be quite difficult. Examining data for patterns will greatly assist in this endeavor, the argument goes, because certain identifiable characteristics and behaviors are likely to be associated with terrorist activity. Often, little more is said, and the debate proceeds to examine whether privacy is important enough to refrain from using such an effective terrorism-fighting tool. Many discussions about security and liberty proceed in this fashion. They commence by assuming that a particular security measure is effective, and the only remaining question is whether the liberty interest is strong enough to curtail that measure. But given the gravity of the security concerns over terrorism, the liberty interest has all but lost before it is even placed on the scale. Judge Richard Posner argues that judges should give the executive branch considerable deference when it comes to assessing the security measures it proposes. In his recent book, Not a Suicide Pact: The Constitution in a Time of National Emergency,¹³ Posner contends that judicial restraint is wise because "when in doubt about the actual or likely consequences of a measure, the pragmatic, empiricist judge will be inclined to give the other branches of government their head."¹⁴ According to Posner, "[j]udges aren't supposed to know much about national security."¹⁵ Likewise, Eric Posner and Adrian Vermeule declare in their new book, Terror in the Balance: Security, Liberty, and the Courts,¹⁶ that "the executive branch, not Congress or the judicial branch, should make the tradeoff between security and liberty."¹⁷ Moreover, Posner and Vermeule declare that during emergencies, "[c]onstitutional rights should be relaxed so that the executive can move forcefully against the threat."¹⁸ The problem with such deference is that, historically, the executive branch has not always made the wisest national security decisions. Nonetheless, Posner and Vermeule contend that notwithstanding its mistakes, the executive branch is better than the judicial and legislative branches on institutional competence grounds.¹⁹ "Judges are generalists," they observe, "and the political insulation that protects them from current politics also deprives them of information, especially information about novel security threats and necessary responses to those threats."²⁰ Posner and Vermeule argue that during emergencies, the "novelty of the threats and of the necessary responses makes judicial routines and evolved legal rules seem inappropriate, even obstructive."²¹ "Judicial routines" and "legal rules," however, are the cornerstone of due process and the rule of law—the central building blocks of a free and democratic society. At many times, Posner, Vermeule, and other strong proponents of security seem to focus almost exclusively on what would be best for security when the objective should be establishing an optimal balance between security and liberty. Although such a balance may not promote security with maximum efficiency, it is one of the costs of living in a constitutional democracy as opposed to an authoritarian political regime. The executive branch may be the appropriate branch for developing security measures, but this does not mean that it is the most adept branch at establishing a balance between security and liberty. In our constitutional democracy, all branches have a role to play in making policy. Courts protect constitutional rights not as absolute restrictions on executive and legislative policymaking but as important interests to be balanced against government interests. As T. Alexander Aleinikoff notes, "balancing now dominates major areas of constitutional law."²² Balancing occurs through various forms of judicial scrutiny, requiring courts to analyze the weight of the government's interest, a particular measure's effectiveness in protecting that interest, and the extent to which the government interest can be achieved without unduly infringing upon constitutional rights.²³ For balancing to be meaningful, courts must scrutinize both the security and liberty interests. With deference, however, courts fail to give adequate scrutiny to security interests. For example, after the subway bombings in London, the New York City Police Department began a program of random searches of people's baggage on the subway. The searches were conducted without a warrant, probable cause, or even reasonable suspicion. In *MacWade v Kelly*,²⁴ the United States Court of Appeals for the Second Circuit upheld the program against a Fourth Amendment challenge. Under the special needs doctrine, when exceptional circumstances make the warrant and probable cause requirements unnecessary, the search is analyzed in terms of whether it is "reasonable."²⁵ Reasonableness is determined by balancing the government interest in security against the interests in privacy and civil liberties.²⁶ The weight of the security interest should turn on the extent to which the program effectively improves subway safety. The goals of the program may be quite laudable, but nobody questions the importance of subway safety. The critical issue is whether the search program is a sufficiently effective way of achieving those goals that it is worth the tradeoff in civil liberties. On this question, unfortunately, the court deferred to the law enforcement officials, stating that the issue "is best left to those with a unique understanding of, and responsibility for, limited public resources, including a finite number of police officers."²⁷ In determining whether the program was "a reasonably effective means of addressing the government interest in deterring and detecting a terrorist attack on the subway system,"²⁸ the court refused to examine the data to assess the program's effectiveness.²⁹ The way the court analyzed the government's side of the balance would justify nearly any search, no matter how ineffective. Although courts should not take a know-it-all attitude, they should not defer on such a critical question as a security measure's effectiveness. The problem with many security measures is that they are not wise expenditures of resources. A small number of random searches in a subway system of over four million riders a day seems more symbolic than effective because the odds of the police finding the terrorist with a bomb are very low. The government also argued that the program would deter terrorists from bringing bombs on subway trains, but nearly any kind of security measure can arguably produce some degree of deterrence. The key issue, which the court did not analyze, is whether the program would lead to deterrence significant enough to outweigh the curtailment of civil liberties. If courts fail to question the efficacy of security measures, then the security interest will prevail nearly all the time. Preventing terrorism has an immensely heavy weight, and any given security measure will provide a marginal advancement toward that goal. In the deference equation, the math then becomes easy. At this point, it is futile to even bother to look at the civil liberties side of the balance. The government side has already won. Proponents of deference argue that if courts did not defer, then they would be substituting their judgment for that of executive officials, who have greater expertise in understanding security issues. Special expertise in national security, however, is often not necessary for balancing security and liberty. Judges and legislators should require the experts to persuasively justify the security measures being developed or used. Of course, in very complex areas of knowledge, such as advanced physics, nonexperts may find it difficult to understand the concepts and comprehend the terminology. But it is not clear that security expertise involves such sophisticated knowledge that it would be incomprehensible to nonexperts. Moreover, the deference argument conflates evaluating a particular security measure with creating such a measure. The point of judicial review is to subject the judgment of government officials to critical scrutiny rather than blindly accept their authority. Critical inquiry into factual matters is not the imposition of the judge's own judgment for that of the decisionmaker under review.³⁰ Instead, it is forcing government officials to explain and justify their policies. Few will quarrel with the principle that courts should not "second guess" the decisions of policy experts. But there is a difference between not "second guessing" and failing to critically evaluate the factual and empirical evidence justifying the government programs. Nobody will contest the fact that security is a compelling interest. The key issue in the balancing is the extent to which the security measure furthers the interest in security. As I have argued elsewhere, whenever courts defer to the government on the effectiveness of a government security measure, they are actually deferring to the government on the ultimate question as to whether the measure passes constitutional muster.³¹ Deference by the courts or legislature is an abdication of their function. Our constitutional system of government was created with three branches, a design structured to establish checks and balances against abuses of power. Institutional competence arguments are often made as if they are ineluctable truths about the nature of each governmental branch. But the branches have all evolved considerably throughout history. To the extent a branch lacks resources to carry out its function, the answer should not be to diminish the power of that branch but to provide it with the necessary tools so it can more effectively carry out its function. Far too often, unfortunately, discussions of institutional competence devolve into broad generalizations about each branch and unsubstantiated assertions about the inherent superiority of certain branches for making particular determinations. It is true, as Posner and Vermeule observe, that historically courts have been deferential to the executive during emergencies.³² Proponents of security measures often advance what I will refer to as the "pendulum theory"—that in times of crisis, the balance shifts more toward security and in times of peace, the balance shifts back toward liberty. For

example, Chief Justice Rehnquist argues that the "laws will thus not be silent in time of war, but they will speak with a somewhat different voice."³³ Judge Posner contends that the liberties curtailed during times of crisis are often restored during times of peace.³⁴ Deference is inevitable, and we should accept it without being overly concerned, for the pendulum will surely swing back. As I argue elsewhere, however, there have been many instances throughout US history of needless curtailments of liberty in the name of security, such as the Palmer Raids, the Japanese Internment, and the McCarthy communist hearings.³⁵ Too often, such curtailments did not stem from any real security need but because of the "personal agendas and prejudices" of government officials.³⁶ We should not simply accept these mistakes as inevitable; we should seek to prevent them from occurring. Hoping that the pendulum will swing back offers little consolation to those whose liberties were infringed or chilled. The protection of liberty is most important in times of crisis, when it is under the greatest threat. During times of peace, when our judgment is not clouded by fear, we are less likely to make unnecessary sacrifices of liberty. The threat to liberty is lower in peacetime, and the need to protect it is not as dire. The greatest need for safeguarding liberty is during times when we least want to protect it. In order to balance security and liberty, we must assess the security interest. This involves evaluating

two components—the gravity of the security threat and the effectiveness of the security measures to address it. It is often merely assumed without question that the security threat from terrorism is one of the gravest dangers we face in the modern world. But this assumption might be wrong. Assessing the risk of harm from terrorism is very difficult because terrorism is such an irregular occurrence and is constantly evolving. If we examine the data from previous terrorist attacks, however, the threat of terrorism has been severely overstated. For example, many people fear being killed in a terrorist attack, but based on statistics from terrorism in the United States, the risk of dying from terrorism is minuscule. According to political scientist John Mueller, [e]ven with the September 11 attacks included in the count . . . the number of Americans killed by international terrorism since the late 1960s (which is when the State Department began its accounting) is about the same as the number killed over the same period by lightning, or by accident-causing deer, or by severe allergic reactions to peanuts.³⁷ Add up the eight deadliest terrorist attacks in US history and they amount to fewer than four thousand fatalities.³⁸ In contrast, flu and pneumonia deaths are estimated to be around sixty thousand per year.³⁹ Another forty thousand die in auto accidents each year.⁴⁰ Based on our experience with terrorism thus far, the risk of dying from terrorism is very low on the relative scale of fatal risks.

Dramatic events and media attention can cloud a rational assessment of risk. The year 2001 was not just notable for the September 11 attacks. It was also the summer of the shark bite, when extensive media coverage about shark bites led to the perception that such attacks were on the rise. But there were fewer shark attacks in 2001 than in 2000 and fewer deaths as well, with only four in 2001 as compared to thirteen in 2000.⁴¹ And regardless of which year had more deaths, the number is so low that an attack is a freak occurrence. It is certainly true that our past experience with terrorism might not be a good indicator of the future. More treacherous terrorism is possible, such as the use of nuclear or biological weapons. This complicates our ability to assess the risk of harm from terrorism. Moreover, the intentional human conduct involved in terrorism creates a sense of outrage and fear that ordinary deaths do not engender. Alleviating fear must be taken into account, even if such fear is irrationally high in relation to other riskier events such as dying in a car crash. But enlightened policy must not completely give in to the panic and irrational fear of the moment. It should certainly attempt to quell the fear, but it must do so thoughtfully. Nevertheless,

most policymakers find it quite difficult to assess the threat of terrorism modestly. In the face of widespread public panic, it is hard for government officials to make only moderate changes. Something dramatic must be done, or political heads will roll. Given the difficulty in assessing the security threat in a more rational manner, it is imperative that the courts meaningfully analyze the effectiveness of security measures. Even if panic and fear might lead to the gravity of the threat being overstated, we should at least ensure that the measures taken to promote security are sufficiently effective to justify the cost. Unfortunately, as I will discuss in the next section, rarely do discussions about the sacrifice of civil liberties explain the corresponding security benefit, why such a benefit cannot be achieved in other ways, and why such a security measure is the best and most rational one to take.

Little scrutiny is given to security measures. They are often just accepted as a given, no matter how ill-conceived ineffective they might be. Some ineffective security measures are largely symbolic, such as the New York City subway search program. The searches are unlikely to catch or deter terrorists because they involve only a minuscule fraction of the millions of daily passengers. Terrorists can just turn to other targets or simply attempt the bombing on another day or at another train station where searches are not taking place. The vice of symbolic security programs is that they result in needless sacrifices of liberty and drain resources from other, more effective security measures. Nevertheless, these programs have a virtue—they can ameliorate fear because they are highly visible. Ironically, the subway search program's primary benefit was alleviating people's fear (which was probably too high), albeit in a deceptive

manner (as the program did not add much in the way of security). **Data mining** represents another kind of security measure, one that currently has little proven effectiveness

and little symbolic value. Data mining programs are often not visible enough to the public to quell much fear. Instead, their benefits come primarily from their actual effectiveness in reducing terrorist threats, which remains highly speculative. Thus far, **data mining is not very accurate** in the behavioral predictions it makes. For example, there are approximately 1.8 million airline passengers each day.⁴² A data mining program to identify terrorists with a false positive rate of 1 percent (which would be exceedingly low for such a program) would flag eighteen thousand people as false positives. This is quite a large number of innocent people. Why is the government so interested in data mining if it remains unclear whether it will ever be very accurate or workable? Part of the government's interest in data mining stems from the aggressive marketing efforts of database companies. After September 11, database companies met with government officials and made a persuasive pitch

about the virtues of data mining.⁴³ The technology sounds quite dazzling when presented by skillful marketers, and it can work quite well in the commercial setting. The problem, however, is that **just because data mining might be effective for businesses trying to predict customer behavior does not make it effective for the government trying to predict who will engage in terrorism.** A high level of accuracy is not necessary when data mining is used by businesses to target marketing to consumers, because the cost of error to individuals is minimal. Amazon.com, for example, engages in data mining to determine which books its customers are likely to find of interest by comparing bookbuying patterns among its customers. Although it is far from precise, it need not be because there are few bad consequences if it makes a wrong book recommendation. Conversely, the consequences are vastly greater for government data mining. Ultimately,

I do not believe that the case has been made that data mining is a wise expenditure of security resources. Those who advocate for security should be just as outraged as those on the liberty side of the debate. Although courts should not micromanage which security measures the government chooses, they should examine the effectiveness of any given security measure to weigh it against the liberty costs. Courts should not tell the executive branch to modify a security measure just because they are not convinced it is the best one, but they should tell the executive that a particular security measure is not effective enough to outweigh the liberty costs. **The very point of protecting liberty is to demand that sacrifices to liberty are not in vain and that security interests, which compromise civil liberties, are sufficiently effective to warrant the cost.**

Second - Relative certainty. The disadvantage may cause violence - surveillance definitely does. Privacy is paramount for dignity and protecting our unique individuality.

Schneier '6 Bruce Schneier is a fellow at the Berkman Center for Internet & Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute and the CTO of Resilient Systems. He is the author of Beyond Fear: Thinking Sensibly About Security in an Uncertain World. Commentary, "The Eternal Value of Privacy", WIRED, May 18, 2006, <http://www.wired.com/news/columns/1,70886-0.html>

The most common retort against privacy advocates -- by those in favor of ID checks, cameras, databases, data mining and other wholesale surveillance measures -- is this line: "If you aren't doing anything wrong, what do you have to hide?" Some clever answers: "If I'm not doing anything wrong, then you have no cause to watch me." "Because the government gets to define what's wrong, and they keep changing the definition." "Because you might do something wrong with my information." My problem with quips like these -- as right as they are -- is that they accept the premise that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect. Two proverbs say it best: Quis custodiet custodes ipsos? ("Who watches the watchers?") and "Absolute power corrupts absolutely." Cardinal Richelieu understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged." Watch someone long enough, and you'll find something to arrest -- or just blackmail -- with. Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political enemies -- whoever they happen to be at the time. Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance. We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need. A future in which privacy would face constant assault was so alien to the framers of the Constitution that it never occurred to them to call our privacy as an explicit right. Privacy was inherent to the nobility of their being and their cause. Of course being watched in your own home was unreasonable. Watching at all was an act so unseemly as to be inconceivable among gentlemen in their day. You watched convicted criminals, not free citizens. You ruled your own home. It's intrinsic to the concept of liberty. For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that -- either now or in the uncertain future -- patterns we leave behind will be brought back to implicate us by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable. How many of us have paused during conversation in the past four-and-a-half years, suddenly aware that we might be eavesdropped on? Probably it was a phone conversation, although maybe it was an e-mail or instant-message exchange or a conversation in a public place. Maybe the topic was terrorism, or politics, or Islam. We stop suddenly, momentarily afraid that our words might be taken out of context, then we laugh at our paranoia and go on. But our demeanor has changed, and our words are subtly altered. This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives. Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy, even when we have nothing to hide.

Surveillance violates our basic ethical imperative to treat people with dignity and protect freedom, but even if utilitarianism is good, you should still vote aff

BURKHART et al. 2007 (Laurie Burkhart, Michael Haubert, and Damon Thorley, undergraduate editors who published a book on surveillance under the supervision of Dr. Dirk S. Hovorka, "The Effect [sic] of Government Surveillance on Social Progress," in Confronting Information Ethics in the New Millennium" <http://www.ethicapublishing.com/5CH1.htm>)

Under utilitarian, duty-based, and rights-based ethical theories the act of heavy government surveillance policy is an ethical violation. From a utilitarian perspective, one must look at the consequences of an action, and determine which consequence would be the most desirable for the greatest number of people involved. In this case, the government is not acting in line with what is the greatest good for the greatest number.

The greatest good is allowing a society to have the ability to freely participate and change the system in order to adhere to what is best for the people. By limiting radical political groups the government can effectively take away this

ability. In taking the ability to change and progress away from the people in a democratic system the government violates the greatest good for the greatest number. The use of government surveillance to hinder radical movements is causing a “chilling effect” on political participation and results in an obstruction of social progress. The consequences of these government actions are undesirable, the actions are considered to be unethical under utilitarian or consequence-based theory. The duty-based and rights-based theories also show extreme surveillance to be an ethical violation. From a duty-based, or deontological perspective, heavy government surveillance is an ethical violation because it does not treat people in a universal or impartial way. Immanuel Kant, one of the most famous and influential deontological theorists, claimed that actions are unethical if they conflict with the idea that all people are free and rational beings. He stated that everyone has a duty to stop such unethical acts and promote freedom and rationality. Furthermore he stated that rules should only be applied if they are universal and impartial. Acts of government surveillance are often carried out with heavy biases against certain types of groups and ideologies, such as the civil rights or communist groups. In addition, using surveillance tactics against certain groups and individuals goes against the idea that people are free and capable of making their own decisions, and implies that people need to be monitored and controlled. Certain types of monitoring and controlling are necessary in any society, but in a democratic society when the control tactics goes as far to limit the effect the people can have on their own society then the system is not only undemocratic ,but unethical as well. The surveillance bias towards particular groups also violates several rules and regulations stated in our countries legal doctrines. Rights-based theory states that an action is unethical if it goes against rights that have been given through contract or law. Surveillance practices of the FBI and other government groups have shown to violate several laws and the rights that have been given to citizens by the government, such as freedom of speech, freedom of assembly, protection against illegal searches, and many more. In order to be ethical under a rights-based theory a democratic government must follow the laws and regulations set forth by the people’s elected government agents. Past and present government surveillance tactics violate these principles and are therefore unethical.

“One does not establish a dictatorship in order to safeguard a revolution; one makes a revolution in order to establish a dictatorship.” -- George Orwell 16 Legal Implications

Our democratic system is built on the people’s participation in politics. This participation is most commonly practiced by voting in government elections and identifying with a major political party. Although these types of political participation are the most practiced and socially accepted they are not the only form of participation the system is built on. As outlined in Amendment I of the U.S. Constitution Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people

peaceably to assemble, and to petition the Government for a redress of grievances¹⁷. Based on these laws the people of our country can speak out, challenge, and criticize the government as they see fit without fear of persecution. The theory behind this system is to allow for free and unaltered participation in the government by the people so that the laws and discourse of the country reflect that of the people’s beliefs. For this legal system to function properly the free participation of the people must be protected. Although our society generally chooses to believe this to be true, U.S. historical evidence shows the contrary. Each radical social movement in the U.S. has posed a general threat to the government administration of that time. From a present day perspective some of these movements brought about positive social change. Aside from the moral value of each radical movement, the government agencies of their times determine what will be in the best interest of the country and exude enormous surveillance and propaganda tactics for or against them. At the time of the civil rights movements the FBI classified pro-black groups as threats to national security. Despite these past classifications, these groups made a large positive impact on our countries values and laws. As a result of these “threats to national security” citizens of our country can now expect to be treated equally under the law and not endure unjust policies based on race. At the basis of all social change there is an opposition to the norm or majority. In the case of the civil rights movement the norm was a predominately racist society with national laws and regulations to perpetuate the racist system. Despite the efforts of government agencies to curb the radical groups and halt the social progress being made the people were able to assemble and cause radical reformations to take place in legal and social aspects of the country. It can be said that although the FBI and government tried to curb the Civil Rights movement the social change did occur and the theory of free political participation was upheld. Although it is true that the government ultimately failed in stopping the movement and societal change, they did not have the same technology that is available today. During the civil rights movement the FBI used basic surveillance technology including wire taps, bugged rooms, stake outs and propaganda. Today technology is advancing at a quicker rate than we can make use of it. The government now has technology and the access to information far greater than that of the 1960’s and can use it however they see fit. If not kept in check the government surveillance can lead to a system in which social change brought about by the people becomes impossible.

Conclusion

Demonstrated by the history in our country each government administration has used every resource they have in order to pursue the values and goals of their administration. As technology increases, so does the power of the government to monitor citizens, infiltrate groups, control information, and further push their view of what is best for the society. In an age of data mining, satellite surveillance, RFID chips, vast social networks, and an overall state of heightened security there is almost no limit to the capabilities of the government and its surveillance. We can assume based on historical facts that the government is currently monitoring to the best of their ability all radical groups in the country as well as the world. With current technology it’s also safe to assume that this surveillance and group monitoring is much more effective than in the past and could possibly end radical political influence before it starts. Coupled with increased technology there has been a decrease of freedom in our legal system with war time laws such as the Patriot Act limiting fundamental rights and legal discourse outlined in the U.S. constitution. The system is moving away from free political participation and towards an information influenced police

state. The U.S. legal system is based on change and adaptability. A historical example of this is the change in role the U.S. legal system took on in the nineteenth century. “An instrumental perspective of law did not simply emerge as a response to new economic forces in the nineteenth century. Rather, judges began to use law in order to encourage social change even in areas where they had previously refrained from doing so. It was not until the nineteenth century that the common law took on its innovating and transforming role in American society¹⁸.” Examples such as this show that the legal system has always played its part in influencing societal change since the early days of this country, but conversely the U.S. society members have also influenced changes to the legal system. The changes and innovation of U.S. law have consistently been influenced by social movements. The labor movements, civil rights movements, and feminist movements have all challenged the government of their time and as a result moved the U.S. towards a more equal and just society. As the power and technology of the government increases today so do the chances of any kind of societal change being halted. “Social movements are not distinct and self-contained; rather, they grow from and give birth to other movements, work in coalition with other movements, and influence each other indirectly through their effects on the larger cultural and political environment¹⁹.” If the government can monitor and stop one major movement they can influence and deter the masses from further radical ideology. In this lies the ethical violation. Under utilitarian, duty-based, and rights-based ethical theories the act of heavy government surveillance policy is an ethical violation. From a utilitarian perspective the government is not acting in line with what is the greatest good for the greatest number. The greatest good is allowing a society to have the ability to freely participate and change the system in order to adhere to what is best for the people. By limiting radical political groups the government can effectively take away this ability. In taking the ability to change and progress away from the people the government violates the greatest good for the greatest number. The duty-based and rights-based theories also show extreme surveillance to be an ethical violation. These theories examine how government surveillance is carried out and the ethical and legal violations that are inherent in the practices. From a duty-based perspective, heavy government surveillance is an ethical violation because it does not treat people in a universal or impartial way. It is often carried out with heavy biases against certain types of groups and ideologies. Not only is the surveillance bias towards particular groups but it also violates several rules and regulations stated in our countries legal doctrines. Surveillance practices of the FBI and other government groups have shown to violate several laws and the rights of the group participants. This type of surveillance discourse causes it to be an ethical violation.

The democratic system needs free political participation and radical movements in order to progress.

History has shown the positive effects radical groups have played in the progression of American society through out U.S. history. If the unethical practices of government surveillance are not kept in check into the future, the ideologies of freedom of speech and the power of the people will be lost forever.

Actions determine morality, not results—consequentialism might be good, but moral side constraints exist that we cannot violate

NAGEL 1979 (Thomas, Philosopher, Mortal Questions, p 58-59)

Many people feel, without being able to say much more about it, that something has gone seriously wrong when certain measures are admitted into consideration in the first place. The fundamental mistake is made there, rather than at the point where the overall benefit of some monstrous measure is judged to outweigh its disadvantages, and it is adopted. An account of absolutism might help us to understand this. If it is not allowable to do certain things, such as killing unarmed prisoners or civilians, then no argument about what will happen if one does not do them can show that doing them would be all right. Absolutism does not, of course, require one to ignore the consequences of one's acts. It operates as a limitation on utilitarian reasoning, not as a substitute for it. An absolutist can be expected to try to maximize good and minimize evil, so long as this does not require him to transgress an absolute prohibition like that against murder. But when such a conflict occurs, the prohibition takes complete precedence over any consideration of consequences. Some of the results of this view are clear enough. It requires us to forgo certain potentially useful military measures, such as the slaughter of hostages and prisoners or indiscriminate attempts to reduce the enemy population by starvation, epidemic infectious diseases like anthrax and bubonic plague, or mass incineration. It means that we cannot deliberate on whether such measures are justified by the fact that they will avert still greater evils, for as intentional measures they cannot be justified in terms of any consequences whatever. Someone unfamiliar with the events of this century might imagine that utilitarian arguments, or arguments of national interest, would suffice to deter measures of this sort. But it has become evident that such considerations are insufficient to prevent the adoption and employment of enormous antipopulation weapons once their use is considered a serious moral possibility. The same is true of the piecemeal wiping out of rural civilian populations in airborne antiguerrilla warfare. Once the door is opened to calculations of utility and national interest, the usual speculations about the future of freedom, peace, and economic prosperity can be brought to bear to ease the consciences of those responsible for a certain number of charred babies.

Our advantage is one of those side constraints—the injustices we have described should not be tolerated at any cost

RAWLS 1971 (John, philosopher, A Theory of Justice, p. 3-4)

Justice is the first virtue of social institutions as truth is of systems of thought. A theory however elegant and economical must be rejected or revised if it is untrue; likewise laws and institutions no matter how efficient and well-arranged must be reformed or abolished if they are unjust. Each person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override. For this reason justice denies that the loss of freedom for some is made right by a greater good shared by others. It does not allow that the sacrifices imposed on a few are outweighed by the larger sum of advantages enjoyed by the many. Therefore in a just society the liberties of equal citizenship are taken as settled; the rights secured by justice are not subject to political bargaining or to the calculus of social interests. The only thing that permits us to acquiesce in an erroneous theory is the lack of a better one; analogously, an injustice is tolerable only when it is necessary to avoid an even greater injustice. Being first virtues of human activities, truth and justice are uncompromising.

No consequence justifies voting neg—either rights are absolute and we win, or they're not, and the neg's moral calculus is incoherent. The question of this debate is whether the plan is a *moral action* or not. The judge as a moral agent is not responsible for intervening actors no matter how bad the consequences sound. The decisions of other agents are outside your power to determine and you should therefore say that you support the aff even if we should perhaps also stop bad consequences that stem from it because consequentialism with no limit results in constantly escalating evils which make it self-defeating and also undermines the value of life

GEWIRTH 1981 (Alan, prof of philosophy at U Chicago, “Are There Any Absolute Rights?,” Philosophical Quarterly, January)

It is a widely held opinion that there are no absolute rights. Consider what would be generally regarded as the most plausible candidate: the right to life. This right entails at least the negative duty to refrain from killing any human being. But it is contended that this duty may be overridden, that a person may be justifiably killed if this is the only way to prevent him from killing some other, innocent person, or if he is engaged in combat in the army of an unjust aggressor nation with which one's own country is at war. It is also maintained that even an innocent person may justifiably be killed if failure to do so will lead to the deaths of other such persons. Thus an innocent person's right to life is held to be overridden when a fat man stuck in the mouth of a cave prevents the exit of speleologists who will otherwise drown, or when a child or some other guiltless person is strapped onto the front of an aggressor's tank, or when an explorer's choice to kill one among a group of harmless natives about to be executed is the necessary and sufficient condition of the others' being spared, or when the driver of a runaway trolley can avoid killing five persons on one track only by killing one person on another track.¹ And topping all such tragic examples is the catastrophic situation where a nuclear war or some other unmitigated disaster can be avoided only by infringing some innocent person's right to life. Despite such cases, I shall argue that certain rights can be shown to be absolute. But first the concept of an absolute right must be clarified.

1. I begin with the Hohfeldian point that the rights here in question are claim-rights (as against liberties, powers, and so forth) in that they are justified claims or entitlements to the carrying out of correlative duties, positive or negative. A duty is a requirement that some action be performed or not be performed; in the latter, negative case, the requirement constitutes a prohibition.

A right is fulfilled when the correlative duty is carried out, i.e., when the required action is performed or the prohibited action is not performed. A right is infringed when the correlative duty is not carried out, i.e., when the required action is not performed or the prohibited action is performed. Thus someone's right to life is infringed when the prohibited action of killing him is performed; someone's right to medical care is infringed when the required action of providing him with medical care is not performed. A right is violated when it is unjustifiably infringed, i.e., when the required action is unjustifiably not performed or the prohibited action is unjustifiably performed. And a right is overridden when it is justifiably infringed, so that there is sufficient justification for not carrying out the correlative duty, and the required action is justifiably not performed or the prohibited action is justifiably performed.

A right is absolute when it cannot be overridden in any circumstances, so that it can never be justifiably infringed and it must be fulfilled without any exceptions.

The idea of an absolute right is thus doubly normative: it includes not only the idea, common to all claim-rights, of a justified claim or entitlement to the performance or non-performance of certain actions, but also the idea of the exceptionless justifiability of performing or not performing those actions as required. These components show that the question whether there are any absolute rights demands for its adequate answer an explicit concern with criteria of justification. I shall here assume what I have elsewhere argued for in some detail: that these criteria, insofar as they are valid, are ultimately based on a certain supreme principle of morality, the Principle of Generic Consistency [PGC].^{*} This

principle requires of every agent that he act in accord with the generic rights of his recipients as well as of himself, i.e., that he fulfil these rights. The generic rights are rights to the necessary conditions of action, freedom and well-being, where the latter is defined in terms of the various substantive abilities and conditions needed for action and for successful action in general. The POC provides the ultimate justificatory basis for the validity of these rights by showing that they are equally had by all prospective purposive agents, and it also provides in general for the ordering of the rights in cases of conflict. Thus if two moral rights are so related that each can be fulfilled only by infringing the other, that right takes precedence whose fulfilment is more necessary for action. This criterion of degrees of necessity for action explains, for example, why one person's right not to be lied to must give way to another person's right not to be killed when these two rights are in conflict. In some cases the application of this criterion requires a context of institutional rules.

2. The general formula of a right is as follows: "A has a right to X against B by virtue of Y". In addition to the right itself, there are four elements here: the subject of the right, the right-holder (A); the object of the right (X); the respondent of the right, the person who has the correlative duty (B); and the justificatory basis or ground of the right (Y). I shall refer to these elements jointly as the contents of the right. Each of the elements may vary in generality. Various rights may conflict with one another as to one or another of these elements, so that not all rights can be absolute.

One aspect of these conflicts is especially important for understanding the question of absolute rights. Although, as noted above, the objects of moral rights are hierarchically ordered (according to the degree of their necessity for action), this is not true of the subjects of the rights. If one class or group of persons inherently had superior moral rights over another class or group (as was held to be the case throughout much of human history), any conflict between their respective rights would be readily resolvable: the rights of the former group would always take precedence, they would never be overridden (at least by the rights of members of other groups), and to this extent they would be absolute.⁸ It is because (as is shown by the PGC as well as by other moral principles) moral rights are equally distributed among all human persons as prospective purposive agents that some of the main conflicts of rights arise. This is most obviously the case where one person's right to life conflicts with another person's, since in the absence of guilt on either side, it is assumed that the two persons have equal rights. Thus the difficulty of supporting the thesis that there are absolute rights derives much of its force from its connection with the principle that all persons are equal in their moral rights.

3. The differentiation of the elements of rights serves to explicate the various levels at which rights may be held to be absolute. We may distinguish three such levels. The first is that of Principle Absolutism. According to this, what is absolute, and thus always valid and never overridden, is only some moral principle of a very high degree of generality which, referring to the subjects, the respondents, and especially the objects of rights in a relatively undifferentiated way, presents a general formula for all the diverse duties of all respondents or agents toward all subjects or recipients. The PGC is such a principle; so too are the Golden Rule, the law of love, Kant's categorical imperative, and the principle of utility. Principle Absolutism, however, may leave open the question whether any specific rights are always absolute, and what is to be done in cases of conflict. Even act-utilitarianism might be an example of Principle Absolutism, for it may be interpreted as saying that those rights are absolute whose fulfillment would serve to maximize utility overall. These rights, whatever they may be, might of course vary in their specific contents from one situation to another.

At the opposite extreme is Individual Absolutism, according to which an individual person has an absolute right to some particular object at a particular time and place when all grounds for overriding the right in the particular case have been overcome. But this still leaves open the question of what are the general grounds or criteria for overriding any right, and what are the other specific relevant contents of such rights.

It is at the intermediate level, that of Rule Absolutism, that the question of absolute rights arises most directly. At this level, the rights whose absoluteness is in question are characterized in terms of specific objects with possible specification also of subjects and respondents, so that a specific rule can be stated describing the content of the right and the correlative duty. The description will not use proper names and other individual referring expressions, as in the case of Individual Absolutism, nor will it consist only in a general formula applicable to many specifically different kinds of rights and duties and hence of objects, subjects, and respondents, as in the case of Principle Absolutism. It is at this level that one asks whether the right to life of all persons or of all innocent persons is absolute, whether the rights to freedom of speech and of religion are absolute, and so forth. The rights whose absoluteness is considered at the level of Rule Absolutism may vary in degree of generality, in that their objects, their subjects, and their respondents may be given with greater or lesser specificity. Thus there is greater specificity as we move along the following scale: the right of all persons to life, the right of all innocent persons to life, the right of all innocent persons to an economically secure life, the right of children to receive an economically secure and emotionally satisfying life from their parents, and so forth.

This variability raises the following problem. For a right to be absolute, it must be conclusively valid without any exceptions. But, as we have seen, rights may vary in generality, and all the resulting specifications of their objects, subjects, or respondents may constitute exceptions to the more general rights in which such specifications are not present. For example, the right of innocent persons to life may incorporate an exception to the right of all persons to life, for the rule embodying the former right may be stated thus: All persons have a right not to be killed except when the persons are not innocent, or except when such killing is directly required in order to prevent them from killing somebody else. Similarly, when it is said that all persons have a right to life, the specification of "persons" may suggest (although it does not strictly entail) the exception-making rule that all animals (or even all organisms) have a right to life except when they are not persons (or not human). Hence, since an absolute right is one that is valid without any exceptions, it may be concluded either that no rights are absolute because all involve some specification, or that all rights are equally absolute because once their specifications are admitted they are entirely valid without any further exceptions.

The solution to this problem consists in seeing that not all specifications of the subjects, objects, or respondents of moral rights constitute the kinds of exception whose applicability to a right debars it from being absolute. I shall indicate three criteria for permissible specifications. First, when it is asked concerning some moral right whether it is absolute, the kind of specification that may be incorporated in the right can only be such as results in a concept that is recognizable to ordinary practical thinking. This excludes rights that are "overloaded with exceptions" as well as those whose application would require intricate utilitarian calculations.⁴

Second, the specifications must be justifiable through a valid moral principle. Since, as we saw above, the idea of an absolute right is doubly normative, a right with its specification would not even begin to be a candidate for absoluteness unless the specification were morally justified and could hence be admitted as a condition of the justifiability of the moral right. There is, for example, a good moral justification for incorporating the restriction of innocence on the subjects of the right not to be killed; but there is not a similarly good moral justification for incorporating racial, religious, and other such particularist specifications. It must be emphasized, however, that this moral specification guarantees only that the right thus specified is an appropriate candidate for being absolute; it is, of itself, not decisive as to whether the right is absolute.

A third criterion is that the permissible specification of a right must exclude any reference to the possibly disastrous consequences of fulfilling the right. Since a chief difficulty posed against absolute rights is that for any right there can be cases in which its fulfillment may have disastrous consequences, to put this reference into the very description of the right would remove one of the main grounds for raising the question of absoluteness. The relation between rights and disasters is complicated by the fact that the latter, when caused by the actions of persons, are themselves infringements of rights. This point casts a new light on the consequentialist's thesis that there are no absolute rights. For when he says that every right may be overridden if this is required in order to avoid certain catastrophes—such as when torture alone will enable the authorities to ascertain where a terrorist has hidden a fused charge of dynamite—the consequentialist is appealing to basic rights. He is saying that in such a case one right—the right not to be tortured—is overridden by another right—the right to life of the many potential victims of the explosion. This raises the following question. Can the process of one right's overriding another continue indefinitely or does the process come to a stop with absolute rights?

In order to deal with this question, two points must be kept in mind. First, even when catastrophes threatening the infringement of basic rights are invoked to override other rights, at least part of the problem created by such conflict depends, as was noted above, on the assumption that all the persons involved have equal moral rights. There would be no serious conflict of rights and no problem about absolute rights if, for example, the rights of the persons threatened by the catastrophe were deemed inferior to those of persons not so threatened.

Second, despite the close connection between rights in general and the rights threatened by disastrous consequences, it is important to distinguish them. For if the appeal to avoidance of disastrous consequences were to be construed simply as an appeal for the fulfillment or protection of certain basic rights, then, on the assumption that certain disasters must always be avoided when they are threatened, the consequentialist would himself be an absolutist. We can escape this untoward result and render more coherent the opposition between absolutism and consequentialism if we recognize a further important assumption of the question whether there are any absolute rights. Amid the various possible specifications of Rule Absolutism, the rights in question are the normative property of distinct individuals.⁶ In referring to some event as a "disaster" or a "catastrophe", on the other hand, what is often meant is that a large mass of individuals taken collectively loses some basic good to which they have a right. It is their aggregate loss that constitutes the catastrophe. (This, of course, accounts for the close connection between the appeal to disastrous consequences and utilitarianism.) Thus the question whether there are any absolute rights is to be construed as asking whether distinct individuals, each of whom has equal moral rights (and who are to be characterized, according to the conditions of Rule Absolutism, by specifications that are morally justifiable and recognizable to ordinary practical thinking), have any rights that may never be overridden by any other considerations, including even their catastrophic consequences for collective rights. II

4. We must now examine the merits of the prime consequentialist argument against the possibility of absolute moral rights: that circumstances can always be imagined in which the consequences of fulfilling the rights would be so disastrous that their requirements would be overridden. The formal structure of the argument is as follows: (1) If R, then D. (2) 0 (~D). (3) Therefore, 0 (~R). For example, (1) if some person's right to life is fulfilled in certain circumstances, then some great disaster may or will occur. But (2) such disaster ought never to (be allowed to) occur. Hence, (3) in such circumstances the right ought not to be fulfilled, so that it is not absolute. Proponents of this argument have usually failed to notice that a parallel argument can be given in the opposite direction. If exceptions to the fulfillment of any moral right can be justified by imagining the possible disastrous consequences of fulfilling it, why cannot exceptionless moral rights be justified by giving them such contents that their infringement would be unspeakably evil? The argument to this effect may be put formally as follows: (1) If ~R, then E. (2) 0 (~E). (3) Therefore, 0(R). For example, (1) if a mother's right not to be tortured to death by her own son is not fulfilled, then there will be unspeakable evil. But (2) such evil ought never to (be allowed to) occur. Hence, (3) the right ought to be fulfilled without any exceptions, so that it is absolute.

Two preliminary points must be made about these arguments. First, despite their formal parallelism, there is an important difference in the meaning of 'then' in their respective first premises. In the first argument, 'then' signifies a consequential causal connection: if someone's right to life is fulfilled, there may or will ensue as a result the quite distinct phenomenon of a certain great disaster. But in the second argument, 'then' signifies a moral conceptual relation: the unspeakable evil is not a causal consequence of a mother's being tortured to death by her own son; it is rather a central moral constituent of it. Thus the second argument is not consequentialist, as the first one is, despite the fact that each of their respective first premises has the logical form of antecedent and consequent.

A related point bears on the second argument's specification of the right in question as a mother's right not to be tortured to death by her own son. This specification does not transgress the third requirement given above for permissible specifications: that reference to disastrous consequences must not be included in the formulation of the right. For the torturing to death is not a disastrous causal consequence of infringing the right; it is directly an infringement of the right itself, just as not being tortured to death by her own son is not a consequence of fulfilling the right but is the right. This distinction can perhaps be seen more clearly in such a less extreme case as the right not to be lied to. Being told a lie is not a causal consequence of infringing this right; rather, it just is an infringement of the right. In each case, moreover, the first two requirements for permissible specifications of moral rights are also satisfied: their contents are recognizable to ordinary practical thinking and they are justified by a valid moral principle. 5. Let us now consider the right mentioned above: a mother's right not to be tortured to death by her own son. Assume (although these specifications are here quite dispensable) that she is innocent of any crime and has no knowledge of any. What justifiable exception could there be to such a right? I shall construct an example which, though fanciful, has sufficient analogues in past and present thought and action to make it relevant to the status of rights in the real world.⁶

Suppose a clandestine group of political extremists have obtained an arsenal of nuclear weapons; to prove that they have the weapons and know how to use them, they have kidnapped a leading scientist, shown him the weapons, and then released him to make a public corroborative statement. The terrorists have now announced that they will use the weapons against a designated large distant city unless a certain prominent resident of the city, a young politically active lawyer named Abrams, tortures his mother to death, this torturing to be carried out publicly in a certain way at a specified place and time in that city. Since the gang members have already murdered several other prominent residents of the city, their threat is quite credible. Their declared motive is to advance their cause by showing how powerful they are and by unmasking the moralistic pretensions of their political opponents.

Ought Abrams to torture his mother to death in order to prevent the threatened nuclear catastrophe? Might he not merely pretend to torture his mother, so that she could then be safely hidden while the hunt for the gang members continued? Entirely apart from the fact that the gang could easily pierce this deception, the main objection to the very raising of such questions is the moral one that they seem to hold open the possibility of acquiescing and participating in an unspeakably evil project. To inflict such extreme harm on one's mother would be an ultimate act of betrayal; in performing or even contemplating the performance of such an action the son would lose all self-respect and would regard his life as no longer worth living.⁷ A mother's right not to be tortured to death by her own son is beyond any compromise. It is absolute.

This absoluteness may be analysed in several different interrelated dimensions, all stemming from the supreme principle of morality. The principle requires respect for the rights of all persons to the necessary conditions of human action, and this includes respect for the persons themselves as having the rational capacity to reflect on their purposes and to control their behaviour in the light of such reflection. The principle hence prohibits using any person merely as a means to the well-being of other persons. For a son to torture his mother to death even to protect the lives of others would be an extreme violation of this principle and hence of these rights, as would any attempt by others to force such an action. For this reason, the concept appropriate to it is not merely ‘wrong’ but such others as ‘despicable’, ‘dishonourable’, ‘base’, ‘monstrous’. In the scale of moral modalities, such concepts function as the contrary extremes of concepts like the supererogatory.

What is supererogatory is not merely good or right but goes beyond these in various ways; it includes saintly and heroic actions whose moral merit surpasses what is strictly required of agents. In parallel fashion, what is base, dishonourable, or despicable is not merely bad or wrong but goes beyond these in moral demerit since it subverts even the minimal worth or dignity both of its agent and of its recipient and hence the basic presuppositions of morality itself. Just as the supererogatory is superlatively good, so the despicable is superlatively evil and diabolic, and its moral wrongness is so rotten that a morally decent person will not even consider doing it. This is but another way of saying that the rights it would violate must remain absolute.

6. There is, however, another side to this story. What of the thousands of innocent persons in the distant city whose lives are imperilled by the threatened nuclear explosion? Don't they too have rights to life which, because of their numbers, are far superior to the mother's right? May they not contend that while it is all very well for Abrams to preserve his moral purity by not killing his mother, he has no right to purchase this at the expense of their lives, thereby treating them as mere means to his ends and violating their own rights? Thus it may be argued that the morally correct description of the alternative confronting Abrams is not simply that it is one of not violating or violating an innocent person's right to life, but rather not violating one innocent person's right to life and thereby violating the right to life of thousands of other innocent persons through being partly responsible for their deaths, or violating one innocent person's right to life and thereby protecting or fulfilling the right to life of thousands of other innocent persons. We have here a tragic conflict of rights and an illustration of the heavy price exacted by moral absolutism. The aggregative consequentialist who holds that that action ought always to be performed which maximizes utility or minimizes disutility would maintain that in such a situation the lives of the thousands must be preferred.

An initial answer may be that terrorists who make such demands and issue such threats cannot be trusted to keep their word not to drop the bombs if the mother is tortured to death; and even if they now do keep their word, acceding in this case would only lead to further escalated demands and threats. It may also be argued that it is irrational to perpetrate a sure evil in order to forestall what is so far only a possible or threatened evil. Philippa Foot has sagely commented on cases of this sort that if it is the son's duty to kill his mother in order to save the lives of the many other innocent residents of the city, then “anyone who wants us to do something we think wrong has only to threaten that otherwise he himself will do some- thing we think worse”.⁸ Much depends, however, on the nature of the “wrong” and the “worse”. If someone threatens to commit suicide or to kill innocent hostages if we do not break our promise to do some relatively unimportant action, breaking the promise would be the obviously right course, by the criterion of degrees of necessity for action. The special difficulty of the present case stems from the fact that the conflicting rights are of the same supreme degree of importance.

It may be contended, however, that this whole answer, focusing on the probable outcome of obeying the terrorists' demands, is a consequentialist argument and, as such, is not available to the absolutist who insists that Abrams must not torture his mother to death whatever the consequences.⁹ This contention imputes to the absolutist a kind of indifference or even callousness to the sufferings of others that is not warranted by a correct understanding of his position. He can be concerned about consequences so long as he does not regard them as possibly superseding or diminishing the right and duty he regards as absolute. It is a matter of priorities. So long as the mother's right not to be tortured to death by her son is unqualifiedly respected, the absolutist can seek ways to mitigate the threatened disastrous consequences and possibly to avert, them altogether. A parallel case is found in the theory of legal punishment: the retributivist, while asserting that punishment must be meted out only to the persons who deserve it because of the crimes they have committed, may also uphold punishment for its deterrent effect so long as the latter, consequentialist consideration is subordinated to and limited by the conditions of the former, antecedentalist consideration.¹⁰ Thus the absolutist can accommodate at least part of the consequentialist's substantive concerns within the limits of his own principle.

Is any other answer available to the absolutist, one that reflects the core of his position? Various lines of argument may be used to show that in refusing to torture his mother to death Abrams is not violating the rights of the multitudes of other residents who may die as a result, because he is not morally responsible for their deaths. Thus the absolutist can maintain that even if these others die they still have an absolute right to life because the infringement of their right is not justified by the argument he upholds. At least three different distinctions may be adduced for this purpose. In the unqualified form in which they have hitherto been presented, however, they are not successful in establishing the envisaged conclusion.

One distinction is between direct and oblique intention. When Abrams refrains from torturing his mother to death, he does not directly intend the many ensuing deaths of the other inhabitants either as end or as means. These are only the foreseen but unintended side-effects of his action or, in this case, inaction. Hence, he is not morally responsible for those deaths. Apart from other difficulties with the doctrine of double effect, this distinction as so far stated does not serve to exculpate Abrams. Consider some parallels. Industrialists who pollute the environment with poisonous chemicals and manufacturers who use carcinogenic food additives do not directly intend the resulting deaths; these are only the unintended but foreseen side-effects of what they do directly intend, namely, to provide profitable demand-fulfilling commodities. The entrepreneurs in question may even maintain that the enormous economic contributions they make to the gross national product outweigh in importance the relatively few deaths that regrettably occur. Still, since they

have good reason to believe that deaths will occur from causes under their control, the fact that they do not directly intend the deaths does not remove their causal and moral responsibility for them. Isn't this also true of Abrams's relation to the deaths of the city's residents?

A second distinction drawn by some absolutists is between killing and letting die. This distinction is often merged with others with which it is not entirely identical, such as the distinctions between commission and omission, between harming and not helping, between strict duties and generosity or supererogation. For the present discussion, however, the subtle differences between those may be overlooked. The contention, then, is that in refraining from killing his mother, Abrams does not kill the many innocent persons who will die as a result; he only lets them die. But one does not have the same strict moral duty to help persons or to prevent their dying as one has not to kill them; one is responsible only for what one does, not for what one merely allows to happen. Hence, Abrams is not morally responsible for the deaths he fails to prevent by letting the many innocent persons die, so that he does not violate their rights to life.

The difficulty with this argument is that the duties bearing on the right to life include not only that one not kill innocent persons but also that one not let them die when one can prevent their dying at no comparable cost. If, for example, one can rescue a drowning man by throwing him a rope, one has a moral duty to throw him the rope. Failure to do so is morally culpable. Hence, to this extent the son who lets the many residents die when he can prevent this by means within his power is morally responsible for their deaths.

A third distinction is between respecting other persons and avoiding bad consequences. Respect for persons is an obligation so fundamental that it cannot be overridden even to prevent evil consequences from befalling some persons. If such prevention requires an action whereby respect is withheld from persons, then that action must not be performed, whatever the consequences.

One of the difficulties with this important distinction is that it is unclear. May not respect be withheld from a person by failing to avert, from him some evil consequence? How can Abrams be held to respect the thousands of innocent persons or their rights if he lets them die when he could have prevented this? The distinction also fails to provide for degrees of moral urgency. One fails to respect a person if one lies to him or steals from him; but sometimes the only way to prevent the death of one innocent person may be by stealing from or telling a lie to some other innocent person. In such a case, respect for one person may lead to disrespect of a more serious kind for some other innocent person.

7. None of the above distinctions, then, serves its intended purpose of defending the absolutist against the consequentialist. They do not show that the son's refusal to torture his mother to death does not violate the other persons' rights to life and that he is not morally responsible for their deaths. Nevertheless, the distinctions can be supplemented in a way that does serve to establish these conclusions.

The required supplement is provided by the principle of the intervening action. According to this principle, when there is a causal connection between some person A's performing some action (or inaction) X and some other person C's incurring a certain harm Z, A's moral responsibility for Z is removed if, between X and Z, there intervenes some other action Y of some person B who knows the relevant circumstances of his action and who intends to produce Z or who produces Z through recklessness. The reason for this removal is that B's intervening action Y is the more direct or proximate cause of Z and, unlike A's action (or inaction), Y is the sufficient condition of Z as it actually occurs.¹¹

An example of this principle may help to show its connection with the absolutist thesis. Martin Luther King Jr. was repeatedly told that because he led demonstrations in support of civil rights, he was morally responsible for the disorders, riots, and deaths that ensued and that were shaking the American Republic to its foundations.¹² By the principle of the intervening action, however, it was King's opponents who were responsible because their intervention operated as the sufficient conditions of the riots and injuries. King might also have replied that the Republic would not be worth saving if the price that had to be paid was the violation of the civil rights of black Americans. As for the rights of the other Americans to peace and order, the reply would be that these rights cannot justifiably be secured at the price of the rights of blacks.

It follows from the principle of the intervening action that it is not the son but rather the terrorists who are morally as well as causally responsible for the many deaths that do or may ensue on his refusal to torture his mother to death. The important point is not that he lets these persons die rather than kills them, or that he does not harm them but only fails to help them, or that he intends their deaths only obliquely but not directly. The point is rather that, it is only through the intervening lethal actions of the terrorists that his refusal eventuates in the many deaths. Since the moral responsibility is not the son's, it does not affect his moral duty not to torture his mother to death, so that her correlative right remains absolute.

This point also serves to answer some related questions about the rights of the many in relation to the mother's right. Since the son's refusal to torture his mother to death is justified, it may seem that the many deaths to which that refusal will lead are also justified, so that the rights to life of these many innocent persons are not absolute. But since they are innocent, why aren't their rights to life as absolute as the mother's? If, on the other hand, their deaths are unjustified, as seems obvious, then isn't the son's refusal to torture his mother to death also unjustified, since it leads to those deaths? But from this it would follow that the mother's right not to be tortured to death by her son is not absolute, for if the son's not infringing her right is unjustified, then his infringing it would presumably be justified. The solution to this difficulty is that it is a fallacy to infer, from the two premises

(1) the son's refusal to kill his mother is justified and (2) many innocent persons die as a result of that refusal, to the conclusion (3) their deaths are justified. For, by the principle of the intervening action, the son's refusal is not causally or morally responsible for the deaths; rather, it is the terrorists who are responsible. Hence, the justification referred to in (1) does not carry through to (2). Since the terrorists' action in ordering the killings is unjustified, the resulting deaths are unjustified. Hence, the rights to life of the many innocent victims remain absolute even if they are killed as a result of the son's justified refusal, and it is not he who violates their rights. He may be said to intend the many deaths obliquely, in that they are a foreseen but unwanted side-effect of his refusal. But he is not responsible for that side-effect because of the terrorists' intervening action.

It would be unjustified to violate the mother's right to life in order to protect the rights to life of the many other residents of the city. For rights cannot be justifiably protected by violating another right which, according to the criterion of degrees of necessity for action, is at least equally important. Hence, the many other residents do not have a right that the mother's right to life be violated for their sakes. To be sure, the mother also does not have a right that their equally important rights be violated in order to protect hers. But here too it must be emphasized that in protecting his mother's right the son does not violate the rights of the others;

for by the principle of the intervening action, it is not he who is causally or morally responsible for their deaths. Hence too he is not treating them as mere means to his or his mother's ends.

8. Where, then, does this leave us? From the absoluteness of the mother's right not to be tortured to death by her son, does it follow that in the described circumstances a nuclear explosion should be permitted to occur over the city so that countless thousands of innocent persons may be killed, possibly including Abrams and his mother?

Properly to deal with this question, it is vitally important to distinguish between abstract and concrete absolutism. The abstract absolutist at no point takes account of consequences or of empirical or causal connections that may affect the subsequent outcomes of the two alternatives he considers. He views the alternatives as being both mutually exclusive and exhaustive. His sole concern is for the moral guiltlessness of the agent, as against the effects of the agent's choices for human weal or woe.

In contrast, as I suggested earlier, the concrete absolutist is concerned with consequences and empirical connections, but always within the limits of the right he upholds as absolute. His consequentialism is thus limited rather than unlimited. Because of his concern with empirical connections, he takes account of a broader range of possible alternatives than the simple dualism to which the abstract absolutist confines himself. His primary focus is not on the moral guiltlessness of the agent but rather on the basic rights of persons not to be subjected to unspeakable evils. Within this focus, however, the concrete absolutist is also deeply concerned with the effects of the fulfilment of these rights on the basic well-being of other persons. The significance of this distinction can be seen by applying it to the case of Abrams. If he is an abstract absolutist, he deals with only two alternatives which he regards as mutually exclusive as well as exhaustive: (1) he tortures his mother to death; (2) the terrorists drop a nuclear bomb killing thousands of innocent persons. For the reasons indicated above, he rejects (1). He is thereby open to the accusation that he chooses (2) or at least that he allows (2) to happen, although the principle of the intervening action exempts him from moral guilt or responsibility.

If, how'ever, Abrams is a concrete absolutist, then he does not regard himself as being confronted only by these two terrible alternatives, nor does he regard them or their negotiations as mutually exclusive. His thought-processes include the following additional considerations. In accordance with a point suggested above, he recognizes that his doing (1) will not assure the non-occurrence of (2). On the contrary, his doing (1) will probably lead to further threats of the occurrence of (2) unless he or someone else performs further unspeakably evil actions (3), (4), and so forth. (A parallel example may be found in Hitler's demand for Czechoslovakia at Munich after his taking over of Austria, his further demand for Poland after the capitulation regarding Czechoslovakia, and the ensuing tragedies.) Moreover, (2) may occur even if Abrams does (1). For persons who are prepared to threaten that they will do (2) cannot be trusted to keep their word.

On the other hand, Abrams further reasons, his not doing (1) may well not lead to (2). This may be so for several reasons. He or the authorities or both must try to engage the terrorists in a dialogue in which their grievances are publicized and seriously considered. Whatever elements of rationality may exist among the terrorists will thereby be reinforced, so that other alternatives may be presented. At the same time, a vigorous search and preventive action must be pursued so as to avert the threatened bombing and to avoid any recurrences of the threat. It is such concrete absolutism, taking due account of consequences and of possible alternatives, that constitutes the preferred pattern of ethical reasoning. It serves to protect the rights presupposed in the very possibility of a moral community while at the same time it gives the greatest probability of averting the threatened catastrophe. In the remainder of this paper, I shall assume the background of concrete absolutism.

9. I have thus far argued that the right of a mother not to be tortured to death by her son is absolute. But the arguments would also ground an extension of the kind of right here at issue to many other subjects and respondents, including fathers, daughters, wives, husbands, grandparents, cousins, and friends. So there are many absolute rights, on the criterion of plurality supplied by Rule Absolutism.

It is sometimes held that moral obligations are "agent-relative" in that, at least in cases of conflict, one ought to give priority to the welfare of those persons with whom one has special ties of family or affection.¹³ Applied to the present question, this view would suggest that the subjects having the absolute right that must be respected by respondents are limited to the kinds of relations listed above. It may also be thought that as we move away from familial and affectional relations, the proposed subjects of rights come to resemble more closely the anonymous masses of other persons who would be killed by a nuclear explosion, so that a quantitative measure of numbers of lives lost would become a more cogent consideration in allocating rights.

These conclusions, however, do not follow. Most of the arguments I have given above for the mother's absolute right not to be tortured to death apply to other possible human subjects without such specifications. My purpose in beginning with such an extreme case as the mother-son relation was to focus the issue as sharply as possible; but, this focus once gained, it may be widened in the ways just indicated. Although the mother has indeed a greater right to receive effective concern from her son than from other, unrelated persons, the unjustifiability of violating right[®] that are on the same level of necessity for action is not affected either by degrees of family relationship or by the numbers of persons affected. Abrams would not be justified in torturing to death some other innocent person in the described circumstances, and in failing to murder he would not be morally responsible for the deaths of other innocent persons who might be murdered by someone else as a consequence.

These considerations also apply to various progressively less extreme objects of rights than the not being tortured to death to which I have so far confined the discussion. The general content of these objects may be stated as follows: All innocent persons have an absolute right not to be made the intended victims of a homicidal project. This right, despite its increase in generality over the object, subject, and respondents of the previous right, still conforms to the requirements of Rule Absolutism. The word "intended" here refers both to direct and to oblique intention, with the latter being subject to the principle of the intervening action. The word "project" is meant to indicate a definite, deliberate design; hence, it excludes the kind of unforeseeable immediate crisis where, for example, the unfortunate driver of a trolley whose brakes have failed must choose between killing one person or five. The absolute right imposes a prohibition on any form of active participation in a homicidal project against innocent persons, whether by the original designers or by those who would accept its conditions with a view to warding off what they would regard as worse consequences. The meaning of "innocent" raises many questions of interpretation into

which I have no space to enter here, but some of its main criteria may be gathered from the first paragraph of this paper. As for 'persons', this refers to all prospective purposive agents.

The right not to be made the intended victim of a homicidal project is not the only specific absolute right, but it is surely one of the most important. The general point underlying all absolute rights stems from the moral principle presented earlier. At the level of Principle Absolutism, it may be stated as follow's: Agents and institutions are absolutely prohibited from degrading persons, treating them as if they had no rights or dignity. The benefit of this prohibition extends to all persons, innocent or guilty; for the latter, when they are justly punished, are still treated as responsible moral agents who are capable of understanding the principle of morality and acting accordingly, and the punishment must not be cruel or arbitrary. Other specific absolute rights may also be generated from this principle. Since the principle requires of every agent that he act in accord with the generic rights of his recipients as well as of himself, specific rights are absolute insofar as they serve to protect the basic presuppositions of the valid principle of morality in its equal application to all persons.

Dead bodies aren't the key metric for decisionmaking—surveillance might not be dramatic, but the failure to confront it now adds up to a worse harm over time as abuses accumulate

SOLOVE 2011 (Daniel, professor of law at George Washington University, Why Privacy Matters Even if You Have 'Nothing to Hide', May 15, <http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/>)

Investigating the nothing-to-hide argument a little more deeply, we find that it looks for a singular and visceral kind of injury. Ironically, this underlying conception of injury is sometimes shared by those advocating for greater privacy protections. For example, the University of South Carolina law professor Ann Bartow argues that in order to have a real resonance, privacy problems must "negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease." She says that privacy needs more "dead bodies," and that privacy's "lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other [types of harm]."

Bartow's objection is actually consistent with the nothing-to-hide argument. Those advancing the nothing-to-hide argument have in mind a particular kind of appalling privacy harm, one in which privacy is violated only when something deeply embarrassing or discrediting is revealed. Like Bartow, proponents of the nothing-to-hide argument demand a dead-bodies type of harm.

Bartow is certainly right that people respond much more strongly to blood and death than to more-abstract concerns. But if this is the standard to recognize a problem, then few privacy problems will be recognized. Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases.

Privacy is often threatened not by a single egregious act but by the slow accretion of a series of relatively minor acts. In this respect, privacy problems resemble certain environmental harms, which occur over time through a series of small acts by different actors. Although society is more likely to respond to a major oil spill, gradual pollution by a multitude of actors often creates worse problems.

Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone. When the government starts monitoring the phone numbers people call, many may shrug their shoulders and say, "Ah, it's just numbers, that's all." Then the government might start monitoring some phone calls. "It's just a few phone calls, nothing more." The government might install more video cameras in public places. "So what? Some more cameras watching in a few more places. No big deal." The increase in cameras might lead to a more elaborate network of video surveillance. Satellite surveillance might be added to help track people's movements. The government might start analyzing people's bank records. "It's just my deposits and some of the bills I pay—no problem." The government may then start combing through credit-card records, then expand to Internet-service providers' records, health records, employment records, and more. Each step may

seem incremental, but after a while, the government will be watching and knowing everything about us.

"My life's an open book," people might say. "I've got nothing to hide." But now the government has large dossiers of everyone's activities, interests, reading habits, finances, and health. What if the government leaks the information to the public? What if the government mistakenly determines that based on your pattern of activities, you're likely to engage in a criminal act? What if it denies you the right to fly? What if the government thinks your financial transactions look odd—even if you've done nothing wrong—and freezes your accounts? What if the government doesn't protect your information with adequate security, and an identity thief obtains it and uses it to defraud you? Even if you have nothing to hide, the government can cause you a lot of harm.

"But the government doesn't want to hurt me," some might argue. In many cases, that's true, but the government can also harm people inadvertently, due to errors or carelessness.

When the nothing-to-hide argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, then draws power from its unfair advantage. The nothing-to-hide argument speaks to some problems but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised with government security measures. When engaged directly, the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing-to-hide argument, in the end, has nothing to say.

"Life key to rights" is backwards—life and death are not inherently good except for the things we enjoy about them which the status quo erodes and the plan protects

Nagel 12 [Thomas, University Professor of Philosophy and Law at New York University, "Mortal Questions", Cambridge University Press, Mar 26, 2012, Pg.1-3]

If death is the unequivocal and permanent end of our existence, the question arises whether it is a bad thing to die.

There is conspicuous disagreement about the matter: some people think death is dreadful; others have no objection to death per se, though they hope their own will be neither premature nor painful. Those in the former category tend to think those in the latter are blind [not privy] to the obvious, while the latter suppose the former to be prey to some sort of confusion. On the one hand it can be said that life is all we have and the loss of it is the greatest loss we can sustain. On the other hand it may be objected that death deprives this supposed loss of its subject, and that if we realize that death is not an unimaginable condition of the persisting person, but a mere blank, we will see that it can have no value whatever, positive or negative.

Since I want to leave aside the question whether we are, or might be, immortal in some form, I shall simply use the word 'death' and its cognates in this discussion to mean permanent death, unsupplemented by any form of conscious survival. I want to ask whether death is in itself an evil; and how great an evil, and of what kind, it might be. The question should be of interest even to those who believe in some form of immortality, for one's attitude toward immortality must depend in part on one's attitude toward death.

If death is an evil at all, it cannot be because of its positive features, but only because of what it deprives us of. I shall try to deal with the difficulties surrounding the natural view that death is an evil because it brings to an end all the goods that life contains. We need not give an account of these goods here, except to observe that some of them, like perception, desire, activity, and thought, are so general as to be constitutive of human life. They are widely regarded as formidable benefits in themselves, despite the fact that they are conditions of misery as well as of happiness, and that a sufficient quantity of more particular evils can perhaps outweigh them. That is what is meant, I think, by the allegation that it is good simply to be alive, even if one is undergoing terrible experiences. The situation is roughly this: There are elements which, if added to one's experience, make life better; there are other elements which, if added to one's experience, make life worse. But what remains when these are set aside is not merely neutral: it is emphatically positive. Therefore life is worth living even when the bad elements of experience are plentiful, and the good ones too meager to outweigh the bad ones on their own. The additional positive weight is supplied by experience itself, rather than by any of its contents.

I shall not discuss the value that one person's life or death may have for others, or its objective value, but only the value it has for the person who is its subject. That seems to me the primary case, and the case which presents the greatest difficulties. Let me add only two observations. First, the value of life and its contents does not attach to mere organic survival: almost everyone would be indifferent (other things equal) between immediate death and immediate coma followed by death twenty years later without reawakening. And second, like most goods, this can be multiplied by time: more is better than less. The added quantities need not be temporally continuous (though continuity has its social advantages). People are attracted to the possibility of long-term suspended animation or freezing, followed by the resumption of conscious life, because they can regard it from within simply as continuation of their present life. If these techniques are ever perfected, what from outside appeared as a dormant interval of three hundred years could be experienced by the subject as nothing more than a sharp discontinuity in the character of his experiences. I do not deny, of course, that this has its own disadvantages. Family and friends may have died in the meantime; the language may have changed; the comforts of social, geographical, and cultural familiarity would be lacking. Nevertheless these inconveniences would not obliterate the basic advantage of continued, though discontinuous, existence.

If we turn from what is good about life to what is bad about death, the case is completely different. Essentially, though there may be problems about their specification, what we find desirable in life are certain states, conditions, or types of activity. It is being alive, doing certain things, having certain experiences that we consider good. But if death is an evil, it is the loss of life, rather than the state of being dead, or nonexistent, or unconscious, that is objectionable.¹ This asymmetry is important. If it is good to be alive, that advantage can be attributed to a person at each point of his life. It is a good of which Bach had more than Schubert, simply because he lived longer. Death, however, is not an evil of which Shakespeare has so far received a larger portion than Proust. If death is a disadvantage, it is not easy to say when a man suffers it.

The obsession with human survival is self-defeating—the tyranny of survival paradoxically destroys more people in the long run and diminishes the value of life

CALLAHAN 1973 (Daniel, institute of Society and Ethics, The Tyranny of Survival, p. 91-3) The value of survival could not be so readily abused were it not for its evocative power. But abused it has been. In the name of survival, all manner of social and political evils have been committed against the rights of individuals, including the right to life. The purported threat of Communist domination has for over two decades fueled the drive of militarists for ever-larger defense budgets, no matter what the cost to other social needs. During World War II, native Japanese-Americans were herded, without due process of law, to detention camps. This policy was later upheld by the Supreme Court in *Korematsu v. United States* (1944) in the general context that a threat to national security can justify acts otherwise blatantly unjustifiable. The survival of the Aryan race was one of the official legitimations of Nazism. Under the banner of survival, the government of South Africa imposes a ruthless apartheid, heedless of the most elementary human rights. The Vietnamese war has seen one of the greatest of the many absurdities tolerated in the name of survival: the destruction of villages in order to save them. But it is not only in a political setting that survival has been evoked as a final and unarguable value. The main rationale B. F. Skinner offers in Beyond Freedom and Dignity for the controlled and conditioned society is the need for survival. For Jacques Monod, in Chance and Necessity, survival requires that we overthrow almost every known religious, ethical and political system. In genetics, the survival of the gene pool has been put forward as sufficient grounds for a forceful prohibition of bearers of offensive genetic traits from marrying and bearing children. Some have even suggested that we do the cause of survival no good by our misguided medical efforts to find means by which those suffering from such common genetically based diseases as diabetes can live a normal life, and thus procreate even more diabetics. In the field of population and environment, one can do no better than to cite Paul Ehrlich, whose works have shown a high dedication to survival, and in its holy name a willingness to contemplate governmentally enforced abortions and a denial of food to surviving populations of nations which have not enacted population-control policies. For all these reasons it is possible to counterpose over against the need for survival a "tyranny of survival." There seems to be no imaginable evil which some group is not willing to inflict on another for sake of survival, no rights, liberties or dignities which it is not ready to suppress. It is easy, of course, to recognize the danger when survival is falsely and manipulatively invoked. Dictators never talk about their aggressions, but only about the need to defend the fatherland to save it from destruction at the hands of its enemies. But my point goes deeper than that. It is directed even at a legitimate concern for survival, when that concern is allowed to reach an intensity which would ignore, suppress or destroy other fundamental human rights and

values. The potential tyranny survival as value is that it is capable, if not treated sanely, of wiping out all other values. Survival can become an obsession and a disease, provoking a destructive singlemindedness that will stop at nothing. We come here to the fundamental moral dilemma. If, both biologically and psychologically, the need for survival is basic to man, and if survival is the precondition for any and all human achievements, and if no other rights make much sense without the premise of a right to life—then how will it be possible to honor and act upon the need for survival without, in the process, destroying everything in human beings which makes them worthy of survival. To put it more strongly, if the price of survival is human degradation, then there is no moral reason why an effort should be made to ensure that survival. It would be the Pyrrhic victory to end all Pyrrhic victories.

Privacy Impacts

The aff should win even under a utilitarian calculus—privacy isn’t about individual rights but the collective goods of a society where justice, deliberation, economic exchange and everything we care about is made possible by protection from the state

SIAVOSHY 2015 (Babak Siavoshy is a fellow and supervising attorney at the Samuelson Law, Technology & Public Policy Clinic at the UC Berkeley School of Law, Why privacy matters even if you don’t care about it (or, privacy as a collective good), Concurring Opinions, June 14, <http://concurringopinions.com/archives/2015/06/privacy-as-a-collective-good.html>)

This leads to what I think is the better (but perhaps more controversial) answer to the puzzle: privacy is worth protecting even if turns out most people don’t care about their own privacy. As counterintuitive as it seems, questions about privacy and surveillance don’t—and shouldn’t—hinge on individual privacy preferences.

That’s because questions about privacy rights, like questions about speech or voting or associative rights, are bigger than any individual or group. They are, instead, about the type of society we (including all those survey-takers) want to live in. Or as scholars have suggested, privacy is best thought of as a collective rather than merely an individual good

Privacy is like voting

Many of our most cherished rights, such as expressive, associational, and voting rights, are understood to protect both individual and collective interests. The right to vote, for example, empowers individuals to cast ballots in presidential elections. But the broader purpose of voting rights—their raison d’être—is to reach collective or systemic goods such as democratic accountability.

The fact that many individuals in the United States don’t vote doesn’t tell us much about whether the right to vote is worth protecting, let alone whether we should enact or scale back a particular set of voter protections. When it comes to voting, we intuitively understand that the right to vote has societal benefits that are worth protecting regardless of individuals’ attitudes towards voting. For example, the very existence of robust voting and electoral rights—the possibility that people might exercise their voting power if unhappy— incentivizes accountability on the part of government officials.

Privacy is like voting. Privacy rights create space for individual freedom, but their raison d'être is protecting broader societal and systemic goods. The point of protecting privacy rights—even rights that we choose not to exercise—is to facilitate the creation and furtherance of these social goods. Absent the space provided by the rights to private thought, private communications, and private associations, it is difficult to imagine how any of the major socio-political movements of the past century—from civil rights, to women's rights, and gay rights—could have survived long enough to influence policy.

The same, perhaps, can be said of major innovations in science, business, and technology. When properly balanced, privacy rights protect the creative process; they create space for deviance, and for experimentation; they allows for the testing and weeding out of weak arguments; they create new pathways for minority viewpoints and groups to gain public support, and for unpopular legal and political arguments to move from off the wall to on the wall.

The question of whether privacy rights are worth protecting is tied to the value we place on these systems and processes—and the public goods they facilitate—rather than to any individual’s interest in the secrecy of their own information. Even if it turns out to be true that most people don’t care about their privacy, that would not be enough to settle important questions about whether (and what) privacy rights society should protect. Privacy rights, like voting rights, are the types of rights that are worth protecting even if many of us don’t care to exercise them.

Rethinking privacy harms

Once we recognize that a critical purpose of privacy rights is to protect collective interests, we have to rethink some of the ways we evaluate privacy harms in our legal and political discourse. For example, courts and policymakers evaluating the harm from (say) data breach or overbroad surveillance must look beyond the intrusion on a particular individual's privacy and give weight to the broader societal harms of the legal rules or rulings being promulgated. In privacy cases, as with first amendment and voting rights cases, the harm to the individuals is often less important than the harm to society.

Unfortunately, courts and policymakers very often undervalue the societal harms of privacy intrusions. In data breach litigation, courts typically throw out privacy claims unless the victims can prove the data thieves misused their stolen information. This is a very high bar that does little justice to the many social costs of the poor security practices that cause data breach. In its 2012 decision in *Clapper v. Amnesty International*, the Supreme Court set a similarly high bar for plaintiffs challenging surveillance laws. The Clapper majority's decision was premised, again, on the theory that the plaintiffs could not prove that they suffered more than speculative harm from the government's expanded surveillance powers, which in the view of four dissenting justices had a "very strong likelihood" of ensnaring lawful communications.

In Fourth Amendment cases courts routinely contort themselves to force decisions with broad implications for collective interests (decisions that fundamentally affect "the right of the people to be secure") into a narrow individual-privacy box. Take *Maryland v. King*, in which the Supreme Court authorized Maryland's practice of genetic testing suspects arrested, but not charged or convicted, with a violent felony. The majority's operative legal analysis focused on the "negligible" intrusion caused when the police swabbed the suspect's cheek with a Q-Tip, and not the brave new world of warrantless genetic testing. In evaluating the reasonableness of the government's conduct, the majority weighed the degree to which the cheek-swab "intrudes upon an individual's privacy," on one hand, and "the promotion of legitimate governmental interests" in crime prevention, on the other.

Put otherwise, the Court weighed the right of the people of Maryland to efficient law enforcement against one man's right to have his cheek let alone. If it doesn't seem like a fair fight, it's because it's not. As the Court concluded, "[a] gentle rub along the inside of the cheek does not break the skin, and it involves virtually no risk, trauma, or pain"—a small price to pay for the safety of the people of Maryland. Not only does Court's legal analysis gives short shrift to societal implications of broadened genetic surveillance, it focuses on the wrong individual harm: the momentary (and "negligible") intrusion of a cheek-swab, rather than the privacy implications of suspicionless DNA searches and lifelong inclusion in ever-searchable, all but permanent, law enforcement DNA databanks.

The Court's pro-privacy decisions are often similarly contrived. In *U.S. v. Jones*, the Court held that the Fourth Amendment regulates the use of GPS trackers by law enforcement. The case presented difficult questions about the scope of privacy rights in public places in the face of new technologies that allow pervasive tracking of location and patterns of life. Instead of grappling with the implications of unchecked, ubiquitous location tracking, the Court fashioned a brand new legal rule rebuking the FBI's minor physical intrusion onto the undercarriage of Mr. Jones's Jeep. The Jones case, of course, wasn't about the car; it was about the broader implications of the type of unchecked, automated, warrantless location surveillance, which has become increasingly routine.

In *Jones*, as in *King*, the justices of the Supreme Court understood the impact of their rulings on collective interests—those stakes are addressed in the merits and amicus briefs, the concurrences and dissents, and even in the majority's dicta. But in each case, the Court went well out of its way to make those stakes seem tangential to what it framed as its real job, crafting rules to protect the cheeks and the car-undercarriages of individual Americans. This misses the forest for the trees. Even recognizing the need for strong limits on judicial decisionmaking (enforced in part through justiciability rules), one must believe that there is—there must be—better ways to do justice to the broader societal impact of legal rules that undermine privacy.

Privacy rights are worth protecting for reasons that go beyond any individual's interests in avoiding embarrassing disclosures, minor physical intrusions, or pecuniary damage. Privacy rights are worth protecting because they create space for innovation, creativity, expression, dissent, competition, and political participation. They are a condition precedent to the healthy functioning of our political and economic system. Policymakers and courts should do more to recognize these social and collective interests protected by privacy in their decisions.

Doctrinal implications

What are the doctrinal implications of recognizing privacy as a collective good? While there is no simple answer, we may look to our experience with other "collective rights" for guidance. When it comes to free expression, association, and voting, Courts and policymakers have long devised doctrinal mechanisms to fill the gaps between the individual and collective interests protected by these rights.

In First Amendment cases, courts apply a modified version of traditional standing requirements—the same requirements used to toss privacy and surveillance claims—to account for the societal harms of speech-chilling statutes. Under the Supreme Court's overbreadth cases, litigants may challenge speech restrictions that are substantially overbroad even where they are unable to demonstrate

individualized harm to their own speech rights. The collateral damage from overbroad statutes on speech and associational rights is just too high, and courts will strike such laws rather than to wait for the perfect litigant.

Courts have also relaxed standing requirements in election law. According to Saul Zipkin's 2014 piece Democratic Standing, when adjudicating disputes involving voting rights courts "attribute[] structural or probabilistic harms to plaintiffs without an individualized showing of particular harm." These doctrinal fixes are necessary to correct the awkward fit between the individual-harms focus of traditional standing doctrine and the core purpose of election law, which is the protection of a system and a process rather than of any individual vote:

Standing, premised on a litigant who has suffered injury in fact, fits awkwardly with election law, which often involves claims of harm to the electorate or the democratic process and presents contexts where it may be impossible to identify an individual who has suffered concrete harm. Surveying an array of election contexts [...] demonstrates that federal courts have applied standing in a distinct manner in this setting, thereby positioning themselves as monitors of the electoral process. [From the abstract].

Courts have not, to my knowledge, adopted similar corrective mechanisms in the context of privacy rights, though they have had several notable opportunities to do so (the Clapper case, discussed above, is a recent example).

Perhaps they should. Modified constitutional standing requirements—or at least a rethinking of what the harms from privacy intrusions entail—may be necessary to do justice to broader privacy interests, at the very least for the subset of privacy rights that are inextricably intertwined with freedom of thought, expression, and the proper functioning of the democratic process (what some have called the rights to intellectual privacy). In many other contexts, remedies crafted by lawmakers, rather than courts, are likely to be more appropriate.

Changing the discourse

To be sure, the doctrinal analogies discussed above quickly reach the limits of their usefulness. Changing a few laws is unlikely to get at the problem's root, which is the contrived and outdated vocabulary of privacy rights and the wooden policy and political discourse built around it. Our inability to conceptualize privacy as more than a purely individual right is damaging: it drives our broken notice-and-consent model of privacy protection, and it makes genuine debate (whether in the courts or otherwise) about the costs and benefits of surveillance difficult and unwieldy.

The longer we avoid grappling with the broader implications of privacy intrusions—the longer we frame the issue as a question of balancing the individual preferences of a few civil libertarians against the convenience and security of the many—the more likely it becomes that the big questions will be decided for us: by technology, by fear, and by the inertia of a new status quo, created without deliberation.

Privacy is the key check on government power—it's a precondition for democracy and dissent

McFARLAND 2012 (Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and a special interest in the intersection of technology and ethics, served as the 31st president of the College of the Holy Cross., "Why We Care about Privacy," June, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>)

Privacy is even more necessary as a safeguard of freedom in the relationships between individuals and groups. As Alan Westin has pointed out, surveillance and publicity are powerful instruments of social control.⁸ If individuals know that their actions and dispositions are constantly being observed, commented on and criticized, they find it much harder to do anything that deviates from accepted social behavior. There does not even have to be an explicit threat of retaliation. "Visibility itself provides a powerful method of enforcing norms."⁹ Most people are afraid to stand apart, to be different, if it means being subject to piercing scrutiny. The "deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."¹⁰ Under these circumstances they find it better simply to conform. This is the situation characterized in George Orwell's 1984 where the pervasive surveillance of "Big Brother" was enough to keep most citizens under rigid control. 11

Therefore privacy, as protection from excessive scrutiny, is necessary if individuals are to be free to be themselves. Everyone needs some room to break social norms, to engage in small "permissible deviations" that help define a person's individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves. As Brian Stelter wrote in the New York Times on the loss of anonymity in today's online world, "The collective intelligence of the Internet's two billion users, and the digital fingerprints that so many users leave on Web sites, combine to make it more and more likely that every embarrassing video, every intimate photo, and every indecent e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view." 12

This ability to develop one's unique individuality is especially important in a democracy, which values and depends on creativity, nonconformism and the free interchange of diverse ideas. That is where a democracy gets its vitality. Thus, as Westin has observed, "Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life." 13

When Brandeis and Warren wrote their seminal article on privacy over one hundred years ago, their primary concern was with the social pressure caused by excessive exposure to public scrutiny of the private affairs of individuals. The problem for them was the popular press, which represented the "monolithic, impersonal and value-free forces of modern society," 14 undermining the traditional values of rural society, which had been nurtured and protected by local institutions such as family, church and other associations. The exposure of the affairs of the well-bred to the curiosity of the masses, Brandeis and Warren feared, had a leveling effect which undermined what was noble and virtuous in society, replacing it with the base and the trivial.

Even apparently harmless gossip, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.... Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence. 15

For Brandeis and Warren, privacy was a means of protecting the freedom of the virtuous to maintain their values against the corrupting influence of the mass media that catered to people's basest instincts.

Although the degrading effect of the mass media is still a problem, today a more serious threat to freedom comes from governments and other large institutions. Over the last century, governments have developed sophisticated methods of surveillance as a means of controlling their subjects. This is especially true of totalitarian states, as the passage from Westin quoted above indicates. The Soviet Union, Communist China, Nazi Germany, Fascist Italy and white-run South Africa all used covert and overt observation, interrogation, eavesdropping, reporting by neighbors and other means of data collection to convince their subjects that independent, "antisocial" thought, speech and behavior was unacceptable. In many cases the mere presence of the surveillance was enough to keep people in line. Where it was not, the data collected was used to identify, round up and punish elements of the population that were deemed dangerous. For example, Ignazio Silone, in his book Bread and Wine, described the use of surveillance in Fascist Italy in this way:

It is well-known [says Minorca] that the police have their informers in every section of every big factory, in every bank, in every big office. In every block of flats the porter is, by law, a stool pigeon for the police.... This state of affairs spreads suspicion and distrust throughout all classes of the population. On this degradation of man into a frightened animal, who quivers with fear and hates his neighbor in his fear, and watches him, betrays him, sells him, and then lives in fear of discovery, the dictatorship is based. The real organization on which the system in this country is based is the secret manipulation of fear. 16

While totalitarian regimes may not seem as powerful or as sinister as they did 50 years ago, surveillance is still used in many places as an instrument of oppression. For example Philip Zimmerman, the author of the PGP (Pretty Good Privacy) data encryption program, reports receiving a letter from a human rights activist in the former Yugoslavia that contained the following testimonial:

We are part of a network of not-for-profit agencies, working among other things for human rights in the Balkans. Our various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and our office in Romania has a constant wiretap.

Last year in Zagreb, the security police raided our office and confiscated our computers in the hope of retrieving information about the identity of people who had complained about their activities.

Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients. 17

More recently social media and the Internet played major roles in the "Arab Spring" uprisings in the Middle East, causing Egypt and Libya to shut down the Internet in their countries in an attempt to stifle dissent. 18 In China there has been an ongoing battle between the government and activist groups over government monitoring and censorship of the Internet. 19

Even in a democracy, there is always the danger that surveillance can be used as a means of control. In the United States, for example, where freedom is such an important part of the national ethos, the FBI, the CIA, the National Security Agency (NSA) and the armed forces have frequently kept dossiers on dissidents. The NSA from 1952 to 1974 kept files on about 75,000 Americans, including civil rights and antiwar activists, and even members of Congress. During the Vietnam war, the CIA's Operation Chaos collected data on over 300,000 Americans. 20 Since then the NSA has had an ongoing program to monitor electronic communications, both in the U.S. and abroad, which has led to constant battles with individuals and groups who have sought to protect the privacy of those communications through encryption and other technologies. 21

Some of the most famous incidents of surveillance of dissidents, of course, occurred during the Nixon administration in the early 1970s. For example, when Daniel Ellsberg was suspected of leaking the Pentagon Papers, an internal critique of government conduct of the Vietnam war, Nixon's agents broke into the office of Ellsberg's psychiatrist and stole his records. 22 And it was a bungled attempt at surveillance of Nixon's political opposition, as well as illegal use of tax returns from the IRS, that ultimately brought down the Nixon administration. 23 More recently, during the 1996 presidential campaign, it was revealed that the Clinton White House had access to the FBI investigative records of over 300 Republicans who had served in the Reagan and Bush administrations. The Clinton administration claimed it was all a mistake caused by using an out-of-date list of White House staff, while the challenger Bob Dole accused them of compiling an "enemies list." >sup>24 Whatever the motivation, the head of the FBI termed the use of the files "egregious violations of privacy." 25

Since the 9/11 terrorist attacks in 2001, there has been even greater urgency in the government's efforts to monitor the activities and communications of people, both foreigners and its own citizens, in order to identify and prevent terrorist threats. The Patriot Act, passed less than two months after 9/11, greatly expanded the government's authority to intercept electronic communications, such as emails and phone calls, including those of U.S. citizens. As a result government agencies have been building the technological and organizational capabilities to monitor the activities and communications of their own citizens. For example, Wired magazine revealed in a recent report how the National Security Agency

has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created. In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it's all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever. 26

The FBI, the Drug Enforcement Agency and the Department of Homeland Security also have many programs to monitor citizens in general, not just those who are under suspicion. These efforts include sifting through media references, 27 tracking chatter on social networks, 28 and monitoring peoples' movements through license plate scanners 29 and video cameras. 30

The mere knowledge that American citizens could be the subjects of surveillance can in itself have a chilling effect on political freedom. "Now it is much more difficult than it once was to dismiss the possibility that one's phone is being tapped, or that one's tax returns may be used for unfriendly political purposes, or that one's life has become the subject of a CIA file. The realization that these activities might take place, whether they really do or not in any particular instance, has potentially destructive effects on the openness of social systems to innovation and dissent." 31

At times the government in the United States has gone beyond surveillance and intimidation and has used the data gathered as a basis for overt oppression. One of the most blatant examples is the internment of over 100,000 Japanese Americans, most of them American citizens, during World War II. The Justice Department used data from the Census Bureau to identify residential areas where there were large concentrations of Japanese Americans, and the army was sent in to round them up. They were taken away from their homes and held in concentration camps for the duration of the war. 32

Governments do need information, including personal information, to govern effectively and to protect the security of their citizens. But citizens also need protection from the overzealous or malicious use of that information, especially

by governments that, in this age, have enormous bureaucratic and technological power to gather and use the information.

The Right to Privacy is a fundamental tenet of a democratic society

UN News Centre 13 – United Nations News Centre (“General Assembly backs right to privacy in digital age,” December 19th, 2013,
<http://www.un.org/apps/news/story.asp?NewsID=46780#.Va1e7vlViko>)BC

19 December 2013 – Deeply concerned that electronic surveillance, interception of digital communications and collection of personal data may negatively impact human rights, the United Nations General Assembly has adopted a consensus resolution strongly backing the right to privacy, calling on all countries take measures to end activities that violate this fundamental “tenet of a democratic society.”

By a text entitled “Right to privacy in the digital age,” the Assembly weighed in on the emerging issue, underscoring that the right to privacy is a human right and affirming, for the first time, that the same rights people have offline must also be protected online. It called on States to “respect and protect the right to privacy, including in the context of digital communication.”

The measure, crafted by Brazil and Germany, was among the more than 65 texts recommended by the Assembly’s Third Committee (Social, Humanitarian and Cultural) yesterday on a range of issues relating mainly to human rights, social development and crime prevention.

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, the text states that governments must ensure full compliance with their obligations under international human rights law. It calls on States to establish or maintain independent, effective domestic oversight capable of ensuring transparency, as appropriate, and accountability for surveillance and/or interception of communications and the collection of personal data.

The resolution also requests the UN High Commissioner for Human Rights, Navi Pillay, to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and the collection of personal data, including on a mass scale, to the Geneva-based Human Rights Council at its 27th session and to the Assembly at its 69th session.

Earlier in the year, Ms. Pillay spotlighted the right to privacy, using the case of United States citizen Edward Snowden to illustrate the urgent need to protect individuals who reveal human rights violations.

“Snowden’s case has shown the need to protect persons disclosing information on matters that have implications for human rights, as well as the importance of ensuring respect for the right to privacy,” she said, adding that national legal systems must ensure avenues for individuals disclosing violations of human rights to express their concern without fear of reprisals.

“The right to privacy, the right to access to information and freedom of expression are closely linked. The public has the democratic right to take part in the public affairs and this right cannot be effectively exercised by solely relying on authorized information.”

Mr. Snowden is a former National Security Agency contractor in the US who has been charged with leaking details of several secret mass electronic surveillance programmes to the press. He fled the country this past spring after the news broke, and according to media reports, he is currently in Russia.

Ms. Pillay noted at the time that while concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programmes, “surveillance without adequate safeguards to protect the right to privacy actually risk impacting negatively on the enjoyment of human rights and fundamental freedoms.”

She also recalled that Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights state that no one shall be subjected to arbitrary interference with one's privacy, family, home or correspondence, and that everyone has the right to the protection of the law against such interference or attacks.

“People need to be confident that their private communications are not being unduly scrutinized by the State,” she said.

privacy is key to self-identity and value to life

Sadowski 13 [Jathan, "Why Does Privacy Matter? One Scholar's Answer", 2/26/13, The Atlantic, www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/] // SKY

Our privacy is now at risk in unprecedented ways, but, sadly, the legal system is lagging behind the pace of innovation. Indeed, the last major privacy law, the Electronic Communications Privacy Act, was passed in 1986! While an update to the law -- spurred on by the General Petraeus scandal -- is in the works, it only aims to add some more protection to electronic communication like emails. This still does not shield our privacy from other, possibly nefarious, ways that our data can be collected and put to use. Some legislators would much rather not have legal restrictions that could, as Rep. Marsha Blackburn stated in an op-ed, "threaten the lifeblood of the Internet: data." Consider Rep. Blackburn's remarks during an April 2010 Congressional hearing: "[A]nd what happens when you follow the European privacy model and take information out of the information economy? ... Revenues fall, innovation stalls and you lose out to innovators who choose to work elsewhere."

Even though the practices of many companies such as Facebook are legal, there is something disconcerting about them. Privacy should have a deeper purpose than the one ascribed to it by those who treat it as a currency to be traded for innovation, which in many circumstances seems to actually mean corporate interests. To protect our privacy, we need a better understanding of its purpose and why it is valuable.

That's where Georgetown University law professor Julie E. Cohen comes in. In a forthcoming article for the Harvard Law Review, she lays out a strong argument that addresses the titular concern "What Privacy Is For." Her approach is fresh, and as technology critic Evgeny Morozov rightly tweeted, she wrote "the best paper on privacy theory you'll get to read this year." (He was referring to 2012.)

At bottom, Cohen's argument criticizes the dominant position held by theorists and legislators who treat privacy as just an instrument used to advance some other principle or value, such as liberty, inaccessibility, or control. Framed this way, privacy is relegated to one of many defenses we have from things like another person's prying eyes, or Facebook's recent attempts to ramp up its use of facial-recognition software and collect further data about us without our explicit consent. As long as the principle in question can be protected through some other method, or if privacy gets in the way of a different desirable goal like innovation, it is no longer useful and can be disregarded.

Cohen doesn't think we should treat privacy as a dispensable instrument. To the contrary, she argues privacy is irreducible to a "fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic. Privacy is shorthand for breathing room to engage in the process of ... self-development."

What Cohen means is that since life and contexts are always changing, privacy cannot be reductively conceived as one specific type of thing. It is better understood as an important buffer that gives us space to develop an identity that is somewhat separate from the surveillance, judgment, and values of our society and culture. Privacy is crucial for helping us manage all of these pressures -- pressures that shape the type of person we are -- and for "creating spaces for play and the work of self-

[development]." Cohen argues that this self-development allows us to discover what type of society we want and what we should do to get there, both factors that are key to living a fulfilled life.

Woodrow Hartzog and Evan Selinger make similar arguments in a recent article on the value of "obscurity." When structural constraints prevent unwanted parties from getting to your data, obscurity protections are in play. These protections go beyond preventing companies from exploiting our information for their financial gain. They safeguard democratic societies by furthering "autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power."

In light of these considerations, what's really at stake in a feature like Facebook's rumored location-tracking app? You might think it is a good idea to willfully hand over your data in exchange for personalized coupons or promotions, or to broadcast your location to friends. But consumption -- perusing a store and buying stuff -- and quiet, alone time are both important parts of how we define ourselves. If how we do that becomes subject to ever-present monitoring it can, if even unconsciously, change our behaviors and self-perception.

In this sense, we will be developing an identity that is absent of privacy and subject to surveillance; we must decide if we really want to live in a society that treats every action as a data point to be analyzed and traded like currency. The more we allow for constant tracking, the more difficult it becomes to change the way that technologies are used to encroach on our lives.

Privacy is not just something we enjoy. It is something that is necessary for us to: develop who we are; form an identity that is not dictated by the social conditions that directly or indirectly influence our thinking, decisions, and behaviors; and decide what type of society we want to live in. Whether we like it or not constant data collection about everything we do -- like the kind conducted by Facebook and an increasing number of other companies -- shapes and produces our actions. We are different people when under surveillance than we are when enjoying some privacy. And Cohen's argument illuminates how the breathing room provided by privacy is essential to being a complete, fulfilled person.

Privacy abuse violates liberty and deprives us of our personal agency – the longer we go without resisting pushes us towards tyranny

Schneier 6 – the CTO of Counterpane Internet Security and the author of Beyond Fear: Thinking Sensibly About Security in an Uncertain World (5/18/2006, Bruce, Wired, "The Eternal Value of Privacy", http://archive.ps-xaf.de/2009/ps-xaf.de/docs/The_Eternal_Value_of_Privacy.pdf // SM)

The most common retort against privacy advocates -- by those in favor of ID checks, cameras, databases, data mining and other wholesale surveillance measures -- is this line: "If you aren't doing anything wrong, what do you have to hide?" Some clever answers: "If I'm not doing anything wrong, then you have no cause to watch me." "Because the government gets to define what's wrong, and they keep changing the definition." "Because you might do something wrong with my information." My problem with quips like these -- as right as they are -- is that they accept the premise that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect. Two proverbs say it best: Quis custodiet custodes ipsos? ("Who watches the watchers?") and "Absolute power corrupts absolutely." Cardinal Richelieu understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged." Watch someone long enough, and you'll find something to arrest -- or just blackmail -- with. Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political

enemies -- whoever they happen to be at the time. Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance. We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need. A future in which privacy would face constant assault was so alien to the framers of the Constitution that it never occurred to them to call out privacy as an explicit right. Privacy was inherent to the nobility of their being and their cause. Of course being watched in your own home was unreasonable. Watching at all was an act so unseemly as to be inconceivable among gentlemen in their day. You watched convicted criminals, not free citizens. You ruled your own home. It's intrinsic to the concept of liberty. For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that -- either now or in the uncertain future -- patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable. How many of us have paused during conversation in the past four-and-a-half years, suddenly aware that we might be eavesdropped on? Probably it was a phone conversation, although maybe it was an e-mail or instant message exchange or a conversation in a public place. Maybe the topic was terrorism, or politics, or Islam. We stop suddenly, momentarily afraid that our words might be taken out of context, then we laugh at our paranoia and go on. But our demeanor has changed, and our words are subtly altered. This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives. Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide.

Moral Imperative

Reject those privacy violations as an *a priori imperative*. Also proves that the disad's all hype.

Wyden '14

(et al; This amicus brief issued by three US Senators - Ron Wyden, Mark Udall and Martin Heinrich. Wyden and Udall sat on the Senate Select Committee on Intelligence and had access to the meta-data program. "BRIEF FOR AMICI CURIAE SENATOR RON WYDEN, SENATOR MARK UDALL, AND SENATOR MARTIN HEINRICH IN SUPPORT OF PLAINTIFF-APPELLANT, URGING REVERSAL OF THE DISTRICT COURT" – Amicus Brief for *Smith v. Obama* – before the United States Ninth Circuit Court of Appeals - Appeal from the United States District Court District of Idaho The Honorable B. Lynn Winmill, Chief District Judge, Presiding Case No. 2:13-cv-00257-BLW – Sept 9th, 2014 – This Amicus Brief was prepared by CHARLES S. SIMS from the law firm PROSKAUER ROSE LLP. This pdf can be obtained at: <https://www.eff.org/document/wyden-udall-heinrich-smith-amicus>)

Respect for Americans' privacy is not a matter of convenience, but a Constitutional imperative. Despite years of receiving classified briefings and asking repeated questions of intelligence officials in both private and public settings, amici have seen no evidence that bulk collection accomplishes anything that other less intrusive surveillance authorities could not. Bulk collection is not only a significant threat to the constitutional liberties of Americans, but a needless one.⁹

Surveillance Kills Privacy

Surveillance undermines reasonable expectations of privacy and threatens democracy

Citron & Macht, 2013, Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law; Affiliate Scholar, Stanford Center on Internet and Society; Affiliate Fellow, Yale Information Society Project., David Gray, Associate Professor of Law, University of Maryland School of Law. We are grateful to Neil Richards for his thoughtful essay and feedback and to Julie Cohen, Leslie Henry, Amanda Pustilnik, Daniel Solove, and the participants in the Harvard Law Review Symposium on Privacy and Technology for their helpful suggestions, “ADDRESSING THE HARM OF TOTAL SURVEILLANCE: A REPLY TO PROFESSOR NEIL RICHARDS,” May, p. 270

The **continuous and indiscriminate surveillance they accomplish is damaging because it violates reasonable expectations of quantitative privacy, by which we mean privacy interests in large aggregations of information** that are independent from particular interests in constituent parts of that whole. To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that **the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.** In adopting this view, we ally ourselves in part with commitments to a quantitative account of Fourth Amendment privacy promoted by at least five Justices of the Supreme Court last Term in *United States v. Jones*. In *Jones*, police officers investigating drug trafficking in and around the District of Columbia attached a GPS-enabled tracking device on defendant *Jones's* car. By monitoring his movements over the course of a month, investigators were able to document both the patterns and the particulars of his travel, which played a critical role in his ultimate conviction. Although the Court resolved *Jones* on the narrow grounds of physical trespass, five justices wrote or joined concurring opinions showing sympathy for the proposition that citizens hold reasonable expectations of privacy in large quantities of data, even if they lack reasonable expectations of privacy in the constitutive parts of that whole. Thus, they would have held that *Jones* had a reasonable expectation in the aggregate of data documenting his public movements over the course of four weeks, even though he did not have any expectation of privacy in his public movements on any particular afternoon. The account of quantitative privacy advanced by the *Jones* concurrences has much in common with the views promoted by Warren and Brandeis. Specifically, the concurring Justices in *Jones* expressed worry that by "making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," programs of broad and indiscriminate surveillance will "chill[] associational and expressive freedoms," and "alter the relationship between citizen and government in a way that is inimical to a democratic society." Their concerns are well-grounded in original understandings of the Fourth Amendment. As Professor William Stuntz has shown, the Fourth Amendment was drafted partly in reaction to eighteenth-century cases involving the British government's use of general warrants to seize personal diaries and letters in support of seditious-libel prosecutions that were designed to suppress political thought. Despite these roots, quantitative privacy is just beginning to receive recognition because it is only now under threat of extinction by technologies like Virtual Alabama and fusion centers.

Surveillance threatens our quantitative privacy

Citron & Gray, 2013 Danielle Keats Citron, and David Gray, Lois K. Macht Research Professor of Law, University of Maryland School of Law; Affiliate Scholar, Stanford Center on Internet and Society; Affiliate Fellow, Yale Information Society Project, Associate Professor of Law, University of Maryland School of Law. We are grateful to Neil Richards for his thoughtful essay and feedback and to Julie Cohen, Leslie Henry, Amanda Pustilnik, Daniel Solove, and the participants in the Harvard Law Review Symposium on Privacy and Technology for their helpful suggestions, Harvard Law Review Forum, Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards, <http://harvardlawreview.org/2013/06/addressing-the-harm-of-total-surveillance-a-reply-to-professor-neil-richards/>, DOA: 4-9-15,

The continuous and indiscriminate surveillance they accomplish is damaging because it violates reasonable expectations of *quantitative* privacy, by which we mean privacy interests in large aggregations of information that are independent from particular interests in constituent parts of that whole. To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.

In adopting this view, we ally ourselves in part with commitments to a quantitative account of Fourth Amendment privacy promoted by at least five Justices of the Supreme Court last Term in *United States v. Jones*. In *Jones*, police officers investigating drug trafficking in and around the District of Columbia attached a GPS-enabled tracking device on defendant Jones's car. By monitoring his movements over the course of a month, investigators were able to document both the patterns and the particulars of his travel, which played a critical role in his ultimate conviction. Although the Court resolved *Jones* on the narrow grounds of physical trespass, five justices wrote or joined concurring opinions showing sympathy for the proposition that citizens hold reasonable expectations of privacy in large quantities of data, even if they lack reasonable expectations of privacy in the constitutive parts of that whole. Thus, they would have held that Jones had a reasonable expectation in the aggregate of data documenting his public movements over the course of four weeks, even though he did not have any expectation of privacy in his public movements on any particular afternoon.

Surveillance crushes privacy and commerce

Alexis Ohanlan, Co-Founder, reddit.com, May 2, 2014, "Munk Debate: Is State Surveillance a Legitimate Defense of Our Freedoms?" The Globe and Mail, <http://www.theglobeandmail.com/globe-debate/is-state-surveillance-a-legitimate-defence-of-our-freedoms/article18368244/>

Alexis Ohanian : We Americans and Canadians have many shared values - though we may never settle who's really to blame for Justin Bieber - an inalienable right to privacy is something secured in our Bill of Rights and Canadian Charter of Rights and Freedoms, respectively. Our democratic societies balance this right to privacy with security, but the technological leap we've made in the last decade that has made possible my career as a tech entrepreneur and investor has also enabled a surveillance state that is simply unacceptable. The NSA has immense capabilities now and the only thing controlling it is secret law. There's precedent of far less efficient surveillance technology being abused - even Dr. Martin Luther King and many more U.S. citizens involved in the civil rights and anti-war movements were

surveilled. Democracy needs sunlight to thrive. Our reputation has attracted the world's best and brightest, as well as their money, for our highly-regarded global tech industry, but now Forrester estimates U.S. companies alone stand to lose \$180-billion to non-U.S. cloud providers. **The NSA's insatiable appetite for data and mass surveillance has polluted the network. We're all connected online but now the very infrastructure of the Internet is no longer healthy because of our brazenness.** From a technological standpoint, the World Wide Web works best when it's "world wide," and yet **we're faced with countries like Brazil and Germany now discussing balkanizing the Internet to guard against intrusion.** Steve Huffman and I can't possibly start reddit (a site that now is one of the most popular in the world with 150 million visitors a month, 42 per cent of whom are non-US) and expect it to become a truly global platform without every potential customer having both access and trust in our servers. We're not just talking about law, **we're talking about keeping technology insecure so that governments can do mass surveillance. That has a huge impact on user trust,** policy debates about privacy, data protection, data localization, and gives comfort to oppressive governments that want to surveil the Internet. This is important, because **what we're doing in the name of counterterrorism is actually undermining security elsewhere - finding security flaws and leaving them for anyone to exploit later is not sound policy.** A rising tide really does lift all boats - or in this case, lock all doors - when it comes to online security. Speaking of which, that word, security, means different things to my opponents. I'm not talking about trading security for privacy, I'm talking about trading one kind of security for another kind of security. First, these tools aren't just being used for counter-terrorism. Second, the things done in the name of counter-terrorism are hurting other kinds of security.

Much of the spying is not related to terrorism and makes possible the total elimination of global privacy

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Some of the surveillance was ostensibly devoted to terrorism suspects. But great quantities of the programs manifestly had nothing to do with national security. The documents left no doubt that **the NSA was equally involved in economic espionage, diplomatic spying, and suspicionless surveillance aimed at entire populations.** Taken in its entirety, the Snowden archive led to an ultimately simple conclusion: **the US government had built a system that has as its goal the complete elimination of electronic privacy worldwide.** Far from hyperbole, **that is the literal, explicitly stated aim of the surveillance state: to collect, store, monitor, and analyze all electronic communication by all people around the globe.** **The agency is devoted to one overarching mission: to prevent the slightest piece of electronic communication from evading its systemic grasp. This self-imposed mandate requires endlessly expanding the NSA's reach.** Every day, the NSA works to identify electronic communications that are not being collected and stored and then develops new technologies and methods to rectify the deficiency. The agency regards itself as needing no specific justification to collect any particular electronic communication, nor any grounds for regarding its targets with suspicion. What the NSA calls "SIGINT"—all signals intelligence—is its target. And the mere fact that it has the capability to collect those communications has become one rationale for doing so. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 1635-1642). Henry Holt and Co.. Kindle Edition.

Surveillance network will eliminate global privacy

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Throughout the five hours of questioning that day—indeed, for the entire time I spoke with him in Hong Kong—**Snowden's tone was almost always stoic, calm, matter-of-fact.** But as he explained what he had

discovered that finally the NSA, and the U.S. Surveillance State moved him to action, he became impassioned, even slightly agitated. "I realized," he said, "that they were building a system whose goal was the elimination of all privacy, globally. To make it so that no one could communicate electronically without the NSA being able to collect, store, and analyze the communication." Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 832-835). Henry Holt and Co.. Kindle Edition.

Mass surveillance of individual movement threatens privacy

Stephen Rushin, Fall 2013, Visiting Assistant Professor, University of Illinois College of Law, Brooklyn Law Review, ARTICLE: The Legislative Response to Mass Police Surveillance, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805 DOA: 1-25-15, p. 13

Eighth, indiscriminate data collection allows law enforcement to aggregate large amounts of information about a single individual, thereby revealing personal information about habits and behaviors. Five of the justices in *Jones* noted in two separate concurrences that the accumulation of large amounts of data on public movements transforms normal surveillance into a potentially unconstitutional invasion of individual privacy. These extensive records on individual movements might reveal private interests, patterns of behavior, or habits. For example, aggregation of surveillance data of an individual might enable "the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." Police and the state can use this type of revealing personal information to target unpopular minorities or conduct fishing expeditions.

Surveillance inconsistent with privacy and democratic values

Joel R. Reidenberg, Summer 2014, Microsoft Visiting Professor of Information Technology Policy, Princeton University; Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law, Wake Forest Law Review, THE DATA SURVEILLANCE STATE IN THE UNITED STATES AND EUROPE, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269, DOA: 1-25-15, p. 584-5

But, as illustrated by the U.S. government's massive collection of telecommunications data; by the UK tapping of transatlantic telecommunications cables; by the Swedish government's warrantless wiretap authority; and by the wiretapping of journalists in France, democratic societies have created a technological infrastructure of surveillance with a legal infrastructure of surveillance authorizations. In effect, the legal framework that each system has established will not be able to preserve, over the long term, citizen privacy and basic democratic values.

The Constitutional Right to Privacy

The constitutional right to privacy

Jonathan Olivito, law student, 2013, Ohio State Law Journal, v. 74, Note: Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy,
<http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/8-Olivito.pdf>, DOA: 1-20-15, p. 689-93

IV. The Assumed Constitutional Right to Informational Privacy

To date, the Supreme Court has not definitively recognized the existence of a constitutional right to informational privacy. Yet, in two cases decided in 1977 the Court assumed the existence of a constitutional right to privacy and applied a balancing test to determine whether the assumed right had been violated. As recently as 2011 the Court adjudicated a claim involving an asserted violation of the assumed constitutional right to privacy.

A. Contours of the Constitutional Right to Privacy

In *Whalen v. Roe*, the Supreme Court first articulated that the Constitution protects privacy outside of the Fourth Amendment context. In *Nixon v. Administrator of General Services*, the Supreme Court reaffirmed this assumption in the context of informational privacy. The Court assumed that privacy consists of two branches: informational privacy; and privacy through autonomy. The right to informational privacy is the right to avoid disclosure of certain personal matters. The right to privacy through autonomy is the right to make certain important life decisions independent of interference. In both *Whalen* and *Nixon*, however, the Court found that the disputed government actions-recording the issuance of prescription drugs and sorting through presidential documents and recordings, respectively-did not amount to violations of this constitutional right. Because the Court did not find a violation of the right to privacy in either instance, the Court found it unnecessary to declare the existence of the constitutional right to privacy or to clearly delineate its boundaries.

In 2011, the Supreme Court once again assumed the existence of the constitutional right to privacy. *NASA v. Nelson*, the Court focused its analysis on the dangers represented by the government's collection and possible dissemination of personal information. Ultimately, the Court found that requiring individuals to provide information on drug use and treatment did not violate a constitutional right to privacy.

The constitutional right to privacy, as construed in *NASA*, does not require a government action to be necessary or the least restrictive means of furthering the governmental interest. Rather, the Court applied a balancing test to determine the constitutionality of *NASA*'s action. In comparing the governmental interests at stake to the privacy violation at issue, the Court considered the degree of use, duration, and value of *NASA*'s practice. The Court also suggested that a constitutional protection of privacy may not be necessary in situations where statutory or regulatory measures allay the privacy concerns.

State courts and lower federal courts have addressed claims alleging a violation of the constitutional right to privacy in three main ways: by applying a balancing test (the intermediate scrutiny approach); by only permitting claims when the interests at stake are fundamental to the concept of liberty; and through non-recognition.

1. The Intermediate Scrutiny Approach

Under the intermediate scrutiny approach, courts attempt to balance the government's interests against the individual's privacy interest. The Second, Third, Fifth, and Ninth Circuits, as well as the Supreme Court of Connecticut, have all adhered to the intermediate scrutiny approach in applying the constitutional right to privacy to claims involving governmental collection or distribution of certain types of personal information.

Courts have typically treated the balancing of individual privacy interests against governmental interests as a question of law to be determined by the court. When courts undertake this balancing test, they consider a multitude of factors, including the contents of the disputed information, the harm that could be caused by disclosure of the information, and the safeguards established to prevent unauthorized disclosure of the information. Ultimately, however, the factors relevant to the balancing test vary from case to case based on the privacy interest purportedly violated.

2. The "Fundamental or Implicit in the Concept of Ordered Liberty" Approach

The Sixth Circuit has taken a slightly different approach to the constitutional right to privacy. The Sixth Circuit finds unconstitutional intrusions to the informational privacy right only when the rights at stake are "'fundamental' or 'implicit in the concept of ordered liberty.'" Through a citation to *Roe v. Wade*, the Sixth Circuit has implied that rights are "fundamental or implicit in the concept of ordered liberty" only if they relate to marriage, procreation, contraception, family relationships, and child rearing and education. A number of commentators have criticized the Sixth Circuit's approach as misinterpreting Supreme Court precedent and inappropriately constraining the application of the constitutional right to privacy.

3. Non-recognition of the Constitutional Right to Privacy

Given that the Supreme Court has never actually stated that the constitutional right to privacy exists, but rather has assumed that it exists for the purpose of disposing of cases, some courts have all but repudiated the right. The D.C. Circuit, for example, has stated that it has "grave doubts as to the existence of a constitutional right to privacy in the nondisclosure of personal information." Yet, even after asserting its doubts as to the existence of a constitutional right to privacy, the D.C. Circuit has assumed for the purpose of adjudicating constitutional privacy claims that the right exists. In applying the assumed right, the D.C. Circuit utilized a balancing test.

In sum, the majority of circuits have recognized the existence of a constitutional right to privacy. Courts recognizing the right have typically utilized a balancing test to determine whether a government action constitutes a violation of the constitutional right to privacy.

History of privacy in the Supreme Court

UMKC Law School, no date, The Right of Privacy,
<http://law2.umkc.edu/faculty/projects/trials/conlaw/rightofprivacy.html> DOA: 2-23-15

he Supreme Court, in two decisions in the 1920s, read the Fourteenth Amendment's liberty clause to prohibit states from interfering with the private decisions of educators and parents to shape the education of children. In *Meyer v Nebraska* (1923), the Supreme Court struck down a state law that prohibited the teaching of German and other foreign languages to children until the ninth grade. The state argued that foreign languages could lead to inculcating in students "ideas and sentiments foreign to the best interests of this country." The Court, however, in a 7 to 2 decision written by Justice McReynolds concluded that the state failed to show a compelling need to infringe upon the rights of parents and teachers to decide what course of education is best for young students. Justice McReynolds wrote:

"While this court has not attempted to define with exactness the liberty thus guaranteed, the term has received much consideration and some of the included things have been definitely stated. Without doubt, it denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men."

Two years later, in *Pierce v Society of Sisters*, the Court applied the principles of *Meyer* to strike down an Oregon law that compelled all children to attend public schools, a law that would have effectively closed all parochial schools in the state.

The privacy doctrine of the 1920s gained renewed life in the Warren Court of the 1960s when, in *Griswold v Connecticut* (1965), the Court struck down a state law prohibiting the possession, sale, and distribution of contraceptives to married couples. Different justifications were offered for the conclusion, ranging from Court's opinion by Justice Douglas that saw the "penumbras" and "emanations" of various Bill of Rights guarantees as creating "a zone of privacy," to Justice Goldberg's partial reliance on the Ninth Amendment's reference to "other rights retained by the people," to Justice Harlan's decision arguing that the Fourteenth Amendment's liberty clause forbade the state from engaging in conduct (such as search of marital bedrooms for evidence of illicit contraceptives) that was inconsistent with a government based "on the concept of ordered liberty."

In 1969, the Court unanimously concluded that the right of privacy protected an individual's right to possess and view pornography (including pornography that might be the basis for a criminal prosecution against its manufacturer or distributor) in his own home. Drawing support for the Court's decision from both the First and Fourth Amendments, Justice Marshall wrote in *Stanley v Georgia*:

"Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving

government the power to control men's minds."

The Burger Court extended the right of privacy to include a woman's right to have an abortion in *Roe v Wade* (1972), but thereafter resisted several invitations to expand the right. *Kelley v Johnson* (1976), in which the Court upheld a grooming regulation for police officers, illustrates the trend toward limiting the scope of the "zone of privacy." (The Court left open, however, the question of whether government could apply a grooming law to members of the general public, who it assumed would have some sort of liberty interest in matters of personal appearance.) Some state courts, however, were not so reluctant about pushing the zone of privacy to new frontiers. The Alaska Supreme Court went as far in the direction of protecting privacy rights as any state. In *Ravin v State* (1975), drawing on cases such as *Stanley* and *Griswold* but also basing its decision on the more generous protection of the Alaska Constitution's privacy protections, the Alaska Supreme Court found constitutional protection for the right of a citizen to possess and use small quantities of marijuana in his own home.

The Supreme Court said in the 1977 case of *Moore v. East Cleveland* that "the Constitution protects the sanctity of the family precisely because the institution of the family is deeply rooted in the Nation's history and tradition." Moore found privacy protection for an extended family's choice of living arrangements, striking down a housing ordinance that prohibited a grandmother from living together with her two grandsons. Writing for the Court, Justice Powell said, "The choice of relatives in this degree of kinship to live together may not lightly be denied by the state."

In more recent decades, the Court recognized in *Cruzan v Missouri Department of Health* (1990) that individuals have a liberty interest that includes the right to make decisions to terminate life-prolonging medical treatments (although the Court accepted that states can impose certain conditions on the exercise of that right). In 2003, in *Lawrence v Texas*, the Supreme Court, overruling an earlier decision, found that Texas violated the liberty clause of two gay men when it enforced against them a state law prohibiting homosexual sodomy. Writing for the Court in *Lawrence*, Justice Kennedy reaffirmed in broad terms the Constitution's protection for privacy:

"These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life....The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. 'It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter.'"

Privacy Key to Democracy

Easy access to citizen data reverses the presumption of innocence, undermining democracy

Joel R. Reidenberg, Summer 2014, Microsoft Visiting Professor of Information Technology Policy, Princeton University; Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law, Wake Forest Law Review, THE DATA SURVEILLANCE STATE IN THE UNITED STATES AND EUROPE,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269, DOA: 1-25-15, p. 605-6

III. The Privacy Turning Point

The existence of retained traffic data, the reliance on uncertain access rules, the recourse to an elusive proportionality, the dependence on private actors, and the privileges accorded to national security collectively place privacy and values in democracy at a turning point. In the aggregate, these elements increase the transparency of citizens' online lives and reduce the sphere of privacy that citizens can enjoy. This transparency is destructive of many fundamental democratic values. First, the transparency reverses the presumption of innocence. The presumption is central to the philosophy underlying the warrant requirement in the Fourth Amendment and the principle that citizens are innocent until proven guilty in the Fifth and Fourteenth Amendments. In Europe, the presumption of innocence is also a fundamental tenet of the Charter of Fundamental Rights of the European Union: "Everyone who has been charged shall be presumed innocent until proved guilty according to law." Yet, data that are collected and retained without any individualized cause or suspicion by private actors for subsequent access by public authorities contravenes the basic constitutional philosophies. If law generally requires collection and retention, the rationale is that all individuals in the data set are suspect. Similarly, if broad access is afforded to data sets that were created for commercial purposes, the core philosophy is that all individuals in the data set are suspect. These practices transform the presumption of innocence into a presumption of suspicion counter to the core constitutional philosophies Second, the forced transparency diffuses the monopoly of the state on law enforcement. Law enforcement, investigation, and intelligence activities are blurred when communications service providers must retain and make available client and user data. Function creep assures that this diffusion of resources for law enforcement to the private sector will lead to increasing demands and an expansion of the scope of enforcement activity to encompass private matters and not just public safety and security. Third, the transparency from private data mining and publicly mandated surveillance (i.e., forced data retention) diminishes the zone of individual freedom. Where data retention is neither sharply limited nor combined with strong, clear access controls, the ability of citizens to make decisions about their personal information and their ability to decide when and how to disclose their thoughts, beliefs, and activities, are impaired. Finally, the transparency of personal information through the national security exceptions assures troubling intelligence gathering from inevitable overreaching. Without a means for effective oversight, the privileges afforded to intelligence operations blur government information gathering into

generic, ambient state surveillance. Nondemocratic regimes strive for this level of knowledge of their citizenry's activities.

Crushing privacy is essential to the operation of all oppressive authorities

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

All oppressive authorities—political, religious, societal, parental—**rely on this vital truth, using it as a principal tool to enforce orthodoxies, compel adherence, and quash dissent.** **It is in their interest to convey that nothing their subjects do will escape the knowledge of the authorities. Far more effectively than a police force, the deprivation of privacy will crush any temptation to deviate from rules and norms.** Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2362-2365). Henry Holt and Co.. Kindle Edition.

Privacy is a fundamental pillar of democracy

Joel R. Reidenberg, Summer 2014, Microsoft Visiting Professor of Information Technology Policy, Princeton University; Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law, Wake Forest Law Review, THE DATA SURVEILLANCE STATE IN THE UNITED STATES AND EUROPE,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269, DOA: 1-25-15, p. 583

Europe and the United States recognize privacy as a fundamental pillar of democracy. The U.S. Constitution enshrines protection against state intrusions, and the Charter of Fundamental Rights of the European Union ("Charter") as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") each mandate that law and public authorities not interfere with "private life."

The country is founded on the protection of privacy

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Still, in many respects the issues raised by the NSA story resonate with numerous episodes from the past, stretching back across the centuries. Indeed, **opposition to government invasion of privacy was a major factor in the establishment of the United States itself, as American colonists protested laws that let British officials ransack at will any home they wished. It was legitimate, the colonists agreed, for the state to obtain specific, targeted warrants to search individuals when there was evidence to establish probable cause of their wrongdoing. But general warrants—the practice of making the entire citizenry subject to indiscriminate searches—were inherently illegitimate.** Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 48-52). Henry Holt and Co.. Kindle Edition.

Privacy Key to Freedom

Privacy essential to freedom

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

“Personal privacy,” the Committee added, is “essential to liberty and the pursuit of happiness” and is necessary to ensure “that all our citizens may live in a free and decent society.” Indeed, “when Government infringes the right of privacy, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated.” The Committee added that, in the words of former Attorney General and Supreme Court Justice Robert H. Jackson, without clear legal limitations, “a federal investigative agency would ‘have enough on enough people’ so that ‘even if it does not elect to prosecute them’ the Government would . . . still ‘find no opposition to its policies.’” Indeed, Jackson added, “even those who are supposed to supervise [our intelligence agencies] are likely to fear [them].””

Right to privacy a defining part of liberty

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

The right to privacy is essential to a free and self-governing society. The rise of modern technologies makes it all the more important that democratic nations respect people’s fundamental right to privacy, which is a defining part of individual security and personal liberty.

Privacy is a central aspect of liberty

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

It is self-evident that as more information is acquired, the risk to privacy increases as well. One reason is that officials might obtain personal or private information that has nothing to do with threats of violence or indeed with criminality at all. History shows that the acquisition of information can create risks of misuse and abuse, perhaps in the form of intrusion into a legitimately private sphere. History also shows that when government is engaged in surveillance, it can undermine public trust, and in that sense render its own citizens insecure. Privacy is a central aspect of liberty, and it must be safeguarded.

Privacy Critical to Self-Actualization

Privacy protects what it means to be human

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

The point is not the hypocrisy of those who disparage the value of privacy while intensely safeguarding their own, although that is striking. It is that the desire for privacy is shared by us all as an essential, not ancillary, part of what it means to be human. We all instinctively understand that the private realm is where we can act, think, speak, write, experiment, and choose how to be, away from the judgmental eyes of others. Privacy is a core condition of being a free person. Perhaps the most famous formulation of what privacy means and why it is so universally and supremely desired was offered by US Supreme Court Justice Louis Brandeis in the 1928 case Olmstead v. U.S.: "The right to be left alone [is] the most comprehensive of rights, and the right most valued by a free people." The value of privacy, he wrote, "is much broader in scope" than mere civic freedoms. It is, he said, fundamental: The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone. Even before Brandeis was appointed to the Court, he was an ardent proponent of the importance of privacy. Together with lawyer Samuel Warren, he wrote the seminal 1890 Harvard Law Review article "The Right to Privacy," arguing that robbing someone of their privacy was a crime of a deeply different nature than the theft of a material belonging. "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality." Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2346-2350). Henry Holt and Co.. Kindle Edition.

Privacy critical to dissent, creativity, and personal exploration

Kathleen Miles, June 2014, The Huffington Post, Glenn Greenwald On Why Privacy Is Vital, Even If You 'Have Nothing To Hide', http://www.huffingtonpost.com/2014/06/20/glenn-greenwald-privacy_n_5509704.html DOA: 2-253-14

'We all need places where we can go to explore without the judgmental eyes of other people being cast upon us,' he said. "Only in a realm where we're not being watched can we really test the limits of who we want to be. It's really in the private realm where dissent, creativity

and personal exploration lie.' He said that people who downplay the importance of privacy typically say, "I have nothing to hide." But, he added, those people aren't willing to publish their social media and email passwords. Greenwald published a series of stories last year based on leaked documents on United States surveillance from former National Security Agency contractor Edward Snowden. He recently published the book No Place to Hide about the fallout from Snowden's actions. 'When we think we're being watched, we make behavior choices that we believe other people want us to make,' he said. "It's a natural human desire to avoid societal condemnation. That's why every state loves surveillance -- it breeds a conformist population.' Greenwald went on to lambaste journalists, politicians and business leaders who have said that digital privacy is unnecessary. He criticized Google chairman Eric Schmidt for saying on CNBC[1] in 2008 that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Greenwald argued that it's detrimental to assume that someone who wants privacy -- say a person calling an HIV clinic or suicide hotline -- should be treated with suspicion. There are all kinds of things we want to hide from other people -- that we tell our psychiatrist, our lawyer, our doctor, our spouse or a stranger on the Internet -- that have nothing to do with criminality,' he said.

Privacy is essential to human freedom and happiness

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Privacy is essential to human freedom and happiness for reasons that are rarely discussed but instinctively understood by most people, as evidenced by the lengths to which they go to protect their own. To begin with, people radically change their behavior when they know they are being watched . They will strive to do that which is expected of them. They want to avoid shame and condemnation. They do so by adhering tightly to accepted social practices, by staying within imposed boundaries, avoiding action that might be seen as deviant or abnormal. The range of choices people consider when they believe that others are watching is therefore far more limited than what they might do when acting in a private realm. A denial of privacy operates to severely restrict one's freedom of choice.

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2355-2356). Henry Holt and Co.. Kindle Edition.

When people are alone they feel comfortable being and expressing themselves

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

What is lost when the private realm is abolished are many of the attributes typically associated with quality of life. Most people have experienced how privacy enables liberation from constraint. And we've all, conversely, had the experience of engaging in private behavior when we thought we were alone—dancing, confessing, exploring sexual expression, sharing untested ideas—only to feel shame at having been seen by others. Only when we believe that nobody else is watching us do we feel free—safe—to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it

means to be ourselves. What made the Internet so appealing was precisely that it afforded the ability to speak and act anonymously, which is so vital to individual exploration. For that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate. A society in which everyone knows they can be watched by the state— where the private realm is effectively eliminated — is one in which those attributes are lost, at both the societal and the individual level. Mass surveillance by the state is therefore inherently repressive, even in the unlikely case that it is not abused by vindictive officials to do things like gain private information about political opponents. Regardless of how surveillance is used or abused, the limits it imposes on freedom are intrinsic to its existence Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2374-2375). Henry Holt and Co.. Kindle Edition.

Privacy fosters moral autonomy essential for democracy

Ruth Gavison, Professor of Law, Hebrew University, PHILOSOPHICAL DIMENSIONS OF PRIVACY, Ferdinand Schoeman, ed., 1984, p.369-70.

Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy. Part of the justification for majority rule and the right to vote is the assumption that individuals should participate in political decisions by forming judgments and expressing preferences. Thus, to the extent that privacy is important for autonomy, it is important for democracy as well.

Privacy is grounded in basic rights of personhood

Charles Fried, former Professor of Law, Harvard, PHILOSOPHICAL DIMENSIONS OF PRIVACY, Ferdinand Schoeman, ed., 1984, p.206.

The view of morality upon which my conception of privacy rests is one which recognizes basic rights in persons, rights to which are all entitled equally, by virtue of their status as persons. These rights are subject to qualification only in order to ensure equal protection of the same rights in others. In this sense, the view is Kantian; it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximizing the happiness or welfare of all. It has received contemporary exposition in the work of John Rawls, who—summing up the fundamental interests of persons in the term “liberty”—has formulated the maxim that social institutions must be framed so as to entitle each person to the maximum liberty compatible with a like liberty for all.

In our society, privacy is key to love, friendship and trust

Jeffrey Johnson, Eastern Oregon State College, PUBLIC AFFAIRS QUARTERLY, July 1992, p.280.

Imagining, or even discovering, some eccentric society where love and friendship existed in the absence of privacy would not count as a counter example. The thesis is that in our culture love, friendship, and trust stand in some law-like relationship to privacy. “Privacy creates the moral capital which we spend in friendship and love.” It is irrelevant whether the connection between privacy and love and friendship is conceptual, semantic, or empirical.

Privacy is essential to resist government regulation of sexuality and biopower

Eskridge (Professor of Law, Georgetown University) 1996 (William N., Jr. *Florida State University Law Review* April 1)(<http://www.law.fsu.edu/journals/lawreview/downloads/244/eskridge.pdf>)

Privacy rights only become important once the Lockean state has evolved into the bureaucratic regulatory state. Same-sex intimacy was practically unregulated in the nineteenth century, and little regulated outside of New York City before World War I. Twentieth century America grew increasingly interested in gender and sexual deviance, and by the 1950s had created a pervasive regulatory regime for it. The objects of that regime—lesbians, homosexual men, butch women, female impersonators, pedophiles, and sex perverts of all stripes—resisted it in the legal argot of their time, the emerging principle or policy of privacy, which boils down to a list of things the state cannot do to one. My account of gay-friendly privacy discourse reveals the familiar problem with privacy as a Millian concept, namely, the lack of criteria by which to distinguish the “private” from the “public,” or acts that only affect the actor from those with third-party effects. Although Justice Louis Brandeis was the first legal thinker to identify the right of privacy as a needed limit on the overzealous state and to explore its constitutional dimensions,

Privacy Key to Personal Security

Privacy protects the security of persons

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

At the same time, **the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .”** (emphasis added). **This form of security is a central component of the right of privacy, which Supreme Court Justice Louis Brandeis famously described as “the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”** As Brandeis wrote, “The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings, and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.” **This protection is indispensable to the protection of security, properly conceived. In a free society, one that is genuinely committed to self-government, people are secure in the sense that they need not fear that their conversations and activities are being watched, monitored, questioned, interrogated, or scrutinized.** Citizens are free from this kind of fear. **In unfree societies, by contrast, there is no right to be let alone, and people struggle to organize their lives to avoid the government’s probing eye.** The resulting unfreedom jeopardizes, all at once, individual liberty, self-government, economic growth, and basic ideals of citizenship.

It might seem puzzling, or a coincidence of language, that the word “security” embodies such different values. But the etymology of the word solves the puzzle; there is no coincidence here. In Latin, the word “securus” offers the core meanings, which include “free from care, quiet, easy,” and also “tranquil; free from danger, safe.” People who are at physical risk because of a threat of external violence are by definition in danger; they are not safe. **So too, people made insecure by their own government, in their persons, houses, papers, and effects, can hardly be “free from care” or “tranquil.”** And indeed, the first sentence of the Constitution juxtaposes the two values, explicitly using the word “secure”: We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America” (emphasis added).

Privacy Key to Freedom of Association

Privacy protection part of the freedom of association

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

The Court first described the freedom of association as a critical constitutionally protected right in NAACP v. Alabama in 1958. In that case, the NAACP challenged a state court order requiring it to disclose its membership lists. The NAACP objected that revealing the identities of its members would impair the rights of these individuals to engage in “lawful association in support of their common beliefs.” In finding that this claim deserved constitutional protection, the Supreme Court stated: **“Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association,** as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly.” In subsequent years, the Supreme Court made clear **that this freedom of association is grounded in the First Amendment.** The freedom of association is thus protected as “an indispensable means of preserving” the First Amendment right of freedom of speech and other individual liberties. It protects not only actual speech, but also the associations among people, especially when they come together to advance common beliefs such as those on political, religious, cultural or economic matters. Government action may impinge on such First Amendment rights even if it is not directly aimed at limiting freedom of speech or association. The Supreme Court has recognized that the First Amendment **“rights of free speech and association . . . are protected** not only against heavy-handed frontal attack, but also **from being stifled by more subtle governmental interference.”** In particular, disclosure of associations among individuals, and of connections between individuals and advocacy groups, can have a chilling effect on the exercise of associational rights that impinges on these constitutional freedoms. In originally outlining the freedom of association in NAACP v. Alabama, the Court explained **that individuals should be free not only to join together in advocacy but also to do so without fear that their associations will be revealed**, noting that: It is hardly a novel perception that **compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved.** This Court has recognized the vital relationship between freedom to associate and privacy in one’s associations. The Court continued by noting that this safeguard was particularly important “where a group espouses dissident beliefs.” Thus, **the constitutional guarantee of associational rights under the First Amendment “encompasses protection of privacy of association in organizations.” The protection for privacy of association stems from recognition that individuals who support controversial causes may be subject to harassment or intimidation if their connections with organizations promoting these causes are disclosed.** The Court has also acknowledged the need to protect privacy where revealing associations to the government could subject an individual to detrimental government action. For example, the Court struck down a requirement that public school teachers identify all the organizations in which they were members, noting that “the pressure upon a teacher to avoid any ties which might displease those who control his professional destiny would be constant and heavy.” Since first recognizing this right to privacy in one’s associations, **the Court has found in**

numerous cases that rules requiring disclosure of affiliations violated the First Amendment because they had a chilling effect that undermined the freedom of association.

International Law Protects Privacy

International law & Treaties protect against surveillance

Marko Milanovic, Lecturer, University of Nottingham School of Law; Visiting Professor, University of Michigan Law School, Fall 2013; Secretary-General, European Society of International Law, Human Rights Treaties and Foreign Surveillance: Privacy and the Digital Age, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485

On any assessment the Assembly's resolution on the right to privacy in the digital age represents a major development. It firmly puts the issue of electronic surveillance within the framework of international human rights law. It directly invokes Article 12 UDHR and Article 17 ICCPR. In the preamble, the Assembly expresses its deep concern 'at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights' (emphasis added). Operative paragraph 3 affirms 'that the same rights that people have offline must also be protected online, including the right to privacy,' while op. para. 4 calls upon states 'to respect and protect the right to privacy, including in the context of digital communication' – the reference to the obligation to protect being especially significant as it requires states to regulate the conduct of non-state actors, such as telecommunications companies

International law protects privacy rights

Marko Milanovic, Lecturer, University of Nottingham School of Law; Visiting Professor, University of Michigan Law School, Fall 2013; Secretary-General, European Society of International Law, Human Rights Treaties and Foreign Surveillance: Privacy and the Digital Age, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485

Rather, want I want to look at is how the legality of such programs would be debated and assessed with the framework of international human rights law, and specifically under the major human rights treaties to which the 'Five Eyes' and other states with sophisticated technological capabilities, such as Germany, France or Russia, are parties – the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). Both of these treaties protect the right to privacy. Drawing almost verbatim on Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 ICCPR provides that: No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. Article 8

ECHR, on the other hand, stipulates that: Everyone has the right to respect for his private and family life, his home and his correspondence.

-

Targeted Surveillance Good/Mass Surveillance Bad

Targeted surveillance doesn't trade off with privacy but current mass surveillance creates a negative balance that's harms privacy rights

Lomas 14 (Natasha, "Digital Privacy Is "The New Frontier Of Human Rights",
<http://techcrunch.com/2014/11/23/privacy-human-rights-frontier/>)

The impact of mass, digitally-enabled state surveillance upon individuals' privacy has been described as "the new frontier of human rights" by Member of the European Parliament, Claude Moraes, who was giving an annual lecture on behalf of the Centre for Research into Information, Surveillance and Privacy at the London School of Economics on Friday.

Moraes is chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), which conducted an inquiry into electronic mass surveillance of European Union citizens last year, in the wake of Edward Snowden's revelations about the NSA's digital dragnets.

Moraes said there is a growing understanding among members of the European Parliament of the need to balance state surveillance practices with individual privacy rights, although he noted there is variation at the level of individual MEPs and Member States, with some (such as the U.K.) taking a far more pro-surveillance and anti-privacy position.

He described the notion that there is an either/or dichotomy between security and privacy as a falsehood — arguing that targeted surveillance and proportionate data capture processes are more effective counter-terrorism measures, and reiterating Snowden's argument that gathering "haystacks" of information hinders rather than helps the cause of tracking down a few interesting "needles".

"Fighting terrorism is actually fought better by understanding that targeted information is a far better thing, rather than this mass surveillance approach," argued Moraes.

"People in Germany who understand what happens when you have unfettered mass surveillance, where information is then out there being used for negative purposes, understand where that can lead. But if you have targeted information... then we are in a society where that privacy balance is preserved," he continued, adding: "It's the terrorists who want to deprive us of the freedoms that we all fight for. They're not interested in these freedoms.

"That's what I find is happening in the current narrative. Certainly across the European Union with more and more of my colleagues understanding that fighting for a balance and an understanding that mass surveillance has its damaging aspects is something that we need to deal with."

By way of an example of a more nuanced mindset in the European Parliament when it comes to surveillance and privacy, Moraes gave the example of the Passenger Name Record agreement between the EU and the US which he said the Parliament will shortly be referring to the European Court of Justice — to judge whether it is "proportionate and necessary".

He also referred back to the ECJ's decision, back in April, to strike down the European Data Retention Directive that was made in the wake of 7/7 terror attacks — with the Court determining it to be disproportionately broad and contra to individual privacy rights.

Moraes noted that such "untargeted data grabs" are the typical political trigger response to terror attacks, and make the business of creating the sought for balance between surveillance and privacy more difficult to achieve — given that security services will always ask for more surveillance powers at times of heightened terror fears, while politicians will want to be seen doing something to shore up national security.

But — at a European Union level, at least — he said those knee-jerk security reactions are being more critically examined now, in a post-Snowden data retention "enlightenment" (as opposed to what he dubbed the pre-Snowden "data retention dark ages").

"Today as a result of having our inquiry even those people who started to call [Snowden] a traitor must now realize we have a whole group of people who must now at least understand that mass

surveillance is something that is at least troubling and that we must do something about it,” he said. “The privacy agenda from the European Union now is very strong.”

Moraes said the LIBE committee is focusing the next stage of its electronic surveillance inquiry on exploring the notion of a digital bill of rights as a way to create structure to support more proportionate surveillance practices that do take individual privacy rights into consideration.

However, despite more support for a “privacy agenda” at the European Parliament level he cautioned there are still huge vested interests pushing in the other direction — so continuing to bang the drum for mass digital surveillance as a security panacea. It’s therefore imperative that the EU thoroughly interrogates the technical and moral complexities underpinning this new human rights frontier, he said.

“The next phase of this enquiry into mass surveillance has to be about our security, a digital bill of rights, about where encryption is going, what the cloud means, where our privacy is going. Privacy is critical. And the idea that there is going to be no privacy unelect, or no idea of where we place privacy has got to be wrong,” said Moraes.

“The next phase of our enquiry has to be on where we take this concept of privacy, where we take the concept of regulation. It is an extremely challenging time... I don’t have huge faith in many Member States to do this, there’s so many vested interests, vested security interests to not do this — but we have to try and do this.”

He added that the big challenge for privacy rights activists now is articulating a strong moral case for privacy, so spreading “more powerful narratives about surveillance” and educating people on why privacy matters — at a time when security concerns and commercial technology services are pushing against it like never before.

“Ultimately the Member States will have to step up to the plate, because they ultimately control the agenda. If people in this room don’t convince the individual Member States and governments of the big countries to make shifts on privacy, and to change the moral and political climate around security and privacy then of course we won’t make real progress. And every time we get the shocks and changes in atmosphere around terrorism then we’ll take a step back. And of course we see that today — with ISIS and ISIL,” he said.

“We need a more powerful moral narrative, more powerful technical narrative... Here’s where this issue is different from many other issues, the knowledge level is very low, amongst people more widely, because it is very technical, because it’s very complex, so although it’s the new frontier of human rights it’s a very complicated frontier of human rights... It’s very different from other human rights issues — it’s one where we have to educate others because they will not always see the importance of it.”

Mass surveillance doesn’t work

Bruce Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation’s Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc.,

3/24/15 [“Why Mass Surveillance Can’t, Won’t, And Never Has Stopped A Terrorist “ Online: [“http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist”](http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist)]

The US intelligence community also likens finding a terrorist plot to looking for a needle in a haystack. And, as former NSA director General Keith Alexander said, “you need the haystack to find the needle.” That statement perfectly illustrates the problem with mass surveillance and bulk collection. When you’re looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you’re also adding much more noise. And despite the NSA’s “collect it all” mentality, its own documents bear this out. The military intelligence community even talks about the problem of “drinking from a fire hose”: having so much irrelevant data that it’s impossible to find the important bits. We saw this problem with the NSA’s eavesdropping program: the false positives overwhelmed the system. In the

years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Suspicious Activity Reports —or SAR — database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent \$8,500 to a Somali group that posed no direct threat to the US — and that was probably trumped up so the NSA would have better talking points in front of Congress. The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon finish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportionate impact on the criteria used to decide who's a likely terrorist, leading to ineffective detection strategies.

Protecting Privacy key to Innovation

The protection of privacy is necessary to innovation

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

A commercial culture that sees privacy as threatening its own valued practices of knowledge production will register privacy regulation as a threat. But a society that values innovation ignores privacy at its peril, for privacy also shelters the processes of play and experimentation from which innovation emerges. In short, privacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the political and intellectual culture that we say we value.

Big data represents innovation but it does not drive innovation, it undermines it

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

Conditions of diminished privacy also impair the capacity to innovate. This is so both because innovation requires the capacity for critical perspective on one’s environment and because innovation is not only about independence of mind. Innovation also requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering. A society that permits the unchecked ascendancy of surveillance infrastructures, which dampen and modulate behavioral variability, cannot hope to maintain a vibrant tradition of cultural and technical innovation. Efforts to repackage pervasive surveillance as innovation — under the moniker “Big Data” — are better understood as efforts to enshrine the methods and values of the modulated society at the heart of our system of knowledge production. The techniques of Big Data have important contributions to make to the scientific enterprise and to social welfare, but as engines of truth production about human subjects they deserve a long, hard second look. An understanding of “innovation” as the absence of regulatory constraint features prominently in contemporary information policy discourse. The need to incentivize innovation is offered as the justification for strengthening proprietary control of intellectual goods and as the justification for regulating information networks lightly (if at all). In debates about information privacy, innovation is increasingly positioned as a justification for withholding data protection, and for looking the other way when privacy breaches appear to violate existing promises to consumers and regulators. Sometimes the opposition between privacy and innovation is explicit, but more often it is implicit in rhetoric that aligns innovation with unfettered information collection and processing.⁴⁵ Innovation then joins the list of values against which privacy must be balanced — and, of course, no one wants to go on record as opposing innovation. Confronted with asserted conflicts between privacy on the one hand and innovation and economic competitiveness on the other, regulators timidly opine that privacy harms result from “unexpected” disclosures of personal information and that more robust guarantees of notice and choice therefore may be needed to “build[] consumer trust in the marketplace.”⁴⁶

Innovation depends on the strong subject

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

This simplistic view of the relationship between privacy and innovation is wrong. It fails to take into account either the nature of innovative practice or the dynamic function of privacy. Innovation does not follow an inevitable, linear arc to a predetermined end. It depends for its realization on innovative practice by situated subjects, and innovative practice is not linear; in Brett Frischmann’s words, it is “multidirectional, stochastic, [and] full of feedback loops.”⁴⁷ External obstacles, whether material or regulatory, affect the feedback loops, but also represent opportunities; innovation emerges from the interplay between freedom and constraint. Innovative practice is threatened most directly when circumstances impose intellectual regimentation, prescribing orthodoxies and restricting the freedom to tinker. It thrives most fully when circumstances yield serendipitous encounters with new resources and ideas, and afford the intellectual and material breathing room to experiment with them.⁴⁸ When the predicate conditions for innovation are described in this way, the problem with characterizing privacy as anti-innovation becomes clear: it is modulation, not privacy, that poses the greater threat to innovative practice. Regimes of pervasively distributed surveillance and modulation seek to mold individual preferences and behavior in ways that reduce the serendipity and the freedom to tinker on which innovation thrives. The suggestion that innovative activity will persist unchilled under conditions of pervasively distributed surveillance is simply silly; it derives rhetorical force from the cultural construct of the liberal subject, who can separate the act of creation from the fact of surveillance. As we have seen, though, that is an unsustainable fiction. The real, socially constructed subject responds to surveillance quite differently — which is, of course, exactly why government and commercial entities engage in it. Clearing the way for innovation requires clearing the way for innovative practice by real people. Innovative practice in turn requires breathing room for critical selfdetermination and physical spaces within which the everyday practice of tinkering can thrive.

Big data will not drive innovation

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

There is, however, a new flavor of innovation on the scene: Big Data. “Big Data” is shorthand for the combination of a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times. The process involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a technique for converting data flows into a particular, highly data-intensive type of knowledge.⁴⁹ The technique of Big Data can be used to analyze data about the physical world — for example, climate or seismological data — or it can be used to analyze physical, transactional, and behavioral data about people. So used, it is vastly more nimble than old practices of category-driven profiling developed in the late twentieth century and now widely criticized.⁵⁰ According to its enthusiasts, Big Data will usher in a new era of knowledge production and innovation, producing enormous benefits to science and business alike. According to its critics, Big Data is profiling on steroids, unthinkably intrusive and eerily omniscient. Big Data’s claims to epistemological privilege stem from its asserted fidelity to reality at a very high level of detail. Its most avid enthusiasts do not paint it simply as an improvement in the state of the profiling art; rather, they claim that Big Data will eliminate the need for models altogether.⁵¹ In place of predetermined and inevitably artificial categories, it will produce predictions and recommendations finely tailored to particular situations. Armed with enough data, researchers of all types will be able to jettison the post hoc, oversimple models through which they — and through them, we — have perceived the world in favor of reality, unfiltered. In the era of Big Data, we will have knowledge without visionaries. In the domain of information processing, we will have innovation without innovators, purged of the sloppiness, bias, and incompleteness that attends ordinary human endeavors. The always-on digital feedback processes of Big Data are highly attuned to individual variation, and therefore capable of

making minute distinctions among individual subjects, but they generate and automatically refine their own analytic frameworks. Even those observers who do not explicitly subscribe to this understanding of Big Data offer tantalizing visions of improved understanding and innovative leaps in areas ranging from pandemic detection and drug design to traffic control and inventory management.⁵² To begin with, it is worth unpacking the atmospherics surrounding some of the more extreme claims about what Big Data promises. There is considerable irony in the spectacle of a technoculture that has long celebrated innovation as the ultimate expression of enlightened individualism seeking a modality for innovation that will transcend individual agency altogether. Irony compounds irony: some of the claims on behalf of Big Data, those framed in terms of a “singularity” waiting in our soon-to-be-realized future, sound quasi-religious, conjuring up the image of throngs of dyed-in-the-wool rationalists awaiting digital rapture.⁵³ To cultural historians, these claims likely have a familiar ring: they are expressions of the “technological sublime,” a utopian (and singularly American) faith in the promise of better living through technology.⁵⁴ Reality lags predictably behind utopia, however, and so it is important to consider the ways in which Big Data as an enterprise is actually developing. Considered more soberly, the claim that Big Data will eliminate the need for scientific modeling simply does not make sense. By this claim I do not mean to imply that the techniques that comprise Big Data lack value as tools for knowledge discovery, nor to deny that those techniques will sometimes represent radical improvements upon preexisting tools. To take just two examples, the application of predictive analytics to massive data sets will certainly enhance climatologists’ understanding of weather patterns and improve epidemiologists’ ability to understand and respond to public health problems. It is beyond serious question that the techniques that comprise Big Data offer vitally important strategies for promoting human flourishing in an increasingly complex, crowded, and interdependent world. But those techniques cannot themselves decide which questions to investigate, cannot instruct us how to place data flows and patterns in larger conceptual or normative perspective, and cannot tell us whether and when it might be fair and just to limit data processing in the service of other values. These shortcomings mean that Big Data cannot replace either human-driven modeling or the prior decisions about direction and scope that set the substantive and ethical parameters for particular programs of investigation. Here it is worth noting that the enthusiasm for Big Data has another set of cultural antecedents that is less immediately obvious, but ultimately more troubling. As Wall Street’s flavor of the month, Big Data stands in a long and undistinguished tradition. The “smartest guys in the room”⁵⁵ no longer work for Enron, Lehman Brothers, or AIG; now they work for Google or Target or Axiom, pursuing the holy grail of knowing customers better than they know themselves. Features in the Wall Street Journal and the Economist pay homage to the heady combination of computing horsepower and technical machismo that the quest demands.⁵⁶ Personalization is the new religion of the information society, and the quant jocks of Big Data are its high priests. The skeptic’s questions about downside risks go unanswered, and often unasked. Innovation is never a neutral quantity. Technologies and artifacts are shaped by the values, priorities, and assumptions of their developers, and often by those of their users as well. Of course, many technologies are designed or refined with particular goals in mind, but here I am referring to a different and less deliberate shaping process, through which artifacts come to reflect and reproduce beliefs about the types of functions and ways of living and working that are important.⁵⁷ To return to a previous example, the design of an in-car GPS interface prioritizes getting from point A to point B most efficiently. The design of a child’s car seat prioritizes modularity and affordability over compact size; therefore, it promotes safety but not the purchase of smaller, more fuel-efficient cars. The techniques of Big Data are no exception to this rule of cultural constructedness.

Big data innovation not verifiable because the results and processes are secret

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

Big Data may seem to update and improve upon traditional scientific modeling because its investigations are both openended and ongoing. Such investigations do not conform to the idea of the scientific research program as a series of limited data collections for the purpose of testing and possibly falsifying a particular hypothesis.⁵⁸ Big Data’s relative advantage (according to

some) is its ability to make sense, in real time, of an ever-changing data landscape. Decisions about research agendas need not be explicit, however. The research agendas that drive Big Data will be those of the entities that deploy it. It is at this point that a more general principle of falsifiability begins to matter. Even within academic computational science, attaining the transparency required to confirm or falsify results is Big Data's Achilles' heel; observers have begun to point to a "credibility crisis" that derives from inadequate disclosure of data sets and methods.⁵⁹ Big Data in the private sector neither pretends nor aspires to transparency; research agendas and data sets are typically kept secret, as are the analytics that underpin them.

Big data innovation based on a false ideology

Julie Cohen, Professor, Georgetown University, "What Privacy Is For," HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

The second problem concerns underlying ideology. Big Data is the ultimate expression of a mode of rationality that equates information with truth and more information with more truth, and that denies the possibility that information processing designed simply to identify "patterns" might be systematically infused with a particular ideology. Those core premises are deeply entrenched within American intellectual culture. Even when private-sector research agendas are uncovered and become the subjects of investigation and critique in the pages of The Atlantic and the New York Times Magazine,⁶⁰ we seem unable to challenge the techniques of Big Data as knowledge-production practices. But the denial of ideology is itself an ideological position. Information is never just information: even pattern identification is informed by values about what makes a pattern and why, and why the pattern in question is worth noting. Pattern identification also is informed by both content and categorization biases in the databases of origin; thus, for example, the Facebook data set has particular demographics and reflects particular beliefs about what makes someone a "friend." Big Data does not interrogate those choices; it does not need to. Big Data is the intellectual engine of the modulated society. Its techniques are techniques for locating and extracting consumer surplus and for managing, allocating, and pricing risk, and it takes data sets at face value. But the values of predictive rationality and risk management are values, and they are the values with which serious critics of Big Data need to contend. The third problem is, once again, the problem of constructed subjectivity, and more specifically the problem of subjectivity constructed in the service of the self-interested agendas of powerful economic actors. The integrity of behavioral and preference data is a longstanding concern within social science research, and this concern has led to the development of elaborate techniques of research design to minimize distortion. Big Data attacks the problem of data integrity from a different direction by gathering behavioral data at the source (and often without the subjects' knowledge). Even when it operates unobserved, however, Big Data cannot neutralize the problem of constructed subjectivity, and instead is more likely both to exacerbate the problem and to insulate it from public scrutiny. The techniques of Big Data subject individuals to predictive judgments about their preferences, and the process of modulation also shapes and produces those preferences. The result is "computational social science" in the wild, a fast-moving and essentially unregulated process of experimentation on unsuspecting populations.⁶¹ Big Data's practitioners are never "just watching." And here informational capitalism's interlinked preferences for consumer surplus extraction and risk management can be expected to move subjectivity in predictably path-dependent directions.⁶²

It's immoral innovation – it privatizes human subject research

Julie Cohen, Professor, Georgetown University, "What Privacy Is For," HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

By now it should be apparent that there are important procedural and ethical objections to some of the most common applications of Big Data. As deployed by commercial entities, Big Data represents the de facto privatization of human subjects research, without the procedural and ethical safeguards that traditionally have been required. Population studies using the techniques of Big Data typically proceed without the sorts of controls that might be instituted by, for example, an institutional review board.⁶³ I tend to think this is a very bad idea. At minimum, it should be uncontroversial to suggest that these issues require further study

All big data innovations only favor consumption and the market

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

The distinction between predictive rationalism and reason directs our attention to the quality of the innovation Big Data seems likely to produce, and to the sorts of innovation most likely to be lost. Even if Big Data did not continually alter its own operands, it would not operate in a vacuum. It is a mistake to think of the techniques of Big Data as simply adding to the amount of information circulating within society. The valorization of predictive rationality and risk management inevitably displaces other kinds of knowledge that might be generated instead. Stimuli tailored to consumptive preferences crowd out other ways in which preferences and self-knowledge might be expressed, and also crowd out other kinds of motivators — altruism, empathy, and so on — that might spur innovation in different directions.⁶⁵ In a consumption-driven economy, the innovations that emerge and find favor will be those that fulfill consumption-driven needs. Contemporary applications of Big Data extend beyond marketing and advertising to core social and cultural functions, including the study of intellectual preferences and the delivery of higher education.⁶⁶ Systematizing those functions according to the dictates of predictive rationality threatens important social values. It crowds out the ability to form and pursue other kinds of agendas for human flourishing, which is indispensable both to maintaining a vital, dynamic society and to pursuing a more just one.

Privacy promotes better innovations

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

In short, privacy is important both because it promotes innovative practice and because it promotes particular kinds of innovation that are extraordinarily important. The human innovative drive is both unpredictable and robust, but it does not follow that all environments are equally favorable to innovation or that all environments will produce the same kinds of innovation. If privacy and serendipity are critical to innovation — by which I mean critical both to the likelihood that innovation will occur and to the substance of that innovation — there is reason to worry when privacy is squeezed to the margins and when the pathways of serendipity are disrupted and rearranged to serve more linear, commercial imperatives. Environments that disfavor critical independence of mind and that discourage the kinds of tinkering and behavioral variation out of which innovation emerges will, over time, predictably and systematically disfavor innovation of all types. Environments designed to promote consumptive and profitmaximizing

choices will systematically disfavor innovations designed to promote other values. The modulated society is dedicated to prediction but not necessarily to understanding or to advancing human material, intellectual, and political well-being. Data processing offers important benefits, but so does privacy. A healthy society needs both.

Consumers don't even try to protect privacy from IoT devices

Melissa W. Bailey, J.D. Candidate, 2016, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, TEXAS LAW REVIEW
<http://www.texasrev.com/wp-content/uploads/2016/04/Bailey.FinalPDF.pdf>

Consumers also disregard their privacy rights on a more granular level through what is called the “Internet of Things” (IoT), or a system of devices that connect to each other via the Internet.¹² Surprisingly, consumers purchase these data devices with little knowledge of—and perhaps little regard for—whom the data can be disclosed to.¹³ Such devices include a pocket breathalyzer whose results can be used against the consumer in court,¹⁴ fitness-tracking devices that could be used to determine disabilities,¹⁵ and a car plug-in that tracks a consumer’s driving data, which then determines the appropriate insurance premium based on the user’s driving habits.¹⁶

IoT responsible for widespread privacy violations

Alexander H. Tran, JD Candidate, Columbia Law School, *The Internet of Things and Potential Remedies in Privacy Tort Law*, March 7, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769675

The IoT represents an amazing technological advancement that can provide enormous benefits to consumers. For example, a recent FTC Staff Report lists several potential benefits resulting from connected IoT devices. IoT health devices can provide better access to consumer health data resulting in greater monitoring of serious health conditions and regular interaction between physician and patient.¹² Further, home automation devices like smart thermostats and smart alarms can allow consumers to control features in their homes while they are commuting to and from work.¹³ However, despite many benefits, these connected devices also generate enormous amounts of consumer data resulting in greater privacy and security concerns.¹⁴ Specifically, some IoT devices collect sensitive sensor data that many consumers may not want to share with the public. Despite its benefits, the IoT also presents many dangers such as potential security and privacy risks. Security risks are prominent because IoT devices may allow intruders to access and misuse sensitive sensor data collected and transmitted from each device.¹⁵ Further, privacy issues are implicated because these devices generally collect sensitive personal information and collection of this data can lead to unpermitted third party inferences or unlawful discrimination.¹⁶ According to a FTC Staff Report, expert IoT panelists suggested that IoT devices present potential security risks in three forms: (1) enabling unauthorized access and misuse of personal information, (2) facilitating attacks on other systems, and (3) creating safety risks.¹⁷ First, unauthorized access of sensor data is dangerous because these breaches may result in exploited vulnerabilities in IoT devices leading to identity fraud and theft.¹⁸ The IoT exacerbates this risk because “as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.”¹⁹ Second, by installing more connected IoT devices, security vulnerabilities in one device may facilitate attacks on the consumer’s network and enable attacks on other systems.²⁰ Finally, there are safety concerns implicated by the IoT because unauthorized persons may create risks to physical safety such as controlling internal computer networks in cars or remotely controlling individual health devices such as insulin pumps used by consumers.²¹ Although all these security risks present potential dangers related to the IoT, this paper will mainly focus on the first issue presented, unauthorized access and misuse of sensitive sensor data relating to personal information. Furthermore, the IoT creates several privacy risks due to the large amount of sensor data recorded, stored, and transmitted by each IoT device. For example, the FTC noted that fewer than 10,000 households using IoT home-automation products, can “generate 150 million discrete data

points a day or approximately one data point every six seconds for each household.”²² This immense volume of sensor data causes privacy issues that several different leading scholars have explored. Before diving into these discussions, I would like to preface my analysis by adopting Professor Paul M. Schwartz privacy paradigm that provides one definition of “privacy.” Professor Schwartz views “privacy” as “control (or rights of control) over the use of personal data or information.”

Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 MINN. L. REV. 1137, 1180 (2002) (“Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information.”).²⁶ Id. (asserting that “[...] although one’s Social Security number does not in and of itself reveal much about an individual, it provides access to one’s financial information, educational records, medical records, and a whole host of other information.”).²⁷ Id. at 1181 (providing an example, “[...] the firm HireCheck serves over 4000 employers to conduct background checks for new hires or current employees. It conducts a national search of outstanding warrants, a Social Security number search to locate age, past and current employers, and former addresses, a driver record search, a search of worker’s compensation claims ‘to avoid habitual claimants or to properly channel assignments,’ a check of civil lawsuit records, as well as searches for many other types of information. These investigations occur without any external oversight, and individuals often do not have an opportunity to challenge the results.”).

Combining information creates widespread privacy problems

Alexander H. Tran, JD Candidate, Columbia Law School, The Internet of Things and Potential Remedies in Privacy Tort Law,, March 7, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769675

Privacy scholar Professor Daniel Solove, suggests that large data sets can create an “aggregation problem” for privacy.²⁵ Professor Solove suggests that individual data (like one’s social security number) viewed in isolation is not revealing, but when combined with other data (such as one’s financial information, educational records, medical records), this can paint a portrait about an individual’s personality called a “digital biography.”²⁶ A digital biography is problematic because consumers’ lives are not only “revealed and recorded, but also can be analyzed and investigated” by unauthorized or unknown third parties like employers and the government.²⁷ Solove argues that the digital biography captures a “distorted persona, one who is constructed by a variety of external details” that is often inaccurate.²⁸ Digital biographies are inaccurate because individuals may omit explanatory details that would explain cross-contextual inferences.²⁹ Without these pertinent details, information viewed in other contexts may become unrepresentative and inaccurate.³

Loss of Privacy Threatens Cyber Security

The collection and storage of data threatens cyber security

- . Jillisa Bronfman, Director, Privacy and Technology Project, Institute for Innovation Law, University of California-Hastings, Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population, DUKE LAW & TECHNOLOGY REVIEW v. 14, February2016,
<http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1289&context=dltr>

Data security is a precondition of privacy protection. The FTC met in November 2013 to hear comments on IoT, and issued a staff report in January 2015. The commenters focused on three areas of harm from security breaches of IoT, including personal information, personal safety, and other systems.⁴⁶ Thus, companies should consider both physical security, including locked doors and facilities, and network security, including authentication and back-up protocols. There are exponentially more security issues in a distributed system vis-à-vis a centralized system such as a single data center. IoT presents several additional levels of security issues, from the device to the network to the collection or storage of data.

Loss of privacy in home IoT devices increases the risk of terrorism

- . Jillisa Bronfman, Director, Privacy and Technology Project, Institute for Innovation Law, University of California-Hastings, Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population, DUKE LAW & TECHNOLOGY REVIEW v. 14, February2016,
<http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1289&context=dltr>

Increasingly, security in the home is the foundation for national security. Looking to hack devices connected from people's homes to the Internet? Searches can be performed online,⁵⁷ to find networked home devices to hack, and can be done by anyone, including those with commercial or political motives. Access to any one device can allow access to an entire networked system, particularly when the device has no password or security mechanism of its own. When hackers from outside the United States reach home networks, they may find easier access to personal data than they have in the past through the portals established by government entities or large commercial operations in the United States. Therefore, security begins at home, and in the home. Indeed, there is a pending threat of cyberterrorism against home monitoring systems if national security is dependent on the passwords consumers enter into their home networks. “Passwords are the ‘keys to the castle’ for important parts of our lives online,” yet they are often a weak link in the security of home networks.⁵⁸ In addition to data collected by devices connected to the Internet, consumers are voluntarily entering much of the private data collected by the home monitoring devices, including entering their names, addresses, personal contacts, medical information and other personal data in order to sign up for services and activate the devices. One example would be in naming the devices, or the sets of data, including using consumers’ and their children’s names.⁵⁹

Privacy Internal Link Turns Case – Markets/Economic Growth

Privacy supports the market

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

Privacy supports the basic market mechanism by hiding enough distracting, value-laden information from market participants. A certain absence of knowledge focuses us on market-relevant considerations such as quality and price over salient but distorting information such as personal or political commitments. The beauty of the market mechanism is that you do not need to know that the person you are dealing with voted for a politician you hate or doubts we landed on the moon, or for any other basis for distrust or discrimination, only that he is offering the best quality good at the lowest price. Privacy also enables the longevity of business partnerships through the facilitation of economic intimacy. Market relationships face an ever-present specter of defection—the prospect of a better deal somewhere else—which participants manage in part through the selective disclosure of preferences and expectations without penalty. In business, as in life, privacy helps you let the right one in, and in the process engenders the trust necessary for economic stability.⁵ Finally, privacy helps keep a check on information asymmetry between people and firms. While economists agree that information asymmetry is undesirable, the standard remedy is to introduce additional information—for instance, through mandatory disclosure laws.⁶ But today's firms are increasingly more capable than consumers of processing new information, such that introducing more information only exacerbates asymmetry and its discontents. Privacy can interrupt this dynamic and help save the market from itself.

Privacy supports efficiency in many areas

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

Several responses to economic skepticism about privacy take the form of pointing out that privacy sometimes yields greater efficiency. In the privacy literature, Richard Murphy, Paul Schwartz, and Peter Swire, among others, pursue this approach.⁴⁰ “The economic argument is powerful, and disables much of the lofty rhetoric of privacy rights,” concedes Murphy, “[b]ut it does not imply that all limits on disclosure of personal information are inefficient.”⁴¹ Sometimes the exogenous preference for privacy outweighs the benefits of disclosure, and disclosing information about people against their will can lead them to distort or withdraw information going forward, erasing the supposed gains to efficiency of lesser privacy. For Schwartz, “a strong economic argument can be made in favor of privacy” in the context of health law.⁴² Schwartz cites the “positive economic role that data privacy plays in many circumstances,” but his arguments focus instead on the unintended consequences of adding information to a marketplace full of critical imperfections.⁴³ For example, employers are likely to make mistakes in discriminating against employees on the basis of genetic predispositions that are unlikely to ever materialize.⁴⁴ Swire points to the role of trade secrets and confidentiality in promoting efficient transactions.⁴⁵ A small handful of economists have reached similar conclusions about the role of privacy in promoting efficiency. In agency theory, work by economist Jacques Cremer, for instance, suggests that better monitoring removes ‘the ability of the employer to refuse to consider employee excuses, which in turns reduces productivity and the

efficiency of agent selection.⁴⁶ Benjamin Hermalin and Michael Katz observe that the protection of privacy can lead to *ex ante* efficiencies even if restrictions on information is inefficient *ex post*; in insurance markets, for instance, health privacy eliminates socially wasteful costs of testing each participant's health.⁴⁷ And the observation that information is necessary to innovation can be met with the claim that consumers who are too nervous about privacy will not adopt new services or modes of commerce like the Internet. In a magisterial literature review of the economics of privacy, which I cannot recommend enough, Alessandro Acquisti and colleagues review decades of economic analysis that they group into three "waves."⁴⁸ Reviewing this work, the authors find that "it is not possible to conclude unambiguously whether privacy protection entails a net 'positive' or 'negative' change in purely economic terms: its impact is context specific."⁴⁹ Privacy can lead to economic inefficiency, but not always.⁵⁰ This insight highlights, I think, a limitation with the insider critique: the critique does not tell us much about the deeper relationship between privacy and markets. The insider critique is more caveat than criticism. It is an important caveat, of course, and should give the traditional economist pause. But even in its strongest form, the critique at most reveals privacy to be yet another lever of efficiency that can ratchet either way depending on where and how it is applied.

Privacy supports the market

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

The preceding section lays out several key ways in which privacy, far from undermining markets, supports the market mechanism itself. In a world without privacy, markets would look and feel very different, and lose many of the affordances and benefits we see today. None of this is to deny that contemporary market forces can be pernicious to privacy and other values, only that markets assume and rely upon privacy even as they sometimes undermine it. If anything, the role of privacy in markets suggests a role for law, explored in greater depth in the next Part, in protecting the market essentially from itself. It may be tempting to conclude that this Article is not a love story at all but a story of misadventures in symbiosis. Markets are parasitic upon privacy, which gains nothing in return. The outside critique, which bemoans the impact of contemporary market forces on privacy and calls for intervention, implicitly paints such a picture. And yet, the notion of a parasitic market misses much. This position fails to acknowledge, let alone account for, the role that markets play in safeguarding privacy or promoting privacy's deepest goals. I do not mean safeguarding in the sense of delivering greater privacy through competition or information markets, as Laudon and others argue.¹³⁷ Again, I point to something more fundamental. I see at least two ways that privacy assumes and relies upon markets to fulfill its important role in society. First, markets help privacy accomplish its deeper goal of supporting human flourishing by helping to meet basic needs and connecting people to the material and cultural resources they require to self-determine. Second, and more basically, markets remain the most plausible mechanism by which to distribute resources that does not necessarily depend on highly detailed information about individuals.

Privacy Generally Good

Privacy critical to happiness

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

This framework provides a useful way of thinking about privacy. Even if we cannot agree whether we have a right to privacy, or what the scope of any particular privacy right should be, the right to pursue it should be as uncontroversial as the right to pursue happiness. In fact, pursuing privacy is probably an important element of achieving happiness for most citizens.²⁵ Almost everyone needs some time and space to be free with their own thoughts or to control personal information or secrets that they value.

Privacy protects the self-determination of the individual

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

In fact, the liberal self who is the subject of privacy theory and privacy policymaking does not exist. As Part II discusses, the self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate. For this self, privacy performs a function that has nothing to do with stasis. Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.

Privacy enables self-development

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

Privacy’s bad reputation has deep roots in privacy theory. This Part traces those roots to the tradition of liberal individualism, which supplies both the conventional understanding of the self that privacy is thought to protect and the criteria that an intellectually defensible theory of the right to privacy must satisfy.⁴ Neither set of commitments has served privacy theory well. The self who benefits from privacy is not the autonomous, precultural island that the liberal individualist model presumes. Nor can privacy be reduced to a fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic. Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development. So understood, privacy is

fundamentally dynamic. In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them.

Liberal self critical to self-actualization

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

I call this vision of selfhood a postliberal one because its relationship to liberalism requires something more difficult and much more productive than antagonism: a realistic appraisal of the liberal model’s undeniable faults and equally undeniable virtues. Liberal selfhood has an important role to play within privacy theory, but that role is different from the one that most privacy scholars have assumed. The liberal self is an aspiration — an idealized model of identity formation that can be approached only incompletely, if at all. This does not mean that all of its attributes are equally attractive and worth pursuing. Certain features of liberal selfhood have been roundly and justifiably critiqued, most notably its abstraction from embodied reality and its independence from relational ties.¹⁹ But others — most notably the liberal self’s capacity for critical independence of thought and judgment, its commitments to self-actualization and reason, and its aspiration to cosmopolitanism — are essential tools for identifying and pursuing the material and political conditions for self-fulfillment and more broadly for human flourishing.²⁰ But here we must come back to privacy, for the development of critical subjectivity is a realistic goal only to the extent that privacy comes into play. Subjectivity is a function of the interplay between emergent selfhood and social shaping; privacy, which inheres in the interstices of social shaping, is what permits that interplay to occur. Privacy is not a fixed condition that can be distilled to an essential core, but rather “an interest in breathing room to engage in socially situated processes of boundary management.”²¹ It enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making. And once this point is established, privacy’s dynamism becomes clear. Lack of privacy means reduced scope for self-making — along the lines of the liberal ideal, or along other lines. Privacy does not negate social shaping. “In a world with effective boundary management, however, there is play in the joints, and that is better than the alternative. . . . Privacy’s goal, simply put, is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep.”²² Privacy will not always produce expressions of subjectivity that have social value, and here I mean expressly to leave open the question whether there might be particular types of privacy claims that do not merit protection or even respect.²³ Even so, privacy is one of the resources that situated subjects require to flourish.

Privacy critical to self-development and actualization as a person

Jathan Sadowski, journalist, Why Does Privacy Matter? One Scholar’s Answer, The Atlantic, February 26, 2013, www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/

Privacy is not just something we enjoy. It is something that is necessary for us to: develop who we are; form an identity that is not dictated by the social conditions that directly or indirectly influence our thinking, decisions, and behaviors; and decide what type of society we want to live in. Whether we like it or not constant data collection about everything we do -- like the kind conducted by Facebook and an increasing number of other companies -- shapes and produces our actions. We are different people when under surveillance than we are when enjoying some privacy. And Cohen's argument illuminates how the breathing room provided by privacy is essential to being a complete, fulfilled person.

Societal Benefits

Protection of privacy needed for a well-functioning, civil society

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Professor Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits.⁵⁰ Professor Joel Reidenberg contends that “[s]ociety as a whole has an important stake in the contours of the protection of personal information.”⁵¹ Professor Spiros Simitis recognizes that “privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone.”⁵² Then-Professor Robert Post asserts that privacy protection “safeguards rules of civility that in some significant measure constitute both individuals and community.”⁵³ Professor Paul Schwartz has further developed the theory of constitutive privacy in arguing for privacy’s importance to civil society.⁵⁴ Schwartz focuses on how the protection of information privacy will further self-governance and democracy on the Internet.⁵⁵

Autonomy

The private expression of ideas and experimentation with ideas is critical to autonomy

Julie E. Cohen, law professor, Georgetown, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000),
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub>

Autonomous individuals do not spring full-blown from the womb. We must learn to process information and to draw our own conclusions about the world around us. We must learn to choose, and must learn something before we can choose anything. Here, though, information theory suggests a paradox: “Autonomy” connotes an essential independence of critical faculty and an imperviousness to influence. But to the extent that information shapes behavior, autonomy is radically contingent upon environment and circumstance. The only tenable resolution—if “autonomy” is not to degenerate into the simple, stimulus-response behavior sought by direct marketers—is to underdetermine environment. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self. The solution to the paradox of contingent autonomy, in other words, lies in a second paradox: To exist in fact as well as in theory, autonomy must be nurtured.¹⁹⁰

A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition.¹⁹¹ But the benefits of informational autonomy (defined to include the condition in which no information is recorded about nonanonymous choices) extend to a much wider range of human activity and choice. We do not experiment only with beliefs and associations, but also with every other conceivable type of taste and behavior that expresses and defines self. The opportunity to ex-

periment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo.¹⁹²

The benefits of informational privacy are related to, but distinct from, those afforded by seclusion from visual monitoring. It is well-recognized that respite from visual scrutiny affords individuals an important measure of psychological repose. Within our society, at least, we are accustomed to physical spaces within which we can be unobserved, and intrusion into those spaces is experienced as violating the boundaries of self.¹⁹³ But the scrutiny, and the repose, can be informational as well as visual, and this does not de- pend entirely on whether the behavior takes place “in private.” The injury, here, does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another.¹⁹⁴ The universe of all information about all record-generating behaviors generates a “picture” that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we all may be more cautious.

The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, *ex ante*, the acceptable spectrum of belief and be- havior.¹⁹⁵ Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical dif- ferences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the skeptical pragmatist, and the iconoclastic postmod- ernist all share a deep-rooted antipathy toward unreflective conformism.¹⁹⁶ The condition of no-privacy threatens not only to chill the expression of ec- centric individuality, but also, gradually, to dampen the force of our aspira- tions to it.¹⁹⁷

Respect for individual autonomy means we don't treat people as collections of data

Julie E. Cohen, law professor, Georgetown, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000),
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub>

First, informational autonomy comports with important values concerning the fair and just treatment of individuals within society. From Kant to Rawls, a central strand of Western philosophical tradition emphasizes respect for the fundamental dignity of persons, and a concomitant commitment to egalitarianism in both principle and practice.¹⁸⁸ Advocates of strong data privacy protection argue that these principles have clear and very specific implications for the treatment of personally-identified data: They require that we forbid data-processing practices that treat individuals as mere conglomerations of transactional data, or that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or genetic desirability. The drafters of the European Data Protection Directive agreed with this characterization; the Directive is explicitly grounded in “the fundamental rights and freedoms of natural persons.”

Privacy is critical to autonomy

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Autonomy

The analysis of Rachels and Fried suggests a deeper and more fundamental issue: personal freedom. As Deborah Johnson has observed, "To recognize an individual as an autonomous being, an end in himself, entails letting that individual live his life as he chooses. Of course, there are limits to this, but one of the critical ways that an individual controls his life is by choosing with whom he will have relationships and what kind of relationships these will be.... Information mediates relationships. Thus when one cannot control who has information about one, one loses considerable autonomy."⁶

To lose control of personal information is to lose control of who we are and who we can be in relation to the rest of society. A normal person's social life is rich and varied,

encompassing many different roles and relationships. Each requires a different *persona*, a different face. This does not necessarily entail deception, only that different aspects of the person are revealed in different roles. Control over personal information and how and to whom it is revealed, therefore, plays an important part in one's ability to choose and realize one's place in society. This operates on many different levels. On a personal level, for example, one ought to be able to choose one's friends. That means that one should be able to choose to whom to reveal some of the personal revelations that are only shared among friends. This choice is only meaningful if one can also choose to exclude some from friendship and the privileged revelations that come with it. Consider the case of Carrie and Jim. Jim met Carrie at a party and was immediately smitten by her grace and beauty. Unfortunately for Jim it was not mutual. Carrie made it quite clear she had no interest in any kind of relationship. But this brush-off just fueled Jim's obsession with her. He began to stalk her, following her wherever she went and looking her up online, until he knew her daily schedule, her friends, and her favorite shops and restaurants. He did careful research on her trash, reading her letters and inspecting her receipts, learning what kind of cosmetics she used and what her favorite ice cream was. He even peeked through her window at night to see what she wore and how she behaved when she was alone. Even if Jim never did anything to attack or harass Carrie, even if she never found out about his prying, she has lost some of her freedom. She did not want him to have access to her personal life, but he seized it anyway.

Privacy is an issue in other, more professional, relationships as well, as the following case illustrates. Fred Draper⁷ grew up in Brooklyn, where as a youth he ran with a very tough crowd. By the time he was 16 he had been convicted of armed robbery and malicious destruction of property, and was on probation until he was eighteen. But Fred was also a very talented student, and he was fortunate enough to have a teacher in high school recognize his potential and take him under his wing. Through a combination of encouragement, guidance and discipline, the teacher was able to get Fred to focus on school and stay out of trouble, so that he graduated with an outstanding record and won a scholarship to NYU. He was successful there also, going on to law school. Upon finishing law school, Fred was hired by a top Wall Street law firm, where he was well on his way to establishing himself as one of their top young lawyers. Then a newspaper reporter took notice of Fred and his growing prominence and decided to see if there was a story there. There was. The reporter traced Fred back to his old neighborhood and learned about his past history. He wrote a story about it, praising Fred for the way he had overcome his past and made a respectable life for himself. But some of Fred clients had a different reaction. They were not comfortable dealing with a former hood from Brooklyn, so they asked that he be taken off their accounts. The firm complied with their wishes and ultimately let Fred go, deciding that he was too much of a liability to keep. This again illustrates the importance of privacy in allowing people the freedom to realize their potentialities. Once the information about his past had leaked out, Fred was no longer able to maintain his professional persona in relation to his clients, a *persona* that he had proved he was capable of fulfilling.

Dignity

This is the most important impact. Respect for dignity is a baseline requirement of ethical conduct.

Kaczor 12 — Christopher Kaczor, Professor of Philosophy at Loyola Marymount University, holds a Ph.D. in Philosophy from the University of Notre Dame, 2012 (“The Importance of Dignity: A Reply to Steven Pinker,” *Public Discourse*—a publication of The Witherspoon Institute, January 31st, Available Online at <http://www.thepublicdiscourse.com/2012/01/4540/>, Accessed 06-17-2015)

Even if we can successfully disambiguate the term, why is dignity important? The concept of dignity does a better job than autonomy in describing and accounting for the intrinsic value of every human being. We are valuable not simply because of our choices, and still less do we have value only while we are exercising our autonomy. We have value even when we are not choosing or cannot choose. In his 2009 Tanner Lectures at UC Berkeley, “Dignity, Rank, and Rights,” Jeremy Waldron pointed out that in ancient times dignity was accorded in particular to persons regarded as royalty or nobility. Noble persons were accorded rights, privileges, and immunities that accorded with their elevated rank. Contemporary society at its best does not reduce the noble but elevates the commoner, making every single human person equal in rank to the Duke or Lady. Although these ideals are often imperfectly realized in our society, still Waldron has a point when he writes, “we are not like a society which has eschewed all talk of caste; we are like a caste society with just one caste (and a very high caste at that): every man a Brahmin. Every man a duke, every woman a queen, everyone entitled to the sort of deference and consideration, everyone’s person and body sacrosanct, in the way that nobles were entitled to deference or in the way that an assault upon the body or the person of a king was regarded as a sacrilege.” The term dignity better captures than most, if not all, other terms the elevated status of the human person.

Do we have any reason for ascribing to all human beings such intrinsic dignity? In an earlier essay, I suggested that there are a number of ways to argue for the proposition that all human beings are endowed with intrinsic dignity and certain inalienable rights. The first is that our dignity should be based on who we are, the kind of being that we are, rather than on how we are functioning in the moment. Dignity should be based on our membership in the human family, rather than on any particular performative activity in which we could engage. Our functioning, whether it be understood in terms of our ability to experience pleasure and pain, or our consciousness, or our intelligence, comes in many degrees. If we think that our value as persons is based on a degreeed characteristic, an accident in terms of Aristotelian metaphysics, then we cannot secure equal basic dignity and equal basic rights for all persons. We should therefore base our fundamental ethical judgments on the substantial identity of who we are rather than on any accidental degreeed quality. Since all human beings are endowed with the same nature, members of the same kind—*homo sapiens*—they all share equally basic rights and dignity.

Privacy is critical to human dignity

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012,

<http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Human Dignity

Autonomy is part of the broader issue of human dignity, that is, the obligation to treat people not merely as means, to be bought and sold and used, but as valuable and worthy of respect in themselves. As the foregoing has made clear, personal information is an extension of the person. To have access to that information is to have access to the person in a particularly intimate way. When some personal information is taken and sold or distributed, especially against the person's will, whether it is a diary or personal letters, a record of buying habits, grades in school, a list of friends and associates or a psychological history, it is as if some part of the person has been alienated and turned into a commodity. In that way the person is treated merely as a thing, a means to be used for some other end.

Mass surveillance denies basic dignity. Privacy is necessary for individuals to be themselves.

Schneier 6 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, 2006 ("The Eternal Value of Privacy," *Wired*, May 18th, Available Online at <http://www.wired.com/news/columns/0,70886-0.html>, Accessed 05-22-2006)

The most common retort against privacy advocates -- by those in favor of ID checks, cameras, databases, data mining and other wholesale surveillance measures -- is this line: "If you aren't doing anything wrong, what do you have to hide?" Some clever answers: "If I'm not doing anything wrong, then you have no cause to watch me." "Because the government gets to define what's wrong, and they keep changing the definition." "Because you might do something wrong with my information." My problem with quips like these -- as right as they are -- is that they accept the premise that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect. Two proverbs say it best: Quis custodiet custodes ipsos? ("Who watches the watchers?") and "Absolute power corrupts absolutely." Cardinal Richelieu understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged." Watch someone long enough, and you'll find something to arrest -- or just blackmail -- with. Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political enemies -- whoever they happen to be at the time. Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance. We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need. A future in which privacy would face constant assault was so alien to the framers of the Constitution that it never occurred to them to call out privacy as an explicit right. Privacy was inherent to the nobility of their being and their cause. Of course being watched in your own home was unreasonable. Watching at all was an act so unseemly as to be inconceivable among

gentlemen in their day. You watched convicted criminals, not free citizens. You ruled your own home. It's intrinsic to the concept of liberty. For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that – either now or in the uncertain future – patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable. How many of us have paused during conversation in the past four-and-a-half years, suddenly aware that we might be eavesdropped on? Probably it was a phone conversation, although maybe it was an e-mail or instant-message exchange or a conversation in a public place. Maybe the topic was terrorism, or politics, or Islam. We stop suddenly, momentarily afraid that our words might be taken out of context, then we laugh at our paranoia and go on. But our demeanor has changed, and our words are subtly altered. This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives. Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide.

Privacy protects human dignity and development

Spiros Simitis, *Reviewing Privacy in an Information Society*, 2003, 135 U. PA. L. REV. 707, 709 , http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review, Simitis is Professor of Civil and Labor Law, Johann Wolfgang Goethe-Universitit, Frankfurt am Main; Data Protection Commissioner, State of Hesse, Federal Republic of Germany.

See, e.g., Judgment of Apr. 2, 1957, 24 Bundesgerichtshof in Zivilsachen [BGHZ] 76 (W. Ger.) (referring to both human dignity and the constitutional right for free development of the individual's personality as the origin of the privacy right); Schacht case, 13 BGHZ 334 (1954) (invoking the constitutional right of respect for human dignity as basis of the privacy right); P. PERLINGIERI, LA PERSONALITA UMANA NELL'ORDINAMENTO GIURIDICO 14 (1972) (The Italian constitution, recognizing that the individual can only develop as a part of the community, places respect for individual human dignity on a par with the life of the community, not subordinate to it.); Bloustein, Group Privacy: The Right to Huddle, 8 RTRR.-CAM. L.J. 219, 278 (1977) ("The right to be let alone protects the integrity and the dignity of the individual."); Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. REV. 962, 1000-07 (1964) (arguing that "all of the tort privacy cases involve the same interest in preserving human dignity and individuality").

Loss of control of information means loss of one's dignity and control over one's life

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Privacy is important for a number of reasons. Some have to do with the consequences of not having privacy. People can be harmed or debilitated if there is no restriction on the public's access to and use of personal information. Other reasons are more fundamental,

touching the essence of human personhood. Reverence for the human person as an end in itself and as an autonomous being requires respect for personal privacy. To lose control of one's personal information is in some measure to lose control of one's life and one's dignity. Therefore, even if privacy is not in itself a fundamental right, it is necessary to protect other fundamental rights.

Identity Development

The breathing room provided by privacy is an end in itself. We can't be "ourselves" without it.

Sadowski 13 — Jathan Sadowski, Doctoral Candidate in Human and Social Dimensions of Science and Technology in the Consortium for Science, Policy and Outcomes at Arizona State University, holds an M.A. in Applied Ethics and the Professions from Arizona State University and a B.S. in Philosophy from the Rochester Institute of Technology, 2013 ("Why Does Privacy Matter? One Scholar's Answer," *The Atlantic*, February 26th, Available Online at <http://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/>, Accessed 04-16-2015)

Even though the practices of many companies such as Facebook are legal, there is something disconcerting about them. Privacy should have a deeper purpose than the one ascribed to it by those who treat it as a currency to be traded for innovation, which in many circumstances seems to actually mean corporate interests. To protect our privacy, we need a better understanding of its purpose and why it is valuable.

That's where Georgetown University law professor Julie E. Cohen comes in. In a forthcoming article for the Harvard Law Review, she lays out a strong argument that addresses the titular concern "What Privacy Is For." Her approach is fresh, and as technology critic Evgeny Morozov rightly tweeted, she wrote "the best paper on privacy theory you'll get to read this year." (He was referring to 2012.)

At bottom, Cohen's argument criticizes the dominant position held by theorists and legislators who treat privacy as just an instrument used to advance some other principle or value, such as liberty, inaccessibility, or control. Framed this way, privacy is relegated to one of many defenses we have from things like another person's prying eyes, or Facebook's recent attempts to ramp up its use of facial-recognition software and collect further data about us without our explicit consent. As long as the principle in question can be protected through some other method, or if privacy gets in the way of a different desirable goal like innovation, it is no longer useful and can be disregarded.

Cohen doesn't think we should treat privacy as a dispensable instrument. To the contrary, she argues privacy is irreducible to a "fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic. Privacy is shorthand for breathing room to engage in the process of ... self-development."

What Cohen means is that since life and contexts are always changing, privacy cannot be reductively conceived as one specific type of thing. It is better understood as an important buffer that gives us space to develop an identity that is somewhat separate from the surveillance, judgment, and values of our society and culture. Privacy is crucial for helping us manage all of these pressures -- pressures that shape the type of person we are -- and for "creating spaces for play and the work of self-[development]." Cohen argues that this self-development allows us to discover what type of society we want and what we should do to get there, both factors that are key to living a fulfilled life.

Woodrow Hartzog and Evan Selinger make similar arguments in a recent article on the value of "obscurity." When structural constraints prevent unwanted parties from getting to your data,

obscurity protections are in play. These protections go beyond preventing companies from exploiting our information for their financial gain. They safeguard democratic societies by furthering "autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power."

In light of these considerations, what's really at stake in a feature like Facebook's rumored location-tracking app? You might think it is a good idea to willfully hand over your data in exchange for personalized coupons or promotions, or to broadcast your location to friends. But consumption -- perusing a store and buying stuff -- and quiet, alone time are both important parts of how we define ourselves. If how we do that becomes subject to ever-present monitoring it can, if even unconsciously, change our behaviors and self-perception.

In this sense, we will be developing an identity that is absent of privacy and subject to surveillance; we must decide if we really want to live in a society that treats every action as a data point to be analyzed and traded like currency. The more we allow for constant tracking, the more difficult it becomes to change the way that technologies are used to encroach on our lives.

Privacy is not just something we enjoy. It is something that is necessary for us to: develop who we are; form an identity that is not dictated by the social conditions that directly or indirectly influence our thinking, decisions, and behaviors; and decide what type of society we want to live in. Whether we like it or not constant data collection about everything we do -- like the kind conducted by Facebook and an increasing number of other companies -- shapes and produces our actions. We are different people when under surveillance than we are when enjoying some privacy. And Cohen's argument illuminates how the breathing room provided by privacy is essential to being a complete, fulfilled person.

Privacy provides an “interior zone” that’s necessary for full and free personal development.

Brooks 15 — David Brooks, Columnist for the *New York Times*, Commentator for PBS *NewsHour*, holds an A.B. in History from the University of Chicago, 2015 (“The Lost Language of Privacy,” *New York Times*, April 14th, Available Online at <http://www.nytimes.com/2015/04/14/opinion/david-brooks-the-lost-language-of-privacy.html>, Accessed 05-15-2015)

Privacy is important to the development of **full individuals** because there has to be **an interior zone** within each person **that other people don't see**. There has to be a zone where half-formed thoughts and delicate emotions can grow and evolve, without being exposed to **the harsh glare of public judgment**. There has to be a place where you can be free to develop ideas and convictions **away from the pressure to conform**. There has to be a spot where you are only yourself and can define yourself. Privacy is important to families and friendships because there has to be a zone where you can be fully known. There has to be a private space where you can share your doubts and secrets and expose your weaknesses with the expectation that you will still be loved and forgiven and supported. Privacy is important for communities because there has to be a space where people with common affiliations can develop bonds of affection and trust. There has to be a boundary between us and them. Within that boundary, you look out for each other; you rally to support each other; you cut each other some slack; you share fierce common loyalties. All **these concentric circles of privacy depend on some level of shrouding**. They

depend on some level of secrecy and awareness of the distinction between the inner privileged space and the outer exposed space. They depend on the understanding that what happens between us stays between us.

Intellectual Freedom

Privacy critical to intellectual freedom and self-expression

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Richards's concept of "intellectual privacy" also recognizes the broader social importance of privacy.⁵⁸ Richards contends that "new ideas often develop best away from the intense scrutiny of public exposure" and that privacy is essential to promoting intellectual freedom.⁵⁹ He also argues that intellectual privacy "should be preserved against private actors as well as against the state" because "[w]e are constrained in our actions by peer pressure at least as much as by the state."⁶⁰

Julie Cohen, Professor, Georgetown University, "What Privacy Is For," HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

While modulation could be undertaken by the government, within systems of informational capitalism it is more typically and effectively undertaken by private actors. Following Manuel Castells, I use "informational capitalism" to refer to the alignment of capitalism as a mode of production with informationalism as a mode of development: "[c]apitalism is oriented toward profit-maximizing, that is, toward increasing the amount of surplus appropriated by capital on the basis of the private control over the means of production and circulation," while "informationalism is oriented . . . toward the accumulation of knowledge and towards higher levels of complexity in information processing."³⁶ In the contemporary information economy, private sector firms like Google, Facebook, and data broker Acxiom use flows of information about consumer behavior to target advertisements, search results, and other content. Advertisers and other client firms rely on the flows of information to construct pricing and risk management templates that maximize their ability to identify high-value consumers and to extract surplus from all consumers. Still other firms rely on flows of information to authenticate access to places (such as workplaces and gaming environments), services (such as banking and telecommunications), and networked information resources (such as software and databases). Information from and about consumers feeds into sophisticated systems of predictive analytics so that surveillant attention can be personalized more precisely and seamlessly. Government is an important secondary beneficiary of informational capitalism, routinely accessing and using flows of behavioral and communications data for its own purposes. The embedding of surveillance functionality within market and political institutions produces "surveillant assemblage[s]," in which information flows in circuits that serve the interests of powerful entities, both private and public.³⁷ In the modulated society, surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power. The surveillant assemblages of informational capitalism do not have as their purpose or effect the "normalized soul training" of the Orwellian nightmare.³⁸ They beckon with seductive appeal. Individual citizenconsumers willingly and actively participate in processes of modulation, seeking the benefits that increased personalization can bring. For

favored consumers, these benefits may include price discounts, enhanced products and services, more convenient access to resources, and heightened social status.³⁹ Within surveillant assemblages, patterns of information flow are accompanied by discourses about why the patterns are natural and beneficial, and those discourses foster widespread internalization of the new norms of information flow.

Privacy is essential to the development of new ideas

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

In practice, of course, few ideas are just thought up by arboreal prodigies (or office-bound academics) working in isolation. Most human inventions are the product of building on the ideas of other people. This is as true of ideas like racial equality or freedom of speech as it is of innovations like the Internet or the iPad. The stuff of our culture—our ideas, our beliefs, our inventions—is invariably the product of a series of small improvements on the ideas of others. Essential to this process is the existence of a large body of work from other people against and upon which we can construct our own ideas. Legal scholar Jessica Litman expresses this point eloquently: Composers recombine sounds they have heard before; playwrights base their characters on bits and pieces drawn from real human beings and other playwrights' characters; novelists draw their plots from lives and other plots within their experience; software writers use the logic they find in other software; lawyers transform old arguments to fit new facts; cinematographers, actors, choreographers, architects, and sculptors all engage in the process of adapting, transforming, and recombining what is already “out there” in some other form. This is not parasitism: it is the essence of authorship. ³ New ideas—political, scientific, artistic, or otherwise—thus depend on access to the ideas of others and the ability to engage with them. And to do this, we need to be able to read freely and then think privately about what we've read in our own time. In the past, access to ideas has come principally from print media—newsstands, bookstores, and libraries, but also from public speeches and performances, television, and radio. However, access to ideas is now increasingly digital—using computers, tablets, and smartphones to access search engines, websites, social networks, and to send texts, emails, and instant messages. Even access to knowledge isn't by itself enough. We need places and spaces (real and virtual) in which to read, to think, to explore. The process of idea generation is one of trial and error. Very often, what seems like a good idea at the time turns out to be a terrible one after testing or further reflection. But to test or examine ideas, we again turn to other people—our friends and confidants, our family and colleagues. We rely on these people for their frank and confidential assessments of whether we're on to something, or whether we're crazy. It's not just new ideas that get tested this way. When we're trying to make up our minds about whether we like government policy, a war, a movie, or even our appearance, we often test novelty with our intimates. We share with our small groups before we are ready to share with the world. We trust them to keep our half-formed notions and beliefs confidential and not to share them with others. At the same time, we also expect that when we are talking to our confidants, third parties are not listening in or recording what we say. These activities and expectations allow us to discuss, test, and reevaluate our ideas before they are ready for public exposure. Intellectual privacy, then, is the protection of all of these individual and social processes, so we may, as Brandeis put it in Whitney, have the “freedom to think as [we] will and to speak as [we] think.” ⁴ If we're interested in the creation of new ideas, we should want people to experiment with controversial

ideas. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 98). Oxford University Press. Kindle Edition.

Surveillance of intellectual activity deters the development of new ideas

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

By the standards of current law, we would probably say that this was a highly speech-protective society. A society with little legal punishment for harmful speech is speech-protective almost by definition. But in such a society, something important is missing, which is intellectual privacy. Intellectual privacy matters because it gives new and possibly heretical ideas room to develop and grow before they are ready for publication. Intellectual privacy gives us the ability to make up our minds about controversial ideas by ourselves or with a few trusted confidants, free from being watched or discovered by others. By contrast, surveillance of intellectual activity deters people from engaging with new ideas and inclines our intellectual explorations to the boring, the bland, and the mainstream. If we know that someone is watching and listening, we will be careful with not just what we say but also what we read and even what we think. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 101). Oxford University Press. Kindle Edition.

Loss of intellectual privacy undermines political freedom

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Intellectual surveillance gives the watcher great power over the watched. Even when what we read or think or say privately might not subject us to imprisonment or liability, the threat of its disclosure could nevertheless cause us to guard our words or thoughts. A watcher can use the threat of disclosure to discredit political opponents. Imagine if there were a public critic of government policy on race relations who was subject to pervasive electronic surveillance. By watching what she read and what she said, the government would not only have an advantage in any debate with this dissident, but it could also use the threat of disclosure of her reading habits to keep her in check. One can imagine such a critic of government policy, if she were aware of surveillance, not only being careful of what she said privately to her confidants but also being careful in what she read and what websites she visited. Without some meaningful guarantee of intellectual privacy, political freedom as we understand it could become impossible.

Intellectual freedom is critical to democracy

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Reasonable societies can certainly disagree about the extent to which government can restrict certain kinds of harmful speech to promote the public good; such a conversation has taken place in the United States and is ongoing in the context of cyber hate speech.¹² But I would maintain that some commitment to intellectual privacy is a necessary requirement for the kinds of democratic freedom that all Western societies aspire to. The aforementioned surveillance example might sound far-fetched, but it is not. For example, concerned that Martin Luther King Jr. was a threat to public order, the FBI listened in to his private telephone conversations in order to seek information with which to blackmail him. As the official government investigation into the King wiretaps concluded in 1976: The FBI collected information about Dr. King's plans and activities through an extensive surveillance program, employing nearly every intelligence-gathering technique at the Bureau's disposal. Wiretaps, which were initially approved by Attorney General Robert F. Kennedy, were maintained on Dr. King's home telephone from October 1963 until mid-1965; the SCLC headquarter's telephones were covered by wiretaps for an even longer period. Phones in the homes and offices of some of Dr. King's close advisers were also wiretapped. The FBI has acknowledged 16 occasions on which microphones were hidden in Dr. King's hotel and motel rooms in an "attempt" to obtain information about the "private activities of King and his advisers" for use to "completely discredit" them. Imagine a dissident like King living in today's information age. Government officials (or political opponents) who wanted him silenced might be able to obtain not just access to his telephone conversations but also his reading habits and emails. Our critic could be blackmailed outright, or he could be discredited by disclosure of the information as an example to others. Perhaps he has not been having an affair but has some other secret. Maybe he is gay, or has a medical condition, or visits embarrassing websites, or has cheated on his expenses or his taxes. All of us have secrets we would prefer not be made public. Surveillance allows those secrets greater opportunities to come out, and it gives the watchers power that can be used nefariously. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (pp. 102-103). Oxford University Press. Kindle Edition.

Moral obligation to protect intellectual freedom – it is the foundation of a free society

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

The commitment to intellectual freedom outlined here is a moral one—that we should protect intellectual freedom and intellectual privacy because they are necessary elements of a good and free society. But my claim about surveillance chilling intellectual experimentation contains a factual assertion as well—that intellectual surveillance deprives people of the privacy they need to make up their minds autonomously. When our intellectual activities are secretly watched, this is an injury to our civil liberties, but my argument that the processes of intellectual experimentation and belief formation are deterred and affected for the worse by surveillance depends upon (1) subjects being watched; (2) the subjects knowing or fearing that they are being watched; and (3) the surveillance causing a disruption in their intellectual activities. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (pp. 105-106). Oxford University Press. Kindle Edition.

Intellectual privacy key to the development of new, subversive ideas

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Keeping out those who would monitor our reading and private communications is essential if we want to generate new ideas, a fact our law has long recognized in subtle and sometimes underappreciated ways. Timothy Macklem has argued that “[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and subversive.”³¹ When there is protection from surveillance, new ideas can be entertained, even when they might be deeply subversive or threatening to conventional beliefs. If we value a pluralistic society or the mental processes that produce new ideas, then some measure of intellectual privacy, some respite from cognitive surveillance, is essential. Any meaningful freedom of speech requires an underlying culture of vibrant intellectual innovation. Intellectual privacy nurtures that innovation, protecting the engine of expression—the imagination of the human mind. To the extent our existing theories of law—First Amendment, Fourth Amendment, or otherwise—are under-protective of intellectual privacy, we must rehabilitate them to take these vital processes into account. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 108). Oxford University Press. Kindle Edition.

Freedom of thought and belief is a core part of our intellectual privacy

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Freedom of thought and belief is the core of our intellectual privacy. This freedom is the defining characteristic of a free society and our most cherished civil liberty. It right encompasses the range of thoughts and beliefs that a person might hold or develop, dealing with matters that are trivial and important, secular and profane. And it protects the individual’s thoughts from scrutiny or coercion by anyone, whether a government official or a private actor such as an employer, a friend, or a spouse. At the level of law, if there is any constitutional right that is absolute, it is this one, which is the precondition for other political and religious rights guaranteed by the Western tradition. Yet curiously, although freedom of thought is widely regarded as our most important civil liberty, it has not been protected in our law as much as other rights, in part because it has been very difficult for the state or others to monitor thoughts and beliefs even if they wanted to. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (pp. 112-113). Oxford University Press. Kindle Edition.

Freedom of thought is essential to human liberty

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

In the nineteenth century, John Stuart Mill developed a broad notion of freedom of thought as an essential element of his theory of human liberty, which comprised “he inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological.”²⁰ In Mill’s view, free thought was inextricably linked to and mutually dependent upon free speech, with the two concepts being a part of a broader idea of political liberty. Moreover, Mill recognized that private parties as well as the state could chill free expression and thought.²¹ Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (p. 113). Oxford University Press. Kindle Edition.

Freedom of thought is the foundation of a free society

Neil Richards, law professor, Washington University, 2015, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Kindle edition, page number at end of card

Modern cases continue to reflect this legacy. The Court has repeatedly declared that the constitutional guarantee of freedom of thought is at the foundation of what it means to have a free society.⁵⁶ In particular, freedom of thought has been invoked as a principal justification for preventing punishment based upon possessing or reading dangerous media. Thus, the government cannot punish a person for merely possessing unpopular or dangerous books or images based upon their content.⁵⁷ As Alexander Meiklejohn put it succinctly, the First Amendment protects, first and foremost, “the thinking process of the community.”⁵⁸ Freedom of thought thus remains, as it has for centuries, the foundation of the Anglo-American tradition of civil liberties. It is the core of intellectual privacy.

Confidential communications are a fundamental civil liberty that are important to our privacy

Neil Richards, law professor, Washington University, 2015, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Kindle edition, page number at end of card

I want to show that confiding, like thinking and reading, is an essential element of intellectual privacy, and I’ll explain why we should continue to protect it in the digital age. In a nutshell, we should protect private communications for the same reason we should protect thinking and reading—they are the ways we make up our minds about the world. As chapter 6 explained, thinking and reading are essential to our intellectual explorations, but sometimes we want to share our half-baked ideas with others before they are ready for public consumption. We make sense of the world in our minds and through our reading habits, but sometimes we also need to confide in trusted intimates—our spouses, partners, friends, priests, and lawyers. Confidential communications are thus a fundamental civil liberty and deserve protection in the digital age, just as they have been protected in the past. Confidentiality doesn’t just protect information; it also protects relationships. It protects the trust we place in each other. Our story of confidentiality and intellectual privacy begins, coincidentally, like our story of tort privacy did, with Louis Brandeis. Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (p. 139). Oxford University Press. Kindle Edition.

Confidentiality critical to intellectual privacy

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Confidentiality matters to intellectual privacy for two very different reasons. The first reason is descriptive. Confidentiality illustrates a very important fact about information: Information is rarely completely public or private, but exists in a middle ground between being truly secret and being known to the world. The second reason is prescriptive. Confidentiality is important because it allows us to generate and develop our beliefs with trusted confidants. It is an important element of intellectual privacy as a guarantee for the civil liberties of freedom of thought and speech.

Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 146). Oxford University Press. Kindle Edition.

Reasons why confidentiality is critical to freedom

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Confidential communications matter because they enable us to share our tentative, half-formed, or possibly heretical ideas with a few trusted confidants before they are ready for public disclosure. But if other people are listening to our telephone calls or reading our paper or electronic mail, we are less likely to share those ideas. We lose the ability to test them out, and our confidants might lose the benefit of our insight. Think for a moment about professional confidences. If we have unusual medical symptoms, we tell a doctor. If we fear legal liability, we might confide in a lawyer. We might share our financial information with an accountant, or our moral doubts or failings with a psychologist, priest, or other counselor. In each case, the promise of some level of confidentiality encourages us to share our information, and it paradoxically encourages us to share more freely, honestly, and completely. When we talk to a doctor about a medical ailment, the doctor needs to know the complete truth, no matter how embarrassing, in order to better treat us. And we want to get the best treatment possible. The presence of the medical duty of confidentiality allows us to share more fully, secure that the knowledge will go no further than our physician. And we get better medical treatment based upon better information. Confidentiality rules reveal not only that information exists in an intermediate state between public and private but also that promises of confidentiality can result in useful (but limited) disclosures of information to our benefit. Let's call this the information-sharing function of confidentiality. If we know our secret will be held in confidence, we're more likely to share it with our confidant. The confidentiality of communications also relies on the information-sharing function of confidentiality. Put simply, we protect the confidentiality of communications to encourage free sharing of ideas and information. In a Wired Magazine article in 200640, security expert Bruce Schneier asked How many of us have paused during conversation in the past four-and-a-half years, suddenly aware that we might be eavesdropped on? Probably it was a phone conversation, although maybe it was an e-mail or instant-message exchange or a conversation in a public place. Maybe the topic was terrorism, or politics, or Islam. We stop suddenly, momentarily afraid that our words might be taken out of context, then we laugh at our paranoia and go on.

But our demeanor has changed, and our words are subtly altered. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 148). Oxford University Press. Kindle Edition.

Confidential communication is essential to intellectual privacy

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Confidential communications are essential to meaningful intellectual privacy. Our confidants are a source of new ideas and information, but without confidentiality they may be reluctant to share subversive or deviant thoughts with us lest others overhear. On the other hand, without the ability to speak with trusted confidants, we lack the capacity to develop our own ideas in collaboration with others before we are ready to share them publicly. 46 Consultation with intimates allows us to better determine if an idea is a good one, and to gauge some expectation of how it will be received if we finally decide to share or publish it. Without a meaningful expectation of confidentiality, then, we would have fewer ideas, and those that we did have might be unlikely to be shared. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 149). Oxford University Press. Kindle Edition.

Relationships

Privacy is critical to relationships

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Privacy and Relationship

Privacy is also needed in the ordinary conduct of human affairs, to facilitate social interchange. James Rachels, for example, argues that privacy is an essential prerequisite for forming relationships.³ The degree of intimacy in a relationship is determined in part by how much personal information is revealed. One reveals things to a friend that one would not disclose to a casual acquaintance. What one tells one's spouse is quite different from what one would discuss with one's employer. This is true of more functional relationships as well. People tell things to their doctors or therapists that they do not want anyone else to know, for example. These privileged relationships, whether personal or functional, require a special level of openness and trust that is only possible if there is an assurance that what is revealed will be kept private. As Rachel's points out, a husband and wife will behave differently in the presence of a third party than when they are alone.⁴ If they were always under observation, they could not enjoy the degree of intimacy that a marriage should have. Charles Fried puts it more broadly. Privacy, he writes, is "necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust... without privacy they are simply inconceivable."⁵

Corporate Surveillance Undermines Democracy

Corporate surveillance undermines democracy by modulating the population in a way that undermines civic engagement

Julie Cohen, Professor, Georgetown University, “What Privacy Is For,” HARVARD LAW REVIEW, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

For all of these reasons, a critique of surveillance as privacy invasion “does not do justice to the productive character of consumer surveillance.”⁴⁰ Modulation is a mode of privacy invasion, but it is also a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories. Yet to speak of networked processes of surveillance and modulation in the industrial era vernacular, as systems for “manufacturing consent,” would be too crude.⁴¹ Rather, in a much more subtle process of continual feedback, stimuli are tailored to play to existing inclinations, nudging them in directions that align with profit-maximizing goals.⁴² So too with political inclinations; particularly as search and social networking become more seamlessly integrated, networked citizen-consumers move within personalized “filter bubbles” that conform the information environment to their political and ideological commitments.⁴³ This is conducive to identifying and targeting particular political constituencies,⁴⁴ but not necessarily to fostering political dialogue among diverse constituencies in ways that might enable them to find common ground. By these increasingly ordinary processes, both public and private regimes of surveillance and modulation diminish the capacity for democratic self-government

Totalitarianism/Loss of Democracy

Loss of privacy and complete control of big data means totalitarian social control

Simon Denyer, October 22, 2016, Washington Post, China's plan to organize its society relies on "big data" to regulate everyone, https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html?tid=pm_world_pop_b

Imagine a world where an authoritarian government monitors everything you do, amasses huge amounts of data on almost every interaction you make, and awards you a single score that measures how “trustworthy” you are. In this world, anything from defaulting on a loan to criticizing the ruling party, from running a red light to failing to care for your parents properly, could cause you to lose points. And in this world, **your score becomes the ultimate truth of who you are — determining whether you can borrow money, get your children into the best schools or travel abroad; whether you get a room in a fancy hotel, a seat in a top restaurant — or even just get a date.** This is not the dystopian superstate of Steven Spielberg's "Minority Report," in which all-knowing police stop crime before it happens. But **it could be China by 2020. It is the scenario contained in China's ambitious plans to develop a far-reaching social credit system, a plan that the Communist Party hopes will build a culture of “sincerity” and a “harmonious socialist society** where "keeping trust is glorious." A high-level policy document released in September listed the sanctions that could be imposed on any person or company deemed to have fallen short. The overriding principle: "If trust is broken in one place, restrictions are imposed everywhere." **A whole range of privileges would be denied, while people and companies breaking social trust would also be subject to expanded daily supervision and random inspections.** The ambition is to collect every scrap of information available online about China's companies and citizens in a single place — and then assign each of them a score based on their political, commercial, social and legal "credit." The government hasn't announced exactly how the plan will work — for example, how scores will be compiled and different qualities weighted against one another. But the idea is that good behavior will be rewarded and bad behavior punished, with the Communist Party acting as the ultimate judge. **This is what China calls “Internet Plus,” but critics call a 21st-century police state.** A version of Big Brother? Harnessing the power of big data and the ubiquity of smartphones, e-commerce and social media in a society where 700 million people live large parts of their lives online, **the plan will also vacuum up court, police, banking, tax and employment records.** Doctors, teachers, local governments and businesses could additionally be scored by citizens for their professionalism and probity. **“China is moving towards a totalitarian society, where the government controls and affects individuals’ private lives,”** said Beijing-based novelist and social commentator Murong Xuecun. "This is like Big Brother, who has all your information and can harm you in any way he wants." At the heart of the social credit system is an attempt to control China's vast, anarchic and poorly regulated market economy, to punish companies selling poisoned food or phony medicine, to expose doctors taking bribes and uncover con men

preying on the vulnerable. “Fraud has become ever more common in society,” Lian Weiliang, vice chairman of the National Development and Reform Commission, the country’s main economic planning agency, said in April. “Swindlers have to pay a price.” Yet in Communist China, the plans inevitably take on an authoritarian aspect: This is not just about regulating the economy, but also about creating a new socialist utopia under the Communist Party’s benevolent guidance. “A huge part of Chinese political theater is to claim that there is an idealized future, a utopia to head towards,” said Rogier Creemers, a professor of law and governance at Leiden University in the Netherlands. “Now after half a century of Leninism, and with technological developments that allow for the vast collection and processing of information, there is much less distance between the loftiness of the party’s ambition and its hypothetical capability of actually doing something,” he said. But the narrowing of that distance raises expectations, says Creemers, who adds that the party could be biting off more than it can chew. Assigning all of China’s people a social credit rating that weighs up and scores every aspect of their behavior would not only be a gigantic technological challenge but also thoroughly subjective — and could be extremely unpopular. “From a technological feasibility question to a political feasibility question, to actually get to a score, to roll this out across a population of 1.3 billion, that would be a huge challenge,” Creemers said. A target for hackers The Communist Party may be obsessed with control, but it is also sensitive to public opinion, and authorities were forced to backtrack after a pilot project in southern China in 2010 provoked a backlash. That project, launched in Jiangsu province’s Suining County in 2010, gave citizens points for good behavior, up to a maximum of 1,000. But a minor violation of traffic rules would cost someone 20 points, and running a red light, driving while drunk or paying a bribe would cost 50. Some of the penalties showed the party’s desire to regulate its citizens’ private lives — participating in anything deemed to be a cult or failing to care for elderly relatives incurred a 50-point penalty. Other penalties reflected the party’s obsession with maintaining public order and crushing any challenge to its authority — causing a “disturbance” that blocks party or government offices meant 50 points off; using the Internet to falsely accuse others resulted in a 100-point deduction. Winning a “national honor” — such as being classified as a model citizen or worker — added 100 points to someone’s score. On this basis, citizens were classified into four levels: Those given an “A” grade qualified for government support when starting a business and preferential treatment when applying to join the party, government or army; or applying for a promotion. People with “D” grades were excluded from official support or employment. The project provoked comparisons with the “good citizen cards” introduced by Japan’s occupying army in China in the 1930s. On social media, residents protested that this was “society turned upside down,” and it was citizens who should be grading government officials “and not the other way around.” The Suining government later told state media that it had revised the project, still recording social credit scores but abandoning the A-to-D classifications. Officials declined to be interviewed for this article. Despite the outcry in Suining, the central government seems determined to press ahead with its plans. Part of the reason is economic. With few people in China owning credit cards or borrowing money from banks, credit information is scarce. There is no national equivalent of the FICO score widely used in the United States to evaluate consumer credit risks. At the same time, the central government aims to police the sort of corporate malfeasance that saw tens of thousands of babies hospitalized

after consuming adulterated milk and infant formula in 2008, and millions of children given compromised vaccines this year. Yet it is also an attempt to use the data to enforce a moral authority as designed by the Communist Party. The Cyberspace Administration of China wants anyone demonstrating “dishonest” online behavior blacklisted, while a leading academic has argued that a media blacklist of “irresponsible reporting” would encourage greater self-discipline and morality in journalism. Lester Ross, partner-in-charge of the Beijing office of law firm WilmerHale, says the rules are designed to stop anyone “stepping out of line” and could intimidate lawyers seeking to put forward an aggressive defense of their clients. He sees echoes of the Cultural Revolution, in which Mao Zedong identified “five black categories” of people considered enemies of the revolution, including landlords, rich farmers and rightists, who were singled out for struggle sessions, persecution and re-education. Under the social credit plan, the punishments are less severe — prohibitions on riding in “soft sleeper” class on trains or going first class in planes, for example, or on staying at the finer hotels, traveling abroad or sending children to the best schools — but nonetheless far-reaching. Xuecun’s criticism of the government won him millions of followers on Weibo, China’s equivalent of Twitter, until the censors swung into action. He fears the new social credit plan could bring more problems for those who dare to speak out. “My social-media account has been canceled many times, so the government can say I am a dishonest person,” he said. “Then I can’t go abroad and can’t take the train.” **Under government-approved pilot projects, eight private companies have set up credit databases that compile a wide range of online, financial and legal information.** One of the most popular is Sesame Credit, part of the giant Alibaba e-commerce company that runs the world’s largest online shopping platform. Tens of millions of users with high scores have been able to rent cars and bicycles without leaving deposits, company officials say, and can avoid long lines at hospitals by paying fees after leaving with a few taps on a smartphone. The Baihe online dating site encourages users to display their Sesame Credit scores to attract potential partners; 15 percent of its users do so. One woman, who works in advertising but declined to be named to protect her privacy, said she had used Baihe for more than two years. Looking for people who display good Sesame Credit scores helps her weed out scammers, she said. “First I will look at his photo, then I will look at his profile,” she said. “He has to use real-name authentication. But I will trust him and talk to him if he has Sesame Credit.” But it is far from clear that the system will be safe from scams. William Glass, a threat intelligence analyst at cybersecurity expert FireEye, says a centralized system would be both vulnerable and immensely attractive to hackers. “There is a big market for this stuff, and as soon as this system sets up, there is great incentive for cybercriminals and even state-backed actors to go in, whether to steal information or even to alter it,” he said. “This system will be the ground truth of who you are. But considering that all this information is stored digitally, it is certainly not immutable, and people can potentially go in and change it.

Failure to protect privacy undermines the civic value of the Internet

Paul M. Schwartz, law professor, 1999, Brooklyn, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613, <http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf>

Yet, information technology in cyberspace also affects privacy in ways that are dramatically different from anything previously possible.⁴ By generating comprehensive records of online behavior, information technology can broadcast an individual's secrets in ways that she can neither anticipate nor control.⁵ Once linked to the Inter- net, the computer on our desk becomes a potential recorder and betrayer of our confidences. In the absence of strong privacy rules, cyberspace's civic potential will never be attained..... At present, however, no successful standards, legal or other- wise, exist for limiting the collection and utilization of personal data in cyberspace.⁶ The lack of appropriate and enforceable privacy norms poses a significant threat to democracy in the emerging Information Age. Indeed, information privacy concerns are the leading reason why individuals not on the Internet are choosing to stay off.⁷ The stakes are enormous; the norms that we develop for per- sonal data use on the Internet will play an essential role in shaping democracy in the Information Age. Nevertheless, the Clinton Administration and legal commentators increasingly view the role of the Internet law of privacy as facilitating wealth-creating transmis- sions of information, including those of personal data.⁸ This Article takes a different tack. It does not oppose a commercial function for cyberspace, but calls for something other than shopping on the Inter- net. Moreover, it argues that unfettered participation in democratic and other fora in cyberspace will not take place without the right kinds of legal limits on access to personal information.⁹

People won't participate online in ways that improve the civic without privacy protections

Paul M. Schwartz, law professor, 1999, Brooklyn, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613, <http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf>

This line of inquiry culminates in the development of a theory of constitutive privacy.¹⁴ Development of this theory involves an ex- ploration of the inadequacies of the traditional liberal understanding of information privacy, which views privacy as a right to control the use

of one's personal data.¹⁵ Building on the important scholarship of Robert Post, the Article then argues that information privacy is best conceived of as a constitutive element of civil society.¹⁶ The Internet's potential to improve shared life in the United States will be squandered unless we structure the kinds of information use necessary for democratic community and individual self-governance.¹⁷ Participants in cyberspace need access to public, quasi-public and private “spaces” where they can engage in civic dialogue and the process of individual self-definition. Creation of such spaces requires the development of privacy norms that fulfill a constitutive function; these rules must draw on adequately complex coordinates to structure the personal data use of different entities.

Privacy violations discourage democratic participation

Paul M. Schwartz, law professor, 1999, Brooklyn, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613, <http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf>

The absence of privacy on the Internet reflects a deeper current, namely the establishment of the managerial data processing model in cyberspace. This Part examines the implications of this development by contrasting the Internet's potential as the new realm of shared life with the consequences of this social arrangement of hierarchical control. The utilization of information technology in cyberspace will act as a powerful negative force in two ways. First, as currently configured, it will discourage unfettered participation in deliberative democracy in the United States.²³⁶ Second, the current use of information technology on the Internet can harm an individual's capacity for self-governance.²³⁷ These two negative effects are significant because our nation's political order is based both on democratic deliberation and on individuals who are capable of forming and acting on their notions of the good.

As this précis makes clear, this Article's Part II is both anchored in and seeks to develop civic republican theory. At first glance, this perspective may appear unusual for scholarship concerned with

information privacy. After all, civic republicanism is a political philosophy that generally is more concerned with obligations than with rights, more interested in community than individuals.²³⁸ Moreover, to the extent that civic republican theorists talk at all about privacy, they have been less concerned with information privacy, dismissed by Michael Sandel as the “old privacy,” than with the freedom to engage in certain activities free of governmental restrictions.²³⁹ This Article will, nevertheless, demonstrate the promise of republican thought for invigorating the debate about information privacy.

Online privacy violations undermine the self-reflection, autonomy, and self-determination that is needed to develop a strong civic Republican society

Paul M. Schwartz, law professor, 1999, Brooklyn, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613, <http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf>

Civic republicanism must undergird its existing concept of democratic deliberation with a foundation based on an individual’s capacity for critical reflection. Outside of this movement, an important corrective attempt is already underway. James E. Fleming has argued, for example, that democracy in general and constitutional law in particular must secure the preconditions for “citizens to apply their capacity for a conception of the good to deliberat[ions] about . . . how to live their own lives.”²⁸⁰ His call is for a deliberative autonomy that is the locus of moral agency, responsibility, and independence.²⁸¹ This quality involves both decisionmaking internal to the individual and a person’s consulting with others, taking their views into account, and associating with them.²⁸²

From this perspective, democracy requires more than group deliberation at a town square located either in Real Space or in cyberspace. It requires individuals with an underlying capacity to form and act on their notions of the good in deciding how to live their lives. This anti-totalitarian principle stands as a bulwark against any coercive standardization of the individual.²⁸³ Yet, a considerable difficulty arises in identifying the kinds of government or group behavior that raises a

threat to personal self-governance. Part of the problem is that autonomy is a notoriously slippery concept.²⁸⁴ Even more to the point, however, communal life requires something beyond isolated decisionmaking—self-governance takes place in individuals who are not located on discrete behavioral islands, but are tied to others and necessarily open to influence through outside persuasion.²⁸⁵

Social life's give-and-take is not merely compatible with individual autonomy, but an essential factor in it because life is lived among others. Prior and ongoing commitments make a difference in the choices we make and in the hierarchy of our goals.²⁸⁶ As a result, we must comprehend autonomous people as being only partially the authors of their lives. As Joseph Raz has proposed, “[t]he ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives.”²⁸⁷ Individuals who exercise self-determination, therefore, should be defined as people who, as part authors of their lives, substantially shape their existence through the choices they make.

Self-determination is a capacity that is embodied and developed through social forms and practices. The threat to this quality arises when private or government action interferes with a person's control of her reasoning process. To understand the harm of this manipulation, consider David Strauss's examination of different kinds of manipulation in the speech context.²⁸⁸ In that setting, coercion occurs when one compels another to pursue the speaker's objectives instead of the victim's own objectives.²⁸⁹ Such coercion can take place through simple use of physical force or through inducements that interject false facts into the thought processes of the listeners.²⁹⁰ Drawing on Strauss's work, we can state that a coercive influence on decisionmaking is that which takes over, or colonizes, a person's thinking processes.²⁹¹

Having developed the idea of individual self-determination and identified the nature of coercion upon it, once again this Article will inquire into the dangers raised by the lack of cyberspace privacy. As we have seen, physical coercion or false statements of fact corrupt decisionmaking by commanding the listener's mind to produce an

outcome that the speaker desires. Autonomy manipulation on the Internet reaches a similar result in a different fashion. Its perfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking.

George Orwell carried out the classic analysis of how surveillance can exert this negative pressure. In the novel *1984*, first published in 1949, Orwell imagined a machine called the "telescreen."²⁹² This omnipresent device broadcasted propaganda on a nonstop basis and allowed the state officials, the "Thought Police," to observe the populace.²⁹³ Computers on the Internet are reminiscent of the telescreen; under current conditions, it is impossible to know if and when the cyber-Thought Police are plugged in on any individual wire. To extend Orwell's thought, one can say that as habit becomes instinct and people on the Internet gain a sense that their every mouse click and key stroke might be observed, the necessary insulation for individual self-determination will vanish.²⁹⁴

Excessive privacy violations – complete information release – undermines democracy

Spiros Simitis, *Reviewing Privacy in an Information Society*, 2003, 135 U. PA. L. REV. 707, 709, http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review; Simitis is Professor of Civil and Labor Law, Johann Wolfgang Goethe-Universität, Frankfurt am Main; Data Protection Commissioner, State of Hesse, Federal Republic of Germany.

The price for an undoubtedly improvement in transparency is a no less evident loss in competence of communication. Habits, activities, and preferences are compiled, registered, and retrieved to facilitate better adjustment, not to improve the individual's capacity to act and to decide. Whatever the original incentive for computerization may have been, processing increasingly appears as the ideal means to adapt an individual to a predetermined, standardized behavior that aims at the highest possible degree of compliance with the model patient, consumer, taxpayer, employee, or citizen. Furthermore, interactive systems do not, despite all contrary assertions,¹⁴ restore a long lost individuality by correcting the effects of mass production in a mass society. On the contrary, the telematic integration forces the individual once more into a preset scheme. The media supplier dictates the conditions under which communication takes place, fixes the possible subjects of the dialogue, and, due to the personal data collected, is in an increasingly better position to influence the subscriber's behavior. Interactive systems, therefore, suggest individual activity where in fact no more than stereotyped reactions occur.⁵ In short, the transparency achieved through automated processing creates possibly the best conditions for colonization of the individual's lifeworld.¹¹ Accurate, constantly updated knowledge of her personal history is systematically incorporated into policies

that deliberately structure her behavior. The more routinized automated processing augments the transparency, however, the more privacy proves to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade.

Significant privacy intrusion means no exercise of freedom of speech, freedom of association, or freedom of assembly

Spiros Simitis, *Reviewing Privacy in an Information Society*, 2003, 135 U. PA. L. REV. 707, 709 , http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review, Simitis is Professor of Civil and Labor Law, Johann Wolfgang Goethe-Universitit, Frankfurt am Main; Data Protection Commissioner, State of Hesse, Federal Republic of Germany.

creates possibly the best conditions for colonization of the individual's lifeworld.¹¹ Accurate, constantly updated knowledge of her personal history is systematically incorporated into policies that deliberately structure her behavior. The more In short, the transparency achieved through automated processing routinized automated processing augments the transparency, however, the more privacy proves to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade. For precisely this reason the West German Federal Constitutional Court, in the National Census Case ("Volkszählungsurteil")-its landmark decision on the census law-spoke of the individual's right to an "informational self-determination".¹¹ According to the court, unrestricted access to personal data imperils virtually every constitutionally guaranteed right. Neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed. In view of these implications of automated data processing, considerations of privacy protection involve more than any one particular right: they determine the choice between a democratic and an authoritarian society."¹¹

Manipulation and control threatens democracy

Spiros Simitis, *Reviewing Privacy in an Information Society*, 2003, 135 U. PA. L. REV. 707, 709 , http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review, Simitis is Professor of Civil and Labor Law, Johann Wolfgang Goethe-Universitit, Frankfurt am Main; Data Protection Commissioner, State of Hesse, Federal Republic of Germany.

The processing of personal data is not unique to a particular society. On the contrary, the attractiveness of information technology transcends political boundaries, particularly because of the opportunity to guide the individual's behavior. For a democratic society, however, the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy.

Privacy is needed to protect individuals from government power

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Privacy is even more necessary as a safeguard of freedom in the relationships between individuals and groups. As Alan Westin has pointed out, surveillance and publicity are powerful instruments of social control.⁸ If individuals know that their actions and dispositions are constantly being observed, commented on and criticized, they find it much harder to do anything that deviates from accepted social behavior. There does not even have to be an explicit threat of retaliation. "Visibility itself provides a powerful method of enforcing norms."⁹ Most people are afraid to stand apart, to be different, if it means being subject to piercing scrutiny. The "deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."¹⁰ Under these circumstances they find it better simply to conform. This is the situation characterized in George Orwell's 1984 where the pervasive surveillance of "Big Brother" was enough to keep most citizens under rigid control.¹¹

Therefore privacy, as protection from excessive scrutiny, is necessary if individuals are to be free to be themselves. Everyone needs some room to break social norms, to engage in small "permissible deviations" that help define a person's individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves. As Brian Stelter wrote in the New York Times on the loss of anonymity in today's online world, "The collective intelligence of the Internet's two billion users, and the digital fingerprints that so many users leave on Web sites, combine to make it more and more likely that every embarrassing video, every intimate photo, and every indelicate e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view."¹²

This ability to develop one's unique individuality is especially important in a democracy, which values and depends on creativity, nonconformism and the free interchange of diverse ideas. That is where a democracy gets its vitality. Thus, as Westin has observed, "Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life."¹³

When Brandeis and Warren wrote their seminal article on privacy over one hundred years ago, their primary concern was with the social pressure caused by excessive exposure to

public scrutiny of the private affairs of individuals. The problem for them was the popular press, which represented the "monolithic, impersonal and value-free forces of modern society,"¹⁴ undermining the traditional values of rural society, which had been nurtured and protected by local institutions such as family, church and other associations. The exposure of the affairs of the well-bred to the curiosity of the masses, Brandeis and Warren feared, had a leveling effect which undermined what was noble and virtuous in society, replacing it with the base and the trivial.

Even apparently harmless gossip, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.... Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.¹⁵

For Brandeis and Warren, privacy was a means of protecting the freedom of the virtuous to maintain their values against the corrupting influence of the mass media that catered to people's basest instincts.

Although the degrading effect of the mass media is still a problem, today a more serious threat to freedom comes from governments and other large institutions. Over the last century, governments have developed sophisticated methods of surveillance as a means of controlling their subjects. This is especially true of totalitarian states, as the passage from Westin quoted above indicates. The Soviet Union, Communist China, Nazi Germany, Fascist Italy and white-run South Africa all used covert and overt observation, interrogation, eavesdropping, reporting by neighbors and other means of data collection to convince their subjects that independent, "antisocial" thought, speech and behavior was unacceptable. In many cases the mere presence of the surveillance was enough to keep people in line. Where it was not, the data collected was used to identify, round up and punish elements of the population that were deemed dangerous. For example, Ignazio Silone, in his book Bread and Wine, described the use of surveillance in Fascist Italy in this way:

It is well-known [says Minorca] that the police have their informers in every section of every big factory, in every bank, in every big office. In every block of flats the porter is, by law, a stool pigeon for the police.... This state of affairs spreads suspicion and distrust throughout all classes of the population. On this degradation of man into a frightened animal, who quivers with fear and hates his neighbor in his fear, and watches him, betrays him, sells him, and then lives in fear of discovery, the dictatorship is based. The real organization on which the system in this country is based is the secret manipulation of fear.¹⁶

While totalitarian regimes may not seem as powerful or as sinister as they did 50 years ago, surveillance is still used in many places as an instrument of oppression. For example

Philip Zimmerman, the author of the PGP (Pretty Good Privacy) data encryption program, reports receiving a letter from a human rights activist in the former Yugoslavia that contained the following testimonial:

We are part of a network of not-for-profit agencies, working among other things for human rights in the Balkans. Our various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and our office in Romania has a constant wiretap. Last year in Zagreb, the security police raided our office and confiscated our computers in the hope of retrieving information about the identity of people who had complained about their activities. Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients.¹⁷

More recently social media and the Internet played major roles in the "Arab Spring" uprisings in the Middle East, causing Egypt and Libya to shut down the Internet in their countries in an attempt to stifle dissent.¹⁸ In China there has been an ongoing battle between the government and activist groups over government monitoring and censorship of the Internet.¹⁹

Even in a democracy, there is always the danger that surveillance can be used as a means of control. In the United States, for example, where freedom is such an important part of the national ethos, the FBI, the CIA, the National Security Agency (NSA) and the armed forces have frequently kept dossiers on dissidents. The NSA from 1952 to 1974 kept files on about 75,000 Americans, including civil rights and antiwar activists, and even members of Congress. During the Vietnam war, the CIA's Operation Chaos collected data on over 300,000 Americans.²⁰ Since then the NSA has had an ongoing program to monitor electronic communications, both in the U.S. and abroad, which has led to constant battles with individuals and groups who have sought to protect the privacy of those communications through encryption and other technologies.²¹

Some of the most famous incidents of surveillance of dissidents, of course, occurred during the Nixon administration in the early 1970s. For example, when Daniel Ellsberg was suspected of leaking the Pentagon Papers, an internal critique of government conduct of the Vietnam war, Nixon's agents broke into the office of Ellsberg's psychiatrist and stole his records.²² And it was a bungled attempt at surveillance of Nixon's political opposition, as well as illegal use of tax returns from the IRS, that ultimately brought down the Nixon administration.²³ More recently, during the 1996 presidential campaign, it was revealed that the Clinton White House had access to the FBI investigative records of over 300 Republicans who had served in the Reagan and Bush administrations. The Clinton administration claimed it was all a mistake caused by using an out-of-date list of White House staff, while the challenger Bob Dole accused them of compiling an "enemies list." >sup>24 Whatever the motivation, the head of the FBI termed the use of the files "egregious violations of privacy."²⁵

Since the 9/11 terrorist attacks in 2001, there has been even greater urgency in the government's efforts to monitor the activities and communications of people, both

foreigners and its own citizens, in order to identify and prevent terrorist threats. The Patriot Act, passed less than two months after 9/11, greatly expanded the government's authority to intercept electronic communications, such as emails and phone calls, including those of U.S. citizens. As a result government agencies have been building the technological and organizational capabilities to monitor the activities and communications of their own citizens. For example, Wired magazine revealed in a recent report how the National Security Agency

has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created. In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it's all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever.²⁶

The FBI, the Drug Enforcement Agency and the Department of Homeland Security also have many programs to monitor citizens in general, not just those who are under suspicion. These efforts include sifting through media references,²⁷ tracking chatter on social networks,²⁸ and monitoring peoples' movements through license plate scanners²⁹ and video cameras.³⁰

The mere knowledge that American citizens could be the subjects of surveillance can in itself have a chilling effect on political freedom. "Now it is much more difficult than it once was to dismiss the possibility that one's phone is being tapped, or that one's tax returns may be used for unfriendly political purposes, or that one's life has become the subject of a CIA file. The realization that these activities might take place, whether they really do or not in any particular instance, has potentially destructive effects on the openness of social systems to innovation and dissent."³¹

At times the government in the United States has gone beyond surveillance and intimidation and has used the data gathered as a basis for overt oppression. One of the most blatant examples is the internment of over 100,000 Japanese Americans, most of them American citizens, during World War II. The Justice Department used data from the Census Bureau to identify residential areas where there were large concentrations of Japanese Americans, and the army was sent in to round them up. They were taken away from their homes and held in concentration camps for the duration of the war.³²

Governments do need information, including personal information, to govern effectively and to protect the security of their citizens. But citizens also need protection from the overzealous or malicious use of that information, especially by governments that, in this age, have enormous bureaucratic and technological power to gather and use the information.

Privacy protects autonomy, self-fulfillment, and socialization needed for democracy

Jathan Sadowski, journalist, Why Does Privacy Matter? One Scholar's Answer, *The Atlantic*, February 26, 2013, www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/

Woodrow Hartzog and Evan Selinger make similar arguments in a recent article on the value of "obscurity." When structural constraints prevent unwanted parties from getting to your data, obscurity protections are in play. These protections go beyond preventing companies from exploiting our information for their financial gain. They safeguard democratic societies by furthering "autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power."

Privacy is needed to check the power of the government

Steven G. Gey, John W. and Ashley E. Frost Professor of Law, Florida State University College of Law, "The Case Against Postmodern Censorship," *UNIVERSITY OF PENNSYLVANIA LAW REVIEW*, "v. 145 n. 2, 12—96, pp. 193-297

The concept of privacy reflects the recognition that even a responsive democratic government often will have institutional interests, values and objectives that are quite distinct from those of individual citizens. Many of these conflicting governmental and individual interests will relate to the most fundamental personal and social values. When the reality of fundamentally conflicting interests is combined with the seductive possibilities presented to the government by its monopoly on the authorized use of absolute power-jails, guns, electric chairs-the prospect always exists that the government will attempt to use its power to settle matters of fundamental value once and for all in favor of its own preferred way of perceiving and organizing the world. At that point, the public/ private dichotomy would be eliminated, but then again so would the possibility of democratic self-governance. Since every citizen would merely reflect the government's own preferred brand of political and social reality, it would no longer be possible to claim that the citizens are deciding anything, except in the farcical Soviet sense of unanimous citizen certification of a foregone political conclusion. The central flaw in the feminist and critical race critiques of the public/private distinction is that these critiques cannot be reconciled with democracy's basic need for some separation between the governors and the governed. Without that separation, democracy cannot exist because there is no group capable of providing popular consent to the government's exercise of power. Likewise, if the government is permitted to break down barriers of privacy and exert direct control over the thoughts and attitudes of the public on matters of great political importance, it will no longer be possible for the public to reject one government and replace it with another government representing a radically different ideological stance. Without this possibility of ideological change, it is difficult to see how such a government could be accurately described as democratic.

Privacy essential for self-actualization needed to support democracy

Julie Cohen, Professor, Georgetown University, "What Privacy Is For," *HARVARD LAW REVIEW*, 2013, <http://harvardlawreview.org/2013/05/what-privacy-is-for/>

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing. It is useful to begin by considering the relationship between citizenship and political and economic institutions. That institutions shape opportunities for the exercise of citizenship is, I think, an unremarkable proposition. Citizenship is more than a status. It is also a set of practices — voting, public debate, and so on — and so the scope for the practice of citizenship will be defined in part by the practices that existing institutions encourage, permit, or foreclose. Less often acknowledged is that institutions configure citizens, inculcating habits of mind and behavior that lend themselves more readily to certain types of practices than to others. Institutions shape not only the scope but also the capacity for citizenship. One of the lessons of American experiments in democracy building, beginning in the 1980s in the former Soviet Union and continuing most recently in Afghanistan and Iraq, is that democracy is difficult to jumpstart. Well-functioning state and market institutions cannot be built in the span of a grant-funded research project or a military campaign. Their rhythms and norms must be learned and then internalized, bringing into being the habits of mind and behavior that democratic citizenship requires.

Social Structure

Without privacy, people will feel compelled to live up to certain schizophrenic norms, making it impossible to function

Robert Post, law professor, Yale, 1989, The Social Foundations of Privacy: Community and the Self in Common Law Tort,
http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers

A "neutral" concept of privacy has certain obvious advantages and uses. It is useful, for example, in the cross-cultural analysis of privacy, because it creates an object of analysis that is independent of the various perceptions of the cultures at issue. It is also useful for efforts to create a functional account of privacy. The hypothesis that "privacy" is necessary to cause certain consequences will be cleaner and more easily verifiable if the "privacy" at issue is conceived as a measurable fact. Thus Robert Merton rests his claim that privacy "is an important functional requirement for the effective operation of social structure" on the neutral definition of privacy as "insulation from observability."⁶ Privacy is necessary, argues Merton, because without it "the pressure to live up to the details of all (and often conflicting) social norms would become literally unbearable; in a complex society, schizophrenic behavior would become the rule rather than the formidable exception it already is."⁶⁵

Privacy protects civility and autonomy

Robert Post, law professor, Yale, 1989, The Social Foundations of Privacy: Community and the Self in Common Law Tort,
http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers

I hope I have made good on my initial claim that the common law tort of invasion of privacy reflects a complex and fascinating apprehension of the social texture of contemporary society. The tort safeguards the interests of individuals in the maintenance of rules of civility. These rules enable individuals to receive and to express respect, and to that extent are constitutive of human dignity. In the case of intrusion, these rules also enable individuals to receive and to express intimacy, and to

that extent are constitutive of human autonomy. In the case of both intrusion and public disclosure, the civility rules maintained by the tort embody the obligations owed by members of a community to each other, and to that extent define the substance and boundaries of community life.

Employment

Release of personal information can damage long-term employment prospects

Michael McFarland, S.J., a computer scientist with extensive liberal arts teaching experience and former 31st president of the College of the Holy Cross, Why We Care about Privacy, June 2012, <http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html>

Similarly someone with an arrest record, even where there is no conviction and the person is in fact innocent, can suffer severe harassment and discrimination. A number of studies have shown that employers are far less likely to hire someone with an arrest record, even when the charges have been dropped or the person has been acquitted.²

Human Rights

Data privacy is a human right

Erin Corken, 2015, Northern Kentucky Law Review, THE CHANGING EXPECTATION OF PRIVACY: KEEPING UP WITH THE MILLENNIAL GENERATION AND LOOKING TOWARD THE FUTURE, v. 42, p. 305-6

When we talk about privacy, the first thing we must do is distinguish between the right to privacy in general and data privacy. The right to privacy in general is a fundamental human right.¹⁵⁴ Data privacy is derived from this fundamental right. As noted above, the first scholarly works that led to modern data privacy law in the United States appeared almost fifty years ago with Westin's seminal works.¹⁵⁵ The first significant scholarly work regarding the right to privacy in general is usually credited as occurring much earlier with Samuel Warren's and Louis Brandeis' 1890 Harvard Law Review article, *The Right to Privacy*.¹⁵⁶ In *The Right to Privacy*, Warren and Brandeis discuss how the common law at the time had already begun to recognize that privacy was something that required due protection.¹⁵⁷ They quote Judge Cooley from his 1878 publication, *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, describing it as "the right to be let alone."¹⁵⁸

Privacy is recognized as a human right in many international treaties

Erin Corken, 2015, Northern Kentucky Law Review, THE CHANGING EXPECTATION OF PRIVACY: KEEPING UP WITH THE MILLENNIAL GENERATION AND LOOKING TOWARD THE FUTURE, v. 42, p. 308

Internationally, the existence of the right to privacy has been much less controversial. The United Nations Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and many other international and regional treaties all expressly recognize the right to privacy as a fundamental human right.¹⁷⁹ Article 12 of the 1948 Universal Declaration of Human Rights, specifically states, "[n]o one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."¹⁸⁰

IoT developments are threatening

Erin Corken, 2015, Northern Kentucky Law Review, THE CHANGING EXPECTATION OF PRIVACY: KEEPING UP WITH THE MILLENNIAL GENERATION AND LOOKING TOWARD THE FUTURE, v. 42, p. 309

The "Internet of Things" is one example of potential danger. The "Internet of Things" refers to the growing number of devices and items that are being embedded with some type of sensor or are otherwise connected to the Internet.²⁰⁵ With the nearly ubiquitous ability to be online nowadays through the spread of Wi-Fi networks, many devices are always connected to a network. This

connection allows for the continuous collection of data, as well as in some cases, the ability to control the device.²⁰⁶ A device that might be considered to be a part of the "Internet of Things" is a Slingbox, which allows a person to control and watch his television while away from home via the Internet.²⁰⁷ Other examples include devices that provide people with the ability to control their home thermostats through applications on their smart phones.²⁰⁸ These conveniences are wonderful when they are working properly, but some analysts speculate that such technology could lead to actual physical threats in the future if someone finds a way to take over control of the devices, and could for example, raise the [*313] temperature in a person's home to the highest setting.²⁰⁹ Another example is the future of automobiles. Vehicles are already starting to come with devices such as GPS systems as standard equipment. These devices are monitoring your location in order to provide you with route information; data about your location is being collected and stored.²¹⁰ Automobile manufacturers are currently working together to develop stricter policies regarding the control and management of the collected data, but they are still collecting it.²¹¹

Privacy is a fundamental human right

Jan Henrik Ziegeldorf, Communication and Distributed Systems, RWTH Aachen University, Oscar Garcia Morchon, Philips Research and Klaus Wehrle, Communication and Distributed Systems, RWTH Aachen University, Privacy in the Internet of Things: Threats and Challenges," SECURITY AND COMMUNICATION NETWORKS 2013,
<https://pdfs.semanticscholar.org/8356/9ba92d199a7a5cb172f4b9e28a145e621f41.pdf>

Privacy is recognized as a fundamental human right in the 1948 Universal Declaration of Human Rights and is anchored in the constitutional law of most countries today. The first major piece of legislation on information privacy was passed with the 1974 US Privacy Act, which established the *fair information practices* (FIPs). The FIPs comprise the principles of notice, consent, individual access and control, data minimization, purposeful use, adequate security and accountability. They have been taken up in [21] by the Organization for Economic Co-operation and Development (OECD), which anticipated trade- barriers from the increasingly diverse national privacy legislation. While US privacy legislation continued with a miscellany of specific sectorial laws, the European Union's aim for comprehensive legislation resulted in the 1995 *Directive 95/46/EC on the protection of individuals with regard to processing of personal data and on the free movement of such data* [22]. The directive embeds the FIPs and adds the principle of *explicit consent*, which basically forbids any kind of data collection without explicit permission from the subject.

Privacy Key To Other Rights

Intellectual privacy is the basis for all other political and religious rights.

Richards 8 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2008 (“Intellectual Privacy,” *Texas Law Review* (87 Tex. L. Rev. 387), December, Available Online to Subscribing Institutions via Lexis-Nexis)

The core of intellectual privacy is the freedom of thought and belief. The freedom to think and to believe as we want is arguably the defining characteristic of a free society and our most cherished civil liberty. n118 This right encompasses the range of thoughts and beliefs that a person might hold or develop, dealing with matters that are trivial and important, secular and profane. And it protects the individual's thoughts from scrutiny or unwilling disclosure by anyone, whether a government official or a private actor such as an employer, a friend, or a spouse. At the level of law, if there is any constitutional right that is absolute, it is this one, which is the precondition for all other political and religious rights guaranteed by the Western tradition.

The impact is the loss of personal autonomy and agency. Privacy is a gateway right, it enables all of our other freedoms.

PoKempne 14,

Dinah, General Counsel at Human Rights Watch, “The Right Whose Time Has Come (Again): Privacy in the Age of Surveillance” 1/21/14 <http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance>

Technology has invaded the sacred precincts of private life, and unwarranted exposure has imperiled our security, dignity, and most basic values. The law must rise to the occasion and protect our rights. Does this sound familiar? So argued Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article announcing “The Right to Privacy.” We are again at such a juncture. The technological developments they saw as menacing—photography and the rise of the mass circulation press—appear rather quaint to us now. But the harms to emotional, psychological, and even physical security from unwanted exposure seem just as vivid in our digital age. **Our renewed sense of vulnerability comes as almost all aspects of daily social life migrate online.** At the same time, corporations and governments have acquired frightening abilities to amass and search these endless digital records, giving them the power to “know” us in extraordinary detail. In a world where we share our lives on social media and trade immense amounts of personal information for the ease and convenience of online living, some have questioned whether privacy is a relevant concept. It is not just relevant, but crucial. **Indeed, privacy is a gateway right that affects our ability to exercise almost every other right, not least our freedom to speak and associate with those we choose, make political choices, practice our religious beliefs, seek medical help, access education, figure out whom we love, and create our family life. It is nothing less than the shelter in which we work out what we think and who we are; a fulcrum of our autonomy as individuals.** The importance of privacy, a right we often take for granted, was thrown into sharp relief in 2013 by the steady stream of revelations from United States government files released by former National Security Agency (NSA) contractor Edward Snowden, and published in the Guardian and other major newspapers around the world. **These revelations, supported by highly classified documents, showed the US, the UK, and other governments engaged in global indiscriminate data interception, largely unchecked by any meaningful legal constraint or oversight, without regard for the rights of millions of people who were not suspected of wrongdoing.** The promise of the digital age is the effortless, borderless ability to share

information. That is its threat as well. As the world's information moves into cyberspace, surveillance capabilities have grown commensurately. The US now leads in ability for global data capture, but other nations and actors are likely to catch up, and some already insist that more data be kept within their reach. In the end, there will be no safe haven if privacy is seen as a strictly domestic issue, subject to many carve-outs and lax or non-existent oversight. Human Rights Watch weighed in repeatedly throughout 2013 on the human rights implications of Snowden's revelations of mass surveillance, and the need to protect whistleblowers. This essay looks at how the law of privacy developed, and where it needs to reach today so that privacy is globally respected by all governments, for all people. Global mass surveillance poses a threat to human rights and democracy, and once again, the law must rise to the challenge.

Rights based Advantage Impact/Framing

The impact is the loss of personal autonomy and agency. Privacy is a gateway right, it enables all of our other freedoms.

PoKempne 2014,

Dinah, General Counsel at Human Rights Watch, “The Right Whose Time Has Come (Again): Privacy in the Age of Surveillance” 1/21/14 <http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance>

Technology has invaded the sacred precincts of private life, and unwarranted exposure has imperiled our security, dignity, and most basic values. The law must rise to the occasion and protect our rights. Does this sound familiar? So argued Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article announcing “The Right to Privacy.” We are again at such a juncture. The technological developments they saw as menacing—photography and the rise of the mass circulation press—appear rather quaint to us now. But the harms to emotional, psychological, and even physical security from unwanted exposure seem just as vivid in our digital age. Our renewed sense of vulnerability comes as almost all aspects of daily social life migrate online. At the same time, corporations and governments have acquired frightening abilities to amass and search these endless digital records, giving them the power to “know” us in extraordinary detail. In a world where we share our lives on social media and trade immense amounts of personal information for the ease and convenience of online living, some have questioned whether privacy is a relevant concept. It is not just relevant, but crucial. Indeed, privacy is a gateway right that affects our ability to exercise almost every other right, not least our freedom to speak and associate with those we choose, make political choices, practice our religious beliefs, seek medical help, access education, figure out whom we love, and create our family life. It is nothing less than the shelter in which we work out what we think and who we are; a fulcrum of our autonomy as individuals. The importance of privacy, a right we often take for granted, was thrown into sharp relief in 2013 by the steady stream of revelations from United States government files released by former National Security Agency (NSA) contractor Edward Snowden, and published in the Guardian and other major newspapers around the world. These revelations, supported by highly classified documents, showed the US, the UK, and other governments engaged in global indiscriminate data interception, largely unchecked by any meaningful legal constraint or oversight, without regard for the rights of millions of people who were not suspected of wrongdoing.

The impact is Totalitarianism, the loss of autonomy due to surveillance enables “turnkey totalitarianism,” destroying democracy.

Haggerty, 2015

Kevin D. Professor of Criminology and Sociology at the University of Alberta, “What’s Wrong with Privacy Protections?” in A World Without Privacy: What Law Can and Should Do? Edited by Austin Sarat p. 230

Still others will say I am being alarmist. My emphasis on the threat of authoritarian forms of rule inherent in populations open to detailed institutional scrutiny will be portrayed as overblown and over dramatic, suggesting I veer towards the lunatic fringe of unhinged conspiracy theorists.⁶⁶ But one does not have to believe secret forces are operating behind the scenes to recognize that our declining private realm presents alarming

dangers. Someone as conservative and deeply embedded in the security establishment as William Binney – a former NSA senior executive – says the security surveillance infrastructure he helped build now puts us on the verge of “turnkey totalitarianism.”⁶⁷ The contemporary expansion of surveillance, where monitoring becomes an ever-more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger of this situation is how our existing surveillance practices can be turned to oppressive uses. From this point forward our expanding surveillance infrastructure stands as a resource to be inherited by future generations of politicians, corporate actors, or even messianic leaders. Given sufficient political will this surveillance infrastructure can be re-purposed to monitor – in unparalleled detail – people who some might see as undesirable due to their political opinions, religion, skin color, gender, birthplace, physical abilities, medical history, or any number of an almost limitless list of factors used to pit people against one another. The twentieth century provides notorious examples of such repressive uses of surveillance. Crucially, those tyrannical states exercised fine-grained political control by relying on surveillance infrastructures that today seem laughably rudimentary, comprised as they were of paper files, index cards, and elementary telephone tapping.⁶⁸ It is no more alarmist to acknowledge such risks are germane to our own societies than it is to recognize the future will see wars, terrorist attacks, or environmental disasters – events that could themselves prompt surveillance structures to be re-calibrated towards more coercive ends. Those who think this massive surveillance infrastructure will not, in the fullness of time, be turned to repressive purposes are either innocent as to the realities of power, or whistling past a graveyard. But one does not have to dwell on the most extreme possibilities to be unnerved by how enhanced surveillance capabilities invest tremendous powers in organizations. Surveillance capacity gives organizations unprecedented abilities to manipulate human behaviors, desires, and subjectivities towards organizational ends – ends that are too often focused on profit, personal aggrandizement, and institutional self-interest rather than human betterment.

Freedom and dignity are ethically prior to security.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed. This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents

and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

Privacy First

Freedom and dignity are ethically prior to security.

Cohen, 2014

Elliot D. Ph.D., ethicist and political analyst. He is the editor in chief of the International Journal of Applied Philosophy, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.. DOI: 10.1057/9781137408211.0011.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed. This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

Privacy must be valued above all else

Goold, 10- Associate Professor at the University of British Columbia Faculty of Law and a Research Associate at the Oxford University Centre for Criminology, (Benjamin, "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy", OVERVÅKNING I EN RETTSSTAT - SURVEILLANCE IN A CONSTITUTIONAL GOVERNMENT, 2010, PDF, page 45-47)//AP

This all of course leads us back to the question at the beginning of this chapter, namely: how much state surveillance is too much? Perhaps the first and most obvious response to this question is that the state should at all times be sensitive to the fact that privacy is a basic human right, and that it is essential to personal development, individual dignity, and the ability of citizens to engage in meaningful social relationships. We have, in the words of Article 8 of the European Convention on Human Rights, a right to "respect for private and family life" because without such privacy we can never truly flourish. Going further, however, the state must also recognize that privacy has an important role to play in the promotion of democracy and the meaningful exercise of a number of other fundamental rights, such as the right to freedom of expression and freedom of association. As a consequence, all state surveillance activities – regardless of whether the justification for such measures is the prevention of crime, the promotion of security, or even the efficient delivery of public services – must be evaluated in terms of the potential cost to political freedom and the maintenance of democratic values. This is particularly important given that, as Bennett and Raab rightly point out, the social value of privacy can be easily forgotten in our efforts to protect individuals from the personal effects of overzealous state surveillance. The social value [of

privacy] is underpowered and survives precariously unless it can be specifically reinforced by a change in the privacy culture, for it is powerfully challenged by the legacy of the conventional paradigm and by forces that tend to the protection of privacy seen as an individual value, if a value at all.⁶² Put simply, there is little point in the state seeking to create a society free from crime and secure against terrorist threats if the overall cost is a severe loss of personal freedom and the introduction of Orwellian, authoritarian government. Put more simply, we know that there is too much surveillance when citizens begin to fear the surveillance activities of the state, and no longer feel free to exercise their lawful rights for fear of unwanted scrutiny and possible censure. Finally, given that a democratic state can only be legitimate and thrive in an atmosphere of mutual trust between government and governed, it follows that any surveillance measure that threatens to erode or destroy that trust must be resisted, or at the very least its potential costs and benefits carefully considered. As anyone who has lived in a state where the rule of law is not taken for granted – and where there is little in the way of institutional trust – will be able to tell you, confidence in the institutions of government is hard won and easily lost.⁶³ For this reason, the presumption should be that any surveillance measure which is directed at the public at large – and which treats all citizens as potential threats or management challenges – has *prima facie* gone a step too far, and demands an extra-ordinary justification. According to this view, mass state surveillance should always be the exception and never the rule. In short, we will know when there is too much state surveillance when political rights and democratic participation are threatened, and it is at this point that the citizenry should demand that the state pulls back and accepts that there are times when it is better for the government to know less rather than more. Of course, some will say that we have already passed this point, that the current surveillance infrastructure already poses a serious threat to democracy and the rule of law. If this is true, then there is an even more pressing need for us to demand a halt to any further expansion in the surveillance apparatus of the state, and a fundamental reappraisal of the state's use of technologies like public area CCTV.

Privacy is a fundamental moral right.

Alfino and Mayes, 2003

Mark Alfino Department of Philosophy Gonzaga University G. Randolph Mayes Department of Philosophy California State University, Sacramento "Reconstructing the right to privacy." Social Theory and Practice 29.1 (2003): 1-18.

The core claim in our theory is that **privacy is a fundamental moral right**. The argument to support this claim is simple, but the consequences and implications of the argument are not. In this section, we focus on establishing the right to privacy as a fundamental moral right and elucidating some of the most obvious implications of the view. We leave further development of the view and an exploration of objections to the next section. In arguing for privacy as a fundamental moral right, we obviously assume that a scheme of rights and correlative duties is a well-justified way to describe social relations among individuals. Specifically, moral rights describe the legitimate exercise of power, both of individuals and others, severally and collectively. Rights can be thought of negatively as mutual protection schemes and positively as a reflection of our best understanding of how individuals establish and maintain their moral agency." At the heart of our understanding of moral agency is a belief about the ability of moral individuals to be "self-legislating" or autonomous. We will look at important differences of emphasis in different definitions of autonomy in a moment, but at present the important point is that in a system of rights and duties the concept of the self-legislating individual is central. In fact, most basic moral rights can be understood as explications of the concept of a self-legislating agent, or the implications of how such a person necessarily interacts with a physical and social world. For example, rights of due process are fundamental moral rights, because in an environment in which I could not be guaranteed a rational (due) process for losing rights and privileges, I could not formulate rational rules for my own conduct. Privacy plays a fundamental and ineliminable role in constructing personal autonomy. To see this, it may help to extend the juridical metaphor at the heart of the notion of autonomy. What kinds of law do agents legislate? To what realm of objects does such law apply? Of course, these are questions that Immanuel Kant posed and answered extensively.¹² Kant demonstrated that a basic heuristic of moral life is an analogy between physical space and the laws of nature that govern it, on the one hand, and moral space and the moral law on the other hand. This analogy lies at the heart of "rights talk." It is common to speak of rights as law-like background conditions from which we can

predict the outcome of claims and torts. Jurists and legislators use rights instrumentally—for good and ill—to establish various kinds of space: a private space of property relationships and private social relationships, a public space of communal expectations for fair treatment and access. When we grant "privilege" to specific kinds of relationships, such as the confidential conversations between priests and confessors or lawyers and their clients, we are using moral laws to configure moral space just as a divine creator might be imagined to configure physical space from a set of possible physical laws. Whether or not we grant moral space any ontological significance, it still helps to elucidate our basic theoretical framework. The analogy between moral and physical space also reminds us of the need to configure the moral space needed for individuals to become autonomous agents upon a realistic view of how individuals actually develop, both cognitively and emotionally. We can criticize competing explications of moral space by reference to our background knowledge of human behavior and development. Facts about our psychology do not by themselves justify moral rights. However, our understanding of the moral space that an autonomous agent inhabits and the moral laws that govern that space must cohere with our understanding of the laws of the physical world, especially those governing the psychological development of human animals and the physical conditions of their existence. Within these constraints we make a variety of choices about which aspects of our physical and psychic environment to value, and in so doing we construct the specific moral space that governs social life.

Additionally, because of foundational nature of privacy, it is not optional.

Allen, 2011

Anita. J.D., Ph.D, Henry R Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania School of Law. Unpopular privacy: what must we hide?. Oxford University Press, 2011. Pp 172-3

Since the 1970s, when scholars first began to analyze privacy in earnest, philosophers have linked the experience of privacy with dignity, autonomy, civility, and intimacy. They linked it also to repose, self-expression, creativity, and reflection. They tied it to the preservation of unique preferences and distinct traditions.

Privacy is a foundational good. The argument that privacy is a right whose normative basis is respect for persons opens the door to the further argument that privacy is also potentially a duty. "To respect someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one's decision," S. I. Benn wrote.³⁵ And to respect oneself may require taking into account the way in which one's personality and life enterprises could be affected by decisions to dispense with foundational goods that are lost when one decides to flaunt, expose, and share rather than to reserve, conceal, and keep. The idea that the experience of privacy is ethically mandatory is logically consistent with leading normative accounts. It is consistent with Robert Post's (citing Erving Goffman and Jeffrey Reiman) "characterization of respecting privacy as respecting civility norms" of deference and demeanor.³⁶ It is likewise consistent with Helen Nissenbaum's analysis of privacy. She defines privacy and its value in relation to norms of the appropriateness of specific behaviors and the distribution of certain information in social and cultural context.⁴⁰ If people are completely morally and legally free to pick and choose the privacy they will experience, such as deferential civility, appropriateness and limited data flow, they are potentially deprived of highly valued states that promote their vital interests, and those of fellow human beings with whom they associate. We need to restrain choice—if not by law, then somehow. **Respect for privacy rights and the ascription of privacy duties must both be a part of a society's formative project for shaping citizens.**

Lior Jacob Strahilevitz has argued that privacy violations can be understood as rechanneling information flow, so that information unknown or obscure in a network becomes known: "Where a defendant's (in a suit alleging informational privacy invasion disclosure materially alters the flow of otherwise obscure information through a social net-work, such that what would have otherwise remained obscure becomes widely known, the defendant should be liable for public disclosure of private facts."⁴¹ Viewed in this way, it may not seem to matter that privacy is invaded unless the person whose information flows out against his will cares. We have to go back to dignitarian ideals about privacy to see why we, as liberals, should care about optional dismissals of privacy. Jeffrey Reiman defined privacy as the "social rituals" that serve to teach us that we are distinct moral persons and autonomous moral agents.⁴² Liberals agree that there is something wrong with being watched and investigated all the time. As legal theorist Daniel Solove argues, surveillance can make "a person feel extremely uncomfortable" and can lead to "self-censorship and inhibition."⁴³ Surveillance is a form of social control. As such, it impacts freedom. I have been urging that

dispensing with one's privacy is yielding to social control, and that that impacts freedom, too.
Realizing this, the notion that some privacy should not be optional, waivable, or alienable should have instant credibility.

Privacy = Moral Obligation

Equal freedom establishes privacy not only as a duty but also as a right

Mokrosinska, 2014

Dorota, Research Fellow in Philosophy at the University of Amsterdam, The Netherlands (2014), Privacy and the Integrity of Liberal Politics: The Case of Governmental Internet Searches. Journal of Social Philosophy, 45: 369–389. doi: 10.1111/josp.12068

I close my argument by drawing attention to the value and the normative status of privacy in political practice. I have argued that privacy is implicated in the concept of public justification that liberals place at the core of the concept of political legitimacy. Public justification requires that people explain to one another how the principles and policies they advocate can be supported by reasons that everyone can reasonably accept. That requirement is substantially linked to the idea of the equal freedom of individuals: equal freedom between individuals acting in the political domain is not realized unless policies are justified to all those who are subject to them. Political liberals tie the concept of public justification to an obligation that falls on individuals as members of political societies. In this context, Rawls speaks of a “duty of civility,”⁶² Lafont and Audi speak of a similar duty.⁶³ Now one cannot appeal to reasons that everyone can accept unless one holds back and refrains from bringing under collective attention one's unreasonable and comprehensive views. This is to say that one cannot perform the duty of civility unless one brackets such material as private. From this perspective, privacy is an aspect of the duty of civility and a condition of equal freedom. Equal freedom requires not only that individuals withhold their unreasonable and/or comprehensive views from the political forum. It also requires that they not attend to similar material in others. Given that such material is equally dysfunctional to the political realm, its exposure would be equally threatening to equal freedom. From that perspective, refraining from seeking, scrutinizing and exposing unreasonable and/or comprehensive beliefs of others is another aspect of the duty of civility. The same point can be expressed in the language of rights. If one's equal freedom cannot be realized unless others refrain from attending to one's (unreasonable) comprehensive views, then one is entitled, by virtue of equal freedom, that they do so. In this sense, **equal freedom establishes privacy not only as a duty but also as a right.**

Moral obligation to protect privacy — just as important as any other right

Gavison 12 — Ruth E. Gavison, Professor of Human Rights Law at Hebrew University Law Faculty. Born in Jerusalem. Received an LLB (cum laude) in 1969, LLM (summa cum laude) in 1971, and BA in economics and philosophy (1970), all from Hebrew University. Law clerk at the Israel Supreme Court (Justice Benjamin Halevi). Admitted to the Israeli bar in 1971. In 1975 she received a D.Phil. in legal philosophy from Oxford University, 2012 (“Privacy and the Limits of Law,” *Yale Law Journal*, Vol 28 No. 3, Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957, Accessed on 7-15-15)

It is here that understanding the reasons for the new concern with privacy becomes crucial. It is true that individuals today enjoy more opportunities for privacy in some areas, but this observation, taken alone, is misleading. The rarity of actions is not a good indication of the need for privacy, or of the extent to which invasions are undesirable. We enjoy our privacy not because of new opportunities for seclusion or because of greater control over our interactions, but be- cause of our anonymity, because no one is interested in us. The moment someone becomes sufficiently interested, he may find it quite easy to take all that privacy away. He may follow us all the time, obtain information about us from a host of data systems, record our conversations, and intrude into our bedrooms. What protects privacy is not the difficulty of invading it, but the lack of motive and interest of others to do so. The important point, however, is that if our privacy is invaded, it may be invaded today in more serious and more permanent ways than ever before. Thus, although most of us are unlikely to experience a substantial loss of

privacy, we have an obligation to protect those who lose their anonymity. In this sense, **privacy is no different from other basic entitlements.** We are not primarily concerned with the rights of criminal suspects because we have been exposed to police brutality ourselves. We know that we may be exposed to it in the future, but, more generally, we want to be part of a society that is committed to minimizing violations of due process.

Privacy - Deontology

Privacy is Kantian — key to human dignity

Buitelaar, 2014

J. C. Professor, Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands "Privacy and Narrativity in the Internet Era." *The Information Society* 30.4 (2014): 266-281.

There are manifold definitions and views of privacy. A seminal starting point is that of Warren and Brandeis (1890), namely, that privacy should be regarded as a general right to the immunity of the person. The right to privacy, as part of the more general right to the immunity of the person, is related to the right to one's personality. From this point of view it can be argued that the value of privacy is grounded in the principle of permitting and protecting an autonomous life (Kant 1996; Rössler 2001). The moral philosopher Kant was an early proponent of the view of the intrinsic value of human dignity (Kant 1996). Kant did, however, put a constraint on this view, namely, that humans owe themselves a duty of self-esteem but also a claim to and the duty to respect other humans. In Article 1 of the Universal Declaration of Human Rights, this Kantian principle of intrinsic human dignity is adopted, where the declaration states that all human beings are born free and equal in dignity and rights. This inherent dignity accounts for the possession of inalienable human rights. These rights find their origin in the capacity of the human being to reflect and make choices. A. R. Miller combines these two concepts to explain the importance of informational self-determination for preservation of privacy: "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to himself, a power that often is essential to maintaining social relationships and personal freedom" (Miller 1971, 25). If the individual can no longer determine to what extent they reveal themselves to the outside world, privacy is robbed of its core value, which is the opportunity to freely decide for oneself. The intrinsic dignity of the individual, from the liberal point of view at least, guarantees the autonomy to act freely and thus make the choices that allow a person to flourish and to develop their personality. This is also the principle of personal freedom enshrined in the German Constitution. Furthermore, privacy provides the individual with a safe place, where they can decide for themselves which relations they enter into. I maintain that they can only do so if they can control who has access to them. When this situation exists, they have the assurance that they can control the patterns of behavior they want to adopt.

702 Surveillance Program

702 Supports Surveillance/Rights Deprivation

702 shoehorns in billions of domestic communications for surveillance

Goitein and Patel 15 - Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program. Served as counsel to Sen. Russell Feingold with a particular focus on government secrecy and privacy rights. Was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit. Faiza Patel serves as co-director of the Brennan Center for Justice's Liberty and National Security Program. Clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Ms. Patel is a graduate of Harvard College and the NYU School of Law. (Elizabeth and Faiza, "What went wrong with the FISA court", Brennan Center for Justice at New York University School of Law, 2015, p.41-42//DM)

As enacted in 1978, FISA required the government to show probable cause that the target of surveillance was a foreign power or an agent of a foreign power. The FAA eliminated this requirement for programmatic surveillance. The target of surveillance may be any non-U.S. person or entity located overseas, and the FISA Court has interpreted the law to allow the government to obtain any communications to, from, or about the target.²⁵⁸ The only limitation is a requirement that the government certify that a significant purpose is the collection of "foreign intelligence."

Consider how these changes could operate in practice. As noted in Part II.C.2, "foreign intelligence information," where non-U.S. persons are concerned, is broadly defined to include information "that relates to . . . (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States."²⁵⁹ This elastic concept is unlikely to impose any meaningful restraint — particularly since the FISA Court is not allowed to probe the government's foreign intelligence certification.²⁶⁰ The only real limitation on surveillance, then, is the target's nationality and location.

Given the prevalence of international communication today, the government could shoehorn literally billions of communications (including communications with Americans) into a warrantless foreign intelligence collection framework, as long as there is a chance that the net will pull in some information relating to security or foreign affairs. This is plainly inconsistent with the admonition of most courts that warrantless foreign intelligence surveillance must be "carefully limited" to "those situations in which the interests of the executive are paramount."²⁶¹

In a 2008 opinion approving Section 702 targeting and minimization procedures, the FISA Court held that limiting the foreign intelligence exception to foreign powers or their agents is unnecessary when the target is a non-citizen overseas.²⁶² This ruling ignores the fact that Section 702 is designed to capture communications involving U.S. persons, and expressly contemplates that U.S. person information may be kept and shared where minimization would be inconsistent with "the need of the United States to obtain, produce, and disseminate foreign intelligence information."²⁶³ Regardless of who is labeled the "target," Section 702 involves the acquisition and use of Americans' information for foreign intelligence purposes, in volumes that likely far exceed the collection in Truong and similar cases. The need to construe the exception narrowly is thus at least as important in the Section 702 context.

702 is the justification for widespread squo domestic surveillance

Goitein and Patel 15 - Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program. Served as counsel to Sen. Russell Feingold with a particular focus on government secrecy and privacy rights. Was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit. Faiza Patel serves as co-director of the Brennan Center for Justice's Liberty and National Security Program. Clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Ms. Patel is a graduate of Harvard College and the NYU School of Law. (Elizabeth and Faiza, "What went wrong with the FISA court", Brennan Center for Justice at New York University School of Law, 2015, /DM)

It is no exaggeration to say that the world of electronic surveillance looks entirely different today than it did in 1978 when the FISA Court was established to oversee foreign intelligence surveillance. Communications technology and the legal framework have fundamentally changed, vastly increasing the nature and quantity of information the government may collect — and decreasing the court's role in supervising these operations.

Although the Supreme Court in Keith attempted to distinguish between surveillance of domestic organizations and surveillance of foreign powers, the demarcation was never clean and has become ever more strained. Advances in technology mean that the exercise of authorities aimed at foreigners abroad inevitably picks up swaths of information about Americans who should enjoy constitutional protections. But rather than develop additional safeguards for this information, the law has developed in the opposite direction: the government's authority to collect communications pursuant to its foreign intelligence-gathering authorities has expanded significantly. At the same time, the safeguard of judicial review — already limited when FISA was first enacted in 1978 — has eroded to near-nothingness. Indeed, in some cases, the role played by the FISA Court is so different from the normal function of a court that it likely violates the Constitution's separation of powers among the legislative, executive, and judicial branches.

A. A Revolution in Communications Technology

The impact of advances in communications technology over the last decades cannot be overstated. In 1978, most domestic telephone calls were carried over copper wires,¹⁰² while most international calls took place via satellite.¹⁰³ To listen to a domestic call, the government had to identify the wire that geographically connected the two ends of a communication and manually tap into it.¹⁰⁴ Capturing a satellite communication to or from a particular source required sophisticated equipment; resulting databases were subject to practical limitations on storage and analytical capability.¹⁰⁵ Cellular phones were not commercially available,¹⁰⁶ and the Internet existed only as a Department of Defense prototype.¹⁰⁷ Surveillance generally had to occur in real time, as electronic communications were ephemeral and unlike later forms of communication (like e-mail) were not usually stored.

Today, a large proportion of communications — including e-mails and international phone calls — are transmitted by breaking down information into digital packets and sending them via a worldwide network of fiber-optic cables and interconnected computers.¹⁰⁸ The government can access these communications by tapping directly into the cables or into the stations where packets of data are sorted.¹⁰⁹ Digital information often is stored for long periods of time on servers that are owned by private third parties, giving the government another way to obtain information, as well as access to a trove of historical data. Most cell phone calls, along with other forms of wireless communication, travel by radio signals that are easily intercepted.

These changes have weakened the relationship between the place where communications are intercepted and the location (and nationality) of the communicants. For communications that travel wholly or in part via packets, each packet may follow a different route, and the route may be unrelated to the locations of the sender or recipient. An e-mail from a mother located in San Diego to her daughter in New York could travel through Paris, and the contents might be stored by an online service provider in Japan. But FISA, as enacted in 1978, is keyed to the location and nationality of the target and the location of acquisition. As discussed further in Part II.B.3.a, the globalization of the communications infrastructure has changed the way the law plays out in practice.¹¹⁰

Technological changes also have expanded the amount of information about Americans the government can acquire under FISA. For one thing, globalization and advances in communications technology have vastly increased the volume — and changed the nature — of international communications. The cost and technological difficulties associated with placing international calls during the era of FISA's passage meant that such calls were relatively rare. In 1980, the average American spent less than 13 minutes a year on international calls.¹¹¹ Today, the number is closer to four and a half hours per person — a thirty-fold increase.¹¹² That number does not include the many hours of Skype, FaceTime, and other Internet-based voice and video communications logged by Americans communicating with family, friends, or business associates overseas. And, of course, the advent of e-mail has removed any barriers to international communication that may have remained in the telephone context, such as multi-hour time differences. Worldwide e-mail traffic has reached staggering levels: in 2013, more than 182.9 billion e-mails were sent or received daily.¹¹³ As international communication has become easier and less costly, the content of communications is much more likely to encompass — and, in combination, to create a wide-ranging picture of — the intimate details of communicants' day-to-day lives.

Technology and globalization also have led to much greater mobility, which in turn has generated a greater need to communicate internationally. Foreign-born individuals comprised around 6 percent of the U.S. population when FISA was enacted but account for more than 13 percent today.¹¹⁴ Immigrants often have family members and friends in their countries of origin with whom they continue to communicate. Similarly, there has been a sharp increase in Americans living, working, or traveling abroad, creating professional or personal ties that generate ongoing communication with non-citizens overseas. The number of Americans who live abroad is nearly four times higher than it was in 1978 and the number of Americans who travel abroad annually is nearly three times higher.¹¹⁵ The number of American students who study abroad each year has more than tripled in the past two decades alone.¹¹⁶ These trends show no signs of abating, suggesting that the volume of international communications will only continue to expand.

In addition, technological changes have made it likely that government attempts to acquire international communications will pull in significant numbers of wholly domestic communications for which Congress intended the government to obtain a regular warrant rather than proceeding under FISA. For instance, a recently declassified FISA Court decision shows that when the NSA taps into fiberoptic cables, it pulls in some bundles of data that include multiple communications — including communications that may not involve the target of surveillance. The NSA claims that it is “generally incapable” of identifying and filtering out such data bundles.¹¹⁷ The result is that the agency routinely collects large numbers of communications —

including “tens of thousands of wholly domestic communications” between U.S. persons — that are neither to, from, or about the actual “target.”¹¹⁸

For all of these reasons, the collection of foreign intelligence surveillance today involves Americans’ communications at a volume and sensitivity level Congress never imagined when it enacted FISA. If the government wished to acquire the communications of a non-citizen overseas in 1978, any collection of exchanges involving Americans could plausibly be described as “incidental.” Today, with international communication being a daily fact of life for large numbers of Americans, the collection of their calls and e-mails in vast numbers is an inevitable consequence of surveillance directed at a non-citizen overseas. The volume of information collected on U.S. persons makes it difficult to characterize existing foreign intelligence programs as focused solely on foreigners and thus exempt from ordinary Fourth Amendment constraints.

Section 702 violates the 4th amendment – causes systematic domestic surveillance and creates a back door around the warrant requirement

Goitein and Patel 15 - Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice’s Liberty and National Security Program. Served as counsel to Sen. Russell Feingold with a particular focus on government secrecy and privacy rights. Was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit. Faiza Patel serves as co-director of the Brennan Center for Justice’s Liberty and National Security Program. Clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Ms. Patel is a graduate of Harvard College and the NYU School of Law. (Elizabeth and Faiza, “What went wrong with the FISA court”, Brennan Center for Justice at New York University School of Law, 2015, p.38-39//DM)

Even if the collection of foreign intelligence is recognized as a “special need” that justifies surveillance without a traditional warrant, the government still must meet the second prong of the Fourth Amendment: the particular surveillance scheme must be “reasonable.”

In Camara, the Supreme Court recognized fire safety as a special need, but it did not simply give the government free rein to search buildings at will. Instead, it required inspectors to obtain court orders based on factors relevant to fire safety, such as the age and nature of the building and the condition of the general area. Individualized orders still had to be obtained before the search, but the standards were altered to match the special need.²³⁵ A similar arrangement may be required for foreign intelligence. As Fourth Amendment expert Professor Orin Kerr has noted: “[T]here is a plausible case to be made that foreign intelligence is a special need, but that [individualized] FISA warrants are still required to conduct foreign intelligence surveillance.”²³⁶

Limits on the discretion vested in government officials are key to establishing the reasonableness of a special needs scheme. For example, even though the Court on several occasions has authorized checkpoints to assess motorists’ sobriety or examine their license and car registration, it has refused to allow roving stops because they allow too much discretion on the part of government officials.²³⁷ The Court has emphasized that meeting the reasonableness standard of the Fourth Amendment requires “at a minimum, that the facts upon which an intrusion is based be capable of measurement against ‘an objective standard,’ whether this be probable cause or a less stringent test.”²³⁸ This focus stems from the Court’s concern about the potential for abuse of discretion; limiting this potential is a fundamental purpose of requiring a warrant under the Fourth Amendment.

As explored in the text box on page 33, the Section 702 program contains few limits on the discretion of analysts in deciding whether an individual is a non-U.S. person located overseas and therefore a valid target for programmatic surveillance. The NSA's targeting procedures set forth several considerations that officials may consider, but ultimately allow the NSA to reach a conclusion based on "the totality of the circumstances." The government has even more discretion in deciding what information is fair game: the statutory definition of foreign intelligence information is open-ended, and, under Section 702, the court cannot review the substance of the government's certification of a foreign intelligence purpose. It is difficult to square these features of programmatic surveillance with the type of "objective standards" that the Supreme Court has insisted on in the special needs context.

Moreover, even if the NSA's targeting and collection met the reasonableness test, the entire program cannot be deemed reasonable unless the government adequately "minimizes" the retention and use of information about U.S. persons that gets pulled in along with information about the foreign target. The FISA Court explicitly recognized this point when it found that the NSA violated the Fourth Amendment by failing to mark and delete wholly domestic e-mails acquired incidentally.²³⁹ Although the NSA remedied this violation to the court's satisfaction, its minimization regime remains notably lax. U.S. person information may be retained for 5 years, and there are multiple loopholes allowing for longerterm retention — including a provision for the indefinite retention of encrypted communications.²⁴⁰ As weak as the minimization rules are, reports suggest that they nonetheless are honored in the breach, with analysts claiming that they must retain seemingly irrelevant information about U.S. persons because the information may prove relevant in the future.²⁴¹

A particularly stark affront to the principle of minimization is the practice known as "back-door searches." To obtain an order from the FISA Court authorizing programmatic collection, the government must certify that its interest lies in foreigners overseas and not any U.S. persons with whom they may be in contact. The law prohibits "reverse targeting," in which the government targets a foreigner as a pretext to gain information about a particular, known U.S. person.²⁴² Consistent with these directives, the minimization procedures governing programmatic surveillance originally barred the government from using U.S. person identifiers to search the pool of communications obtained under Section 702.²⁴³ In 2011, the FISA Court granted the government's request to lift this bar.²⁴⁴ Today, officials routinely search through Section 702 data for information about the very U.S. persons the government certified it was not targeting.²⁴⁵

This practice allows the government to dispense with the much stricter substantive and procedural requirements that Congress put in place for obtaining foreign intelligence on an American target.²⁴⁶ It also allows the FBI to shrug off the Fourth Amendment when conducting domestic criminal investigations. The FBI performs searches of databases containing Section 702 data whenever it opens an investigation or an "assessment"²⁴⁷ — a type of investigation in which agents do not have a factual predicate to suspect criminal activity, let alone probable cause.²⁴⁸ Although the FISA Court has blessed back-door searches, it is difficult to see how a program that allows domestic law enforcement officers to listen to Americans' calls and read their e-mails without any fact-based suspicion of wrongdoing can be squared with the constitutional test of "reasonableness."

Privacy key to competitiveness

Failure to provide privacy protections to US persons wrecks US competitiveness

Donohue, 15 - Professor of Law, Georgetown University Law Center (Laura, "SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT" 38 Harv. J.L. & Pub. Pol'y 117, Winter, lexis)

The difficulty, for Section 702 purposes, enters in regard to Kennedy's reliance on the rule that he saw as most consistent with the United States' role as a sovereign nation. n447 "[W]e must interpret constitutional protections," he wrote, "in light of the undoubted power of the United States to take actions to assert its legitimate power and authority abroad." n448 What is the scope of the United States' legitimate power and authority abroad? To what degree is it rooted in the legal status of the individual against whom the state is acting? And what is the relationship between different forms of legal relationships and membership in the political community?

Let us focus here on the types of relationships most at issue with regard to Section 702: global electronic communications. One danger in according non-U.S. persons Fourth Amendment rights via (substantial) virtual contact with the United States is that individuals could use such contacts to evade detection. n449 Foreign persons could become members of Amazon Prime, communicate with associates in the United States via Verizon, and take Massive Open Online Courses (MOOCs) from the latest American university to offer them, perhaps even in the process obtaining a U.S. college or graduate degree. This could then become a shield to mask behavior that may undermine U.S. national security.

One response to this might be that in a global communications environment, privacy protections must be thought about in a broader sense. It matters little whether a customer is French, English, or American. Privacy rights should be extended to customers by nature of their dual status with U.S. persons qua customers--or even as a concomitant of their rights as people. This was the thrust of part of Privacy and Civil Liberties Oversight Board's (PCLOB) analysis that suggested privacy be regarded as a human right.

There is a realpolitik argument to be made here as well, which ties more directly to U.S. foreign interests. Namely, U.S. failure to [*228] ensure privacy protections may lead to a loss in U.S. competitiveness. And economic concerns are central to U.S. national security. Consider the impact of the public release of information about NSA Section 702 surveillance on the U.S. cloud computing industry. There was an immediate, detrimental impact on the strength of the U.S. economy. Billions of dollars are now on the line because of concerns that the services provided by U.S. information technology companies are neither secure nor private. n450 The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach \$ 35 billion over the next three years. n451 Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as \$ 180 billion by 2016, unless something is done to restore overseas' confidence in data held by U.S. companies. n452

Failure to extend privacy protections to individuals with substantial connections to the country via industry would, in this view, make it harder, not easier for the United States to assert its legitimate power and authority abroad. So, under Kennedy's reasoning, one could argue that Fourth Amendment rights should be extended to individuals economically tied to U.S. entities. This determination, however, is ultimately one of policy--not law. Deciding whether a greater national security threat is entailed in loss of competitiveness of U.S. industry, versus loss of protections extended to non-U.S. persons in the interests of privacy, is part of the weighing that must be done by the executive branch in pursuing its interests abroad. In this way, the Rehnquist opinion and [*229] the Kennedy concurrence can be read as compatible with not extending Fourth Amendment rights to individuals lacking a legal relationship (in other words, those stemming directly from the individual's status as a member of the political community). n453

Should End NSA Surveillance

Defund section 702

Vitka 15 *Federal Policy Manager at the Sunlight Foundation (Sean, “Ban on secret backdoor searches of American's data passes the House (again)”, Sunlight Foundation, 6/12/15, <http://sunlightfoundation.com/blog/2015/06/12/ban-on-secret-backdoor-searches-of-americans-data-passes-the-house-again//GK>

Recently, Sunlight and a bipartisan group of 26 other organizations — including the ACLU, Demand Progress and FreedomWorks — called on the House of Representatives to support an amendment to the Defense Appropriations bill that would end secret, warrantless surveillance on Americans' information. I'm happy to announce that our allies on the Hill — in particular Reps. Thomas Massie, R-Ky., Zoe Lofgren, D-Calif., and the other lawmakers who supported ambitious reforms like this when people thought they were impossible — have succeeded so far: The amendment passed the House, just as it did last year. As we explain in the letter: First, the amendment would defund warrantless government searches of the database of information collected under Section 702 of the Foreign Intelligence Surveillance Act of 1978 using U.S. person identifiers, absent certain circumstances. Although Section 702 prohibits the government from intentionally targeting the communications of U.S. persons, it does not explicitly restrict deliberately querying communications of Americans that were “inadvertently” or “incidentally” collected under Section 702. Moreover, following an apparent change in the NSA's internal practices in 2011, the NSA now is explicitly permitted under certain circumstances to conduct searches using U.S. person names and identifiers without a warrant. In March, James Clapper, the Director of the Office of National Intelligence, confirmed in a letter to Senator Wyden that such warrantless queries of U.S. person communications are being conducted. Second, the amendment would prohibit the use of appropriated funds to require or request that United States persons and entities build security vulnerabilities into their products or services in order to facilitate government surveillance, except as provided for by the Communications Assistance for Law Enforcement Act. The letter also specifically called for the House, in particular leadership, to ensure that this amendment stays in the bill. This amendment is the same as one that passed last year with an overwhelming 293 votes. But that doesn't mean this is a sure bet; it's incumbent on anyone who cares about this issue to reach out to their lawmakers and make their voices heard as soon as possible. Indeed, after passing last year with 293 votes, it was stripped out of the omnibus that ultimately became law. This is a step in the right direction for meaningful surveillance reform — let's make sure this bipartisan effort doesn't fail again.

Defund the NSA

Schneier, 15, fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Ch. 13)//AK

I have just proposed that the NSA's espionage mission be separated from its surveillance mission, and that the military's role in cyberspace be restricted to actions against foreign military targets. To accomplish this, I advocate breaking up the NSA and restoring and strengthening the various agencies' responsibilities that existed prior to 9/11:

- As part of the Department of Defense, the NSA should focus on espionage against foreign governments.
- The Department of Justice should be responsible for law enforcement and terrorism investigations. To that end, it should conduct only targeted and legally permissible surveillance

activities, domestic and foreign, and should pursue leads based on the expertise of FBI agents and not NSA databases.

- The NSA's defensive capabilities in cryptography, computer security, and network defense should be spun off and become much more prominent and public. The National Institute of Standards and Technology (NIST), a civilian agency outside the Department of Defense, should reassert control over the development of technical standards for network security. The Computer Security Act of 1987 attempted to keep the NSA out of domestic security by making it clear that NIST—then called the National Bureau of Standards—had the lead in establishing technical security standards. We need to strengthen that law and ensure it's obeyed.
- The US's offensive cyber capabilities should remain with US Cyber Command. That organization should subsume the NSA's hacking capabilities (that's TAO). The general in charge of US Cyber Command should not also be the director of the NSA.

This is a long-range plan, but it's the right one. In the meantime, we should reduce the NSA's funding to pre-9/11 levels. That in itself would do an enormous amount of good.

End programmatic surveillance recommendation

Goitein and Patel 15 - Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program. Served as counsel to Sen. Russell Feingold with a particular focus on government secrecy and privacy rights. Was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit. Faiza Patel serves as co-director of the Brennan Center for Justice's Liberty and National Security Program. Clerked for Judge Sidhu at the International Criminal Tribunal for the former Yugoslavia. Ms. Patel is a graduate of Harvard College and the NYU School of Law. (Elizabeth and Faiza, "What went wrong with the FISA court", Brennan Center for Justice at New York University School of Law, 2015 //DM)

A. End Programmatic Surveillance

The most effective reform would be for Congress to end programmatic surveillance. This would entail expressly prohibiting bulk collection under Section 215 and similar provisions, as well as repealing Section 702 and replacing it with a regime requiring an individualized court order for the interception of communications involving U.S. persons, regardless of whether they are the identified target of the surveillance.

Ending programmatic surveillance would return the FISA Court to its traditional role of applying the law to the facts of a particular case.²⁷¹ This would mitigate many of the Article III concerns relating to the absence of a case or controversy. If the standard for issuing a surveillance order were sufficiently strict (discussed below), ending programmatic surveillance could address Fourth Amendment objections as well.

But these changes would not fully cement the constitutional status of the FISA Court's activities. FISA orders will never look entirely like criminal warrants because they rarely culminate in criminal prosecutions, thus removing the primary vehicle for challenging their legitimacy. Concerns about the lack of adversarial process thus would remain even if programmatic surveillance were replaced with an individualized regime. To address them, the reforms listed in the next section would be needed.

Defund SIGINT Enabling Project

Obmres 1/22/15 – J.D. from Stetson University College of Law, L.L.M. from American University Washington College of Law (Devon, NSA DOMESTIC SURVEILLANCE FROM THE PATRIOT ACT TO THE FREEDOM ACT: THE UNDERLYING HISTORY, CONSTITUTIONAL BASIS, AND THE EFFORTS AT REFORM, 39 Seton Hall Legislation Journal p. 28)//JJ

None of the proposed legislation addresses the issue of NSA/NIST collaboration in creating backdoors to encryption systems. Additional congressional oversight could address the issue, but to address it at the outset and staunch the financial harm befalling the United States tech industry, the most readily available way to address the issue, would be the budgetary mechanism of defunding the SIGINT Enabling Project. This would limit the NSA's ability to strong-arm NIST and major telecoms and reinstate public trust in the tech industry.¹⁴³

Section 702 Doesn't Reduce Terrorism

702 not key to terror – other claims lack data

Bergen et al, 14 – a Professor of Practice at Arizona State University and a fellow at Fordham University's Center on National Security (Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, "Do NSA's Bulk Surveillance Programs Stop Terrorists?", New America Foundation, 1/13/2014, https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf)//MBB

It is difficult to determine the precise importance to counterterrorism of the NSA's surveillance programs under Section 702 in cases such as those above, because the NSA also conducts or has conducted surveillance under a range of other authorities. Not only are there the traditional, targeted FISA authorities and Section 702 of 2008's FISA Amendments Act, there is also Executive Order 12333, which primarily governs surveillance undertaken outside of the United States that is not targeted at U.S. persons, as well as the authorities that were used prior to 2008 to justify the Bush administration's warrantless wiretapping program, those being the temporary Protect America Act of 2007 and President Bush's own claims of inherent executive authority. The attempt to divine how useful Section 702 has been is also complicated by the fact that unlike the Section 215-based telephone metadata collection program, the exact scope and methods of the 702-based programs are still unclear.

However, according to the White House review panel's report, surveillance conducted under Section 702 authorities "has produced significant information in many, perhaps most, of the 54 situations in which signals intelligence has contributed to the prevention of terrorist attacks since

2007.”⁸² But the wording of the report also raises doubts about the importance of those contributions from Section 702, because the report concludes that it would be “difficult to assess precisely how many of these investigations would have turned out differently without the information learned through section 702.”⁸³

XO 12333 Doesn't Target US Citizens

XO 12333 exclusively governs foreign surveillance – incidental US information isn't used

Schlanger 15 [Margo, Professor of Law at the University of Michigan Law School, and the founder and director of the Civil Rights Litigation Clearinghouse., Intelligence Legalism and the National Security Agency's Civil Liberties Gap,
file:///C:/Users/Jonah/Downloads/Intelligence%20Legalism%20and%20the%20National%20Security%20Agency-s%20Civil%20Li%20(2).pdf] Schloss3

Executive Order 12,333 (invariably referred to orally as, simply, “twelve triple three”) is the “foundational” federal surveillance authority, applicable to all activities not otherwise regulated that touch or might touch U.S. person information.⁶⁴ Executive Order 12,333 has been amended three times since President Reagan issued it first in 1981, most recently and significantly in 2008, but it has retained its basic character.⁶⁵ As the organizing document for the nation’s intelligence operations, it applies to the entire Intelligence Community (IC). ⁶⁶ Individual IC elements then implement it via more focused guidelines, which are required to be signed by the Attorney General.⁶⁷ For the wide swathes of foreign intelligence surveillance that are not covered by FISA, regulation under Executive Order 12,333 occurs without judicial involvement. That is, where FISA does not apply, it is 12,333 that limits the collection, retention, use, and dissemination of U.S. person information, no matter what the method of surveillance— even if, for example, the communications are acquired from some foreign partner agency. The Executive Order explains that its “general principles . . . in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests.”⁶⁸ For surveillance, its basic approach is two-fold: it insists on in-advance fully vetted written procedures, and it authorizes specific surveillance without court approval only if the Attorney General approves.

702 not US Citizens

Violation – section 702 is strictly over foreign citizens

Mukasey 14 – former U.S. Attorney General, judge for the Southern District of New York, B.A. from Columbia, LL.B. from Yale (Michael, SAFE AND SURVEILLED: FORMER U.S. ATTORNEY GENERAL MICHAEL B. MUKASEY ON THE NSA, WIRETAPPING, AND PRISM, National Security Law Journal, 3/25/14, https://www.nslj.org/wp-content/uploads/3_NatlSecLJ_196-209_Mukasey.pdf)//JJ

The other program that's been the subject of debate is administered under Section 702 of the Foreign Intelligence Surveillance Act (FISA). That program allows the Attorney General and the Director of National Intelligence to authorize jointly, for up to a year, surveillance that's targeted at foreign persons reasonably believed to be located outside this country, provided that the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern the use of the information once it's gathered. Under this program, NSA can operate within the United States to gather the content of telephone calls and Internet traffic of people outside the United States.

How's that possible? Well, it's possible because the Internet and telephone messages that flow overseas pass through servers in the United States, so though telephone conversation or an exchange of e-mail may be between parties located entirely outside this country, the NSA can monitor cables passing through the United States to get that information. The NSA generates specific identifiers that may include, for example, telephone numbers or e-mail addresses of foreign persons outside this country, and then use[s] those identifiers to pick out communications that it is entitled to get from the general flow. The surveillance by law may not target anyone of any nationality known to be in this country or intentionally target a U.S. person anywhere in the world. In other words, they can't do reverse targeting on U.S. persons by listening in on foreign conversations. In order to get the content of communications involving anyone in the United States or any U.S. person located anywhere in the world, it's necessary to get a warrant supported by a showing of probable cause, just as one would in an ordinary criminal case.

Section 702 is purely for international surveillance

Logiurato, politics editor, 13 [Brett, Business Insider's politics editor. He graduated from Syracuse University in 2011 with degrees in newspaper and online journalism and political science., Here's The Law The Obama Administration Is Using As Legal Justification For Broad Surveillance, <http://www.businessinsider.com/fisa-amendments-act-how-prism-nsa-phone-collection-is-it-legal-2013-6>] Schloss

"Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States," Clapper said. "It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States.

Section 702 targets non-Americans believed to be outside the country.

Sales, Syracuse law professor, 2014

(Nathan, "NSA SURVEILLANCE: ISSUES OF SECURITY, PRIVACY AND CIVIL LIBERTY: ARTICLE: Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy", I/S: A Journal of Law and Policy for the Information Society, Summer, lexis)

The second program--known as PRISM or section 702--uses court orders issued under section 702 of FISA n18 to collect the content of certain international communications **In particular, the NSA targets specific non-Americans who are reasonably believed to be located outside the country, and also engages in bulk collection of some foreign-to-foreign communications** that happen to be passing through telecommunications infrastructure in the United States. n19 The FISA [*527] court does not approve individual surveillance applications each time the NSA wishes to intercept these communications; instead, it issues once-a-year blanket authorizations. n20 As detailed below, in 2011 the FISA court struck down the program on constitutional and statutory grounds after the government disclosed that it was inadvertently intercepting a significant number of communications involving Americans; n21 the court later upheld the program when the NSA devised a technical solution that prevented such over-collection. n22

FISA by design avoids issues related to domestic surveillance

Morrison, NYU law professor, 2008

(Trevor, ""The Story of United States v. United States District Court (Keith): The Surveillance Power", 11-20, http://lsr.nellco.org/cgi/viewcontent.cgi?article=1047&context=columbia_pllt)

In 1978, Congress responded by passing the Foreign Intelligence Surveillance Act (FISA).¹⁹⁴ As the Senate Judiciary Committee explained in a statement outlining the need for the legislation, "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."¹⁹⁵ Congress sought to "curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it," while [still] permitting the legitimate use of electronic surveillance to obtain foreign intelligence information."¹⁹⁶ FISA is sometimes viewed as a response to the Supreme Court's suggestion in Keith that Congress adopt special standards for surveillance in national security cases.¹⁹⁷ Yet, while Keith and FISA are certainly connected in important respects,¹⁹⁸ FISA does not take up the precise invitation issued in Keith. **That invitation applied to the category of surveillance addressed in the case—so-called “domestic security” surveillance for intelligence**

purposes.¹⁹⁹ **FISA does not cover such surveillance. In fact, “[n]o congressional action has ever been taken regarding the use of electronic surveillance in the domestic security area.”**²⁰⁰ For cases falling in that area, therefore, Keith’s direct application of the Fourth Amendment continues to govern.

Section 702 only deals with non US persons outside the US. McNeal, Pepperdine law professor and PhD, 2014

(Gregory, “Reforming The Foreign Intelligence Surveillance Court’s Interpretive Secrecy Problem”, 11-13, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2524067)

Section 702 authorizes the targeting of persons, and persons are defined in FISA. Persons are not only individuals, but also groups, entities, associations, corporations, or foreign powers.²⁷ As the PCLOB noted, the “definition of ‘person’ is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a ‘person’, but an entire foreign country cannot be a ‘person’ targeted under Section 702.”²⁸

Surveillance under section 702 may not intentionally target U.S. persons.²⁹ To ensure that only the appropriate people are being targeted by the NSA, the agency uses selectors “such as email addresses and telephone numbers. The NSA must make determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis. It cannot simply assert that it is targeting a particular terrorist group.”³⁰ **Pursuant to the terms of the statute, the non-U.S. persons targeted by the NSA must be “reasonably believed to be located outside the United States.”**³¹ The statute authorizes the government to compel “electronic communication service provider[s]” to assist the government in targeting non U.S. persons reasonably believed to be located outside the United States.³² Finally, the statute makes clear that the purpose for which non-U.S. persons are to be targeted is “to acquire foreign intelligence information.”³³ **Further, the government cannot use “what is generally referred to as ‘reverse targeting,’ which would occur if the government were to intentionally target persons reasonably believed to be located outside the United States ‘if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States.’”**³⁴

XO 12333 not domestic

Curtailing Executive Order 12333 has no effect on surveillance of US citizens

Executive Order 12333 (“Executive Order 12333 United States Intelligence Activities”, an amended version from 2003, 2004, and 2008, <http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf>//GK

Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information: (a) Information that is publicly available or collected with the consent of the person concerned; (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

Curtailing XO 12333 isn't topical—it surveils non-US persons

Arnbak and Goldberg 14- cybersecurity and information law research at the Institute for Information Law, LL.M degree from Leiden University, A Competitive Strategy and Game Theory degree from London School of Economics University of Amsterdam; Associate professor in the Computer Science Department at Boston University, PhD from Princeton University, B.A.S.c from University of Toronto (Axel and Sharon, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad”, Working Paper, June 27, 2014)//TT

2.3.1 Scope of the Third Regulatory Regime under EO 12333: Electronic Surveillance Conducted Abroad.

As discussed in the Section 2.2, electronic surveillance falls within the EO 12333 regime when it is conducted on foreign soil, and when it does not fall within the 1978 FISA definition of ‘electronic surveillance’. Or as the N.S.A. recently put it, when surveillance is “conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA.” [5, p. 2-3]. 4

While FISA surveillance is conducted from U.S. soil, EO 12333 surveillance is mostly conducted abroad. EO 12333 presumes that network traffic intercepted on foreign soil belongs to non-U.S. persons (cf. s. 9.8 & 9.18.e.2 of USSID 18 defining ‘foreign communications’ and ‘U.S. person’). Companies and associations are also considered in the EO 12333 definition of U.S. persons.

These entities may be assumed to be non-U.S. persons if they have their headquarters outside the U.S. Even when it is known to the N.S.A. that a company is legally controlled by a U.S. company, it may be assumed a non-U.S. person. Taken together, the rules for presuming a non-U.S. person under this regime are permissive on the individual-, group- and organizational levels.

Surveillance must be non-public information

Information held by third parties lacks right to privacy – prefer U.S. government definitions, not the rest of the world's

Donohue 15 – Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law (Lauren, HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY, Symposium Articles, 4 Am. U. Bus. L. Rev. 11 p.42, 2015, Hein Online)//JJ

1. Residual Rights in Third Party Data

One central question that divides the United States from numerous other countries and regions-including the European Union-centers on who owns an individual's data. In the United States, since Smith v. Maryland (addressing pen registers and trap and trace devices), and U.S. v. Miller (focusing on financial records), all three branches have treated information held by third parties as lacking an individual right to privacy.

In contrast, the EU considers that the individual who has provided data to a third party to still have a privacy interest in the information. The recent European Court decision, recognizing the right to anonymity, necessarily presupposes a continued interest in data, even once it is obtained by a third party.

Excludes zero day vulnerabilities

Undermining encryption isn't a surveillance program

Greene and Rodriguez 14 — David Greene is an EFF Senior Staff Attorney, and Katitza Rodriguez is an EEF International Rights Director (David and Katitza, “NSA Mass Surveillance Programs - Unnecessary and Disproportionate”, Electronic Frontier Foundation, May 29, 2014//DM)

BULLRUN

- Not in and of itself a surveillance program, BULLRUN is an operation by which the NSA undermines the security tools relied upon by users, targets and non-targets, and US persons and non-US persons alike. The specific activities include dramatic and unprecedented efforts to attack security tools, including:
 - Inserting vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets;
 - Actively engaging US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs;
 - Shaping the worldwide commercial cryptography marketplace to make it more vulnerable to the NSA's surveillance capabilities;
 - Secretly inserting design changes in systems to make them more vulnerable to NSA surveillance, and
 - Influencing policies, international standards, and specifications for commercial public key technologies.

Alternative – Reasonable Suspicion

Reasonable suspicion with oversight solves the case but avoids terrorism

Sievert 14 * Professor, Bush School of Government and U.T. Law School, author of three editions of Cases and Materials on US Law and National Security (Ronald, “Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978”, National Security Law Journal Vol. 3, Issue 1 – Fall 2014)//GK

Although the author believes this reasonable suspicion standard should apply to all FISA interceptions, the most urgent need, and the one that may be most favorably considered by Congress, relates to the monitoring of Al Qaeda, ISIS (the Islamic State of Iraq and Syria, also known as “ISIL”) and those who are attempting an attack with a WMD. Therefore, FISA should be changed to allow interception where there is reasonable suspicion to believe the target is a person subject to an AUMF or engaged in an effort to employ a WMD in the United States or against U.S.

facilities. Harvard Law professor Jack Goldsmith argued when he was head of the Office of Legal Counsel in 2003 that both the AUMF as well as the concept of special needs should permit the President to monitor Al Qaeda without going through the traditional requirements of the FISA statute. 272 His argument was later supported by the wording of Hamdi v. Rumsfeld, stating that the AUMF

allowed the President to utilize all necessary elements of military force against Al Qaeda and the Taliban.²⁷³ Surely, monitoring the enemy is one such element of military force. Goldsmith's position is strongly opposed by those who state that FISA requires the President to follow the procedures established by Congress and not act without FISA court approval.²⁷⁴ But assuming Congress can intrude on the President's authority in this area, there is nothing preventing Congress from amending the FISA statute to provide for more efficient interception when the target is the subject of an AUMF or planning a WMD attack. Abandoning probable cause would certainly raise legal concerns similar to those expressed in United States v. Truong²⁷⁵ and by the petitioners in In Re Sealed Case,²⁷⁶ if the intent and direct result was ordinary criminal prosecution as opposed to intelligence collection. At the same time, an interception intended to obtain intelligence is likely to pick up evidence of national security crimes (sabotage, terrorism, espionage). The government should be able to use this evidence under the doctrine that the government can use anything it finds while it is legally present.²⁷⁷ The solution in part would be to draw upon the 2001 FISA Court's practice and prohibit criminal division direction and control of intelligence wiretaps. In addition, as Judge Posner has suggested, "the use of intercepted information for any other purpose other than investigating (or prosecuting) threats to national security would be forbidden. Information could not be used as evidence or leads in the prosecution of ordinary crime."²⁷⁸ Finally, if the government thought it was likely to uncover criminal acts other than national security crimes, it would be wise in those few cases to go the extra step and seek to demonstrate probable cause instead of reasonable suspicion before obtaining a judicial warrant. Any public fears regarding the creation of a new FISA could be assuaged by establishing an independent body to look after the concerns of the civilian community. We have seen such entities in Germany's G-10 committee, the U.K.'s Interception of Communications Commission, and Italy's Data Protection Authority. These organizations perform a variety of roles, from reviewing all surveillance after the fact to issuing reports to the legislature, or, in some cases, examining individual allegations of excessive surveillance. An American version of this independent body would exist alongside the judiciary, which would grant the initial interception warrant based on a finding of reasonable suspicion. Any objective individual who steps back and reviews the series of attempted attacks on the United States in the last fifteen years understands our population is in great danger, and this is especially so if our adversaries obtain some type of WMD. It is folly to hamstring our intelligence services by imposing a criminal law search standard that is neither constitutionally required nor mandated by the recognized human rights principles of the international community. It is imperative, therefore, that we correct the mistakes of the past and enact a new, more effective Foreign Intelligence Surveillance Act.

A reasonable suspicion standard solves better than probable cause – protects privacy and avoids terrorism

Sievert 14 * Professor, Bush School of Government and U.T. Law School, author of three editions of Cases and Materials on US Law and National Security (Ronald, "Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978", National Security Law Journal Vol. 3, Issue 1 – Fall 2014)//GK

The analysis above, however, strongly suggests that a statute authorizing intelligence surveillance warrants based on reasonable suspicion alone would and should pass constitutional muster. Time and again the Supreme Court has recognized that detailed searches can be conducted without establishing probable cause, even when the results of those searches could, as with intelligence surveillance, potentially result in criminal prosecution. Such a statute would insure that the government's overwhelming interest in safeguarding our population would be met far better than it is now with the obstacles created by the burdensome FISA standard of probable cause. Privacy would be protected by a warrant process guaranteeing judicial control and guidance so that surveillance could not be initiated for political, partisan, or personal reasons, and by the need to demonstrate there was reasonable suspicion, or

specific articulable facts to suspect a specific target. Congress overreacted when it imposed the highest criminal law search standard on foreign intelligence surveillance and the result of their decision has proven hazardous to the American people. Meanwhile, OUR European allies have demonstrated a civilized respect for individual privacy but, as will be discussed in the next section, many recognize that imposing such hurdles is far too dangerous when it comes to protecting a nation's security.

Privacy/Tyranny Advantage Answers

Corporate records are a greater threat to privacy

John McLaughlin teaches at the Johns Hopkins School of Advanced International Studies. He was deputy director and acting director of the CIA from 2000 to 2004, January 2, 2014, Washington Post, "NSA Intelligence-Gathering Programs Keep us Safe," http://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html

Regarding outrage over the NSA's collection of telephone calling records, or metadata, I don't know why anyone would have greater confidence in this information being held by private companies. And given the perceived threat to privacy, it's astonishing how little attention has been paid to the Senate commerce committee's recent report on companies that gather personal information on hundreds of millions of Americans and sell it to marketers, often highlighting people with financial vulnerability. Some companies group the data into categories including "rural and barely making it," "retiring on empty" and "credit crunched: city families." The aim is often to sell financially risky products to transient consumers with low incomes, the report found. That's a real scandal — and a universe away from the NSA's ethical standards and congressional oversight. The NSA, of course, is not perfect. But it is less a victim of its actions — the independent commission appointed by President Obama found no illegality or abuses — than of the broad distrust of government that has taken root in the United States in recent decades. Studies by Pew and others show distrust of government around 80 percent, an all-time high.

NSA sees way less than 1% of web traffic

MailOnline, August 12, 2013

NSA claims it only reviews.00004 percent of Internet traffic on a daily basis, <http://www.dailymail.co.uk/news/article-2390604/NSA-claims-reviews-00004-percent-Internet-traffic-daily-basis.html>

The National Security Agency made the claims in a rare, publicly-released document defending its surveillance programs. The seven-page document was released late Friday. NSA denies claims that it has used foreign partners to circumvent U.S. laws The NSA has claimed in a publicly-released document that it only reviews.00004% of Internet traffic on a daily basis. The seven-page document, titled 'The National Security Agency: Missions, Authorities, Oversight and Partnerships,' was released late Friday. It compares the amount of Internet data that the NSA collects to the size of a dime on a basketball court. According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that,' the agency states. 'However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission - that's less than one part in a million. 'Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.' The NSA denies claims that it has used foreign partners to get around U.S. laws.

No US citizens, even those living abroad, are subject to warrantless surveillance

Asia Tribune, April 25, 2014, <http://www.asiantribune.com/node/79305>

An internal (US) National Security Agency (NSA) document perfected April 16 and yet to attract the attention of those who are very much interested in Washington's domestic and foreign surveillance network reveals the manner in which the vast and extensive spy network is managed and executed. The document, which Asian Tribune read in entirety, reveals that no US citizen is subject to NSA surveillance, whether the citizen is within the borders of the United States or abroad. Even if the American citizen living in a foreign country - possibly in his country of birth - is very much involved in that country's defense, national security or foreign affairs, areas the NSA is much interested on behalf of the US administration, under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the NSA is prohibited from bringing him under surveillance.

Government can't indiscriminately sift through data

The Christian Science Monitor, July 22, 2013, How will Obama defend secret NSA program in court? Letter offers clue.; The ACLU is challenging the NSA's secret data-collection program in court. The Obama administration responded with a letter making its case for why the program is constitutional and necessary, <http://www.csmonitor.com/USA/Justice/2013/0722/How-will-Obama-defend-secret-NSA-program-in-court-Letter-offers-clue>

The Justice Department disagrees with those assessments. The letter, by David Jones, an assistant US attorney, argues that the program's checks and balances are adequate. For example, the government may not eavesdrop on anyone's phone calls or record anything participants say. All it can do is collect phone numbers making and receiving certain calls, as well as the date, time, and duration of each call - the so called "metadata." Even then, the letter continues, "the Government is prohibited ... from indiscriminately sifting through the data. The data-base may only be queried for intelligence purposes by NSA analysts where there is a reasonable, articulable suspicion ("RAS"), based on specific facts." If the government wants to take a closer look, any data gleaned must be associated with people or phone numbers already identified and approved by the secret Foreign Intelligence Surveillance Court. In 2012, the letter revealed, the court approved fewer than 300 "query terms" that would allow intelligence analysts to pursue a phone call further. These protocols are overseen by the Justice Department and intelligence officials, and congressional intelligence committees are briefed regularly. "Thus, the program has been approved and is rigorously overseen by all three branches of the Government." For these reasons, the program " is fully consistent with the Fourth Amendment," states the letter. "Most fundamentally, the program does not involve 'searches' of plaintiffs' persons or effects, because the collection of ... metadata from the business records of a third-party telephone service provider, without

collecting the contents of plaintiffs' communications, implicates no 'legitimate expectation of privacy' that is protected by the Constitution."

Extensive oversight of surveillance programs

Deputy Attorney General James **Cole July 31, 2013**, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs" <https://www.hsl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

JAMES COLE: Thank you, Mr. Chairman, Mr. Ranking Member, members of the committee, for inviting us here today to speak about the 215 business records program and section 702 of FISA.

With these programs and other intelligence activities, **we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties.** We believe **these two programs have achieved the right balance. First of all, both programs are conducted under public statutes passed and later reauthorized by Congress.** Neither is a program that has been hidden away or off the books. In fact, all three branches of government play a significant role in the oversight of these programs. The judiciary, through the Foreign Intelligence Surveillance Court plays a role in authorizing the programs and overseeing compliance. The executive branch conducts extensive internal reviews to ensure compliance. And Congress passes the laws, oversees our implementation of those laws and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. **The 215 program involves the collection of metadata from telephone calls.** These are telephone records maintained by the phone companies. **They include the number the call was dialed from, the number the call was dialed to,** the date and time of the call and the length of the call. The records do not include the names or other personal identifying information. **They do not include cell site or other location information. And they do not include the content of any phone calls.** These are the kinds of records that under long-standing Supreme Court precedent are not protected by the Fourth Amendment. **The short court order that you have seen published in the newspapers only allows the government to acquire the phone records. It does not allow the government to access or use them.** The terms under which the government may access or use the records is covered by another, more detailed court order that the DNI declassified and released today. That other court order, called the primary order, provides that the government can only search the data if it has reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations. **The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented.** The

document of the analyst's justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance. In the criminal context, the government could obtain the same types of records with a grand jury subpoena without going to the court. But here we go to the court every 90 days to see the court's authorization to collect the records. In fact, since 2006 the court has authorized the program on 34 separate occasions involving 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems. And if there have been, the court will take a very hard look and make sure that we have corrected those problems. As we have explained before, the 11 judges on the FISA court are far from a rubber stamp. Instead, they review all of our pleadings thoroughly, they question us. And they don't approve an order until they are satisfied that we have met all statutory and constitutional requirements. In addition to the judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with the 215 programs, we would report those to the two committees right away. Any significant interpretations by the FISA court would likewise be reported to the committees under our statutory obligations, including opinions of any significant interpretation, along with any of the court orders that go with that. In addition, Congress plays a role in reauthorizing the provision under the -- under which the government carries out this program, and has done so since 2006. Section 215 of the Patriot Act has been renewed several times since the program was initiated, including most recently for an additional four years in 2011. In connection with those recent renewals, the government provided a classified briefing paper to the House and Senate Intelligence Committees, to be made available to all members of Congress. The briefing paper, and a second updated version of it, set out the operation of the programs in detail, explained that the government and the FISA court had interpreted the Section 215 authorization to authorize bulk collection of telephone metadata and stated that the government was in fact collecting such information. The DNI also declassified and released those two paper today. We also made offers to brief any member of the 215 program. And the availability of the paper and the opportunity for oral briefings were communicated through dear colleagues letters issued by the chairs of the intelligence committees to all members of Congress. Thus, although we could not talk publicly about the program at the time, since it was properly classified, the executive branch took all reasonable, available steps to ensure that members of Congress were appropriately informed about the programs when they renewed it. I

Surveillance programs are minimal invasions of privacy and prevent terrorism

Senator Dianne Feinstein, 10-20-, 13, USA Today,
<http://www.usatoday.com/story/opinion/2013/10/20/nsa-call-records-program-sen-dianne-feinstein-editorials-debates/3112715/>

The call-records program is not surveillance. It does not collect the content of any communication, nor do the records include names or locations. The NSA only collects the type of information found on a telephone bill: phone numbers of calls placed and received, the time of the calls and duration. The Supreme Court has held this "metadata" is not

protected under the Fourth Amendment. This program helps "connect the dots" — the main failure of our intelligence before 9/11. Former FBI director Robert Mueller and Director of National Intelligence James Clapper testified that if this program existed before 9/11, it likely would have identified the presence inside the U.S. of hijacker Khalid al-Mihdhar.**The NSA uses these records to identify connections between known and suspected terrorists (as well as terror conspirators and supporters). The overwhelming majority of records are never reviewed before being destroyed, but it is necessary for the NSA to obtain "the haystack" of records in order to find the terrorist "needle."** Only a strictly limited number of NSA analysts (among the thousands of professionals at the agency) may search the phone records database and only after articulating a specific reason that must be approved by a senior official. Those decisions are reviewed regularly by the Justice Department, Congress and the Foreign Intelligence Surveillance Act (FISA) Court, which imposes strict privacy protections.**To be effective, the NSA must be able to conduct these queries quickly, without regard to which phone carrier a terrorist or conspirator uses. And the records must be available for a few years — longer than phone companies need them for billing purposes.** Since its inception, this program has played a role in stopping roughly a dozen terror plots and identifying terrorism supporters in the U.S. Given the threats we face from al-Qaeda and others, we need all legal tools at our disposal.**The Senate Intelligence Committee will soon consider legislation to add public reporting requirements and more court review, and to codify existing procedures into law. I hope this will restore public confidence to a program that continues to protect the homeland from terrorism.**

People voluntarily give up the data, the government just uses it for public safety

Olivier Sylvain, 2014, Associate Professor, Fordham University School of Law, Summer Wake Forest Law Review, FAILING EXPECTATIONS: FOURTH AMENDMENT DOCTRINE IN THE ERA OF TOTAL SURVEILLANCE,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473101, DOA: 1-24-15, p. 491-2

These firms, meanwhile, assume that the benefits of large-scale data aggregation and sorting far exceed any of the disadvantages. **Google and Facebook have developed algorithms that analyze the finest details of users' online behavior and send targeted advertisements to those users based on that information.** Users do not seem particularly bothered by disclosures because they continue to acquire applications that know or predict their tastes before they even know what they want.

C. Paradoxes in Expectation

Private companies are not the only entities that trade and share users' personal online information. **Governments, too, are in the business of collecting and analyzing personal data, and sometimes purchasing them.** Their reasons, however, are different. **Federal, state, and local agencies generally rely on the interests in national security, law enforcement,** and public safety. Emergent surveillance technologies are perfectly suited to achieving these public ends. Properly designed algorithms can help to search online data for possible wrongdoing and even anticipate lawlessness.

What has emerged, then, is a government-industry partnership that, on the one hand, counts on users' demonstrable willingness to share personal information with data brokers and, on the other hand, furthers the government interest in public safety. This is not a devious plan that was hatched in some dark, shadowy office on Capitol Hill or at Fort Meade, although it sometimes feels that way. The Internet's early designers and proponents did not have total surveillance in mind. To the contrary, the early designers sought to avert centralized control, placing the intelligence of the network at the "ends" with users.

The Internet changed quite dramatically after Congress formally commercialized it in the mid-1990s. Indeed, **since then, total surveillance has become its defining characteristic.** Today, **the most popular service providers, sites, and applications have designed sophisticated techniques for aggregating and sharing as much data about each and every visitor as legally possible.**

And users have been complicit at every step, divulging all manners of information in order to receive the full benefits of the networked information economy. They volunteer their personal information to service providers and application developers and, whether they know it or not, allow those companies to monitor and trade this information with third parties.

Court has upheld the collection of call metadata because Americans have no expectation of privacy in dialing phone numbers

Washington Post, April 25, 2014, http://www.washingtonpost.com/world/national-security/surveillance-court-rejected-verizon-challenge-to-nsa-calls-program/2014/04/25/78d430c2-ccc2-11e3-93eb-6c0037dde2ad_story.html

Verizon in January filed a legal challenge to the constitutionality of the National Security Agency's program that collects billions of Americans' call-detail records, but a surveillance court rejected it, according to newly declassified documents and individuals with knowledge of the matter. **In denying the phone company's petition** in March, Foreign Intelligence Surveillance Court **Judge Rosemary M. Collyer embraced the arguments put forth by the government that the program is constitutional in light of a Supreme Court decision in 1979 that Americans have no expectation of privacy in dialing phone numbers.**

Fourth Amendment Answers

Metadata collection doesn't violate the Fourth Amendment because it is part of national security authority

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,

<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15,

p. 901

Controversy has arisen again over the federal government's electronic surveillance efforts to gather intelligence on foreign terrorist groups. Recent disclosures, both authorized and illicit, have described two secret National Security Agency (NSA) programs. The first collects telephone "metadata" such as calling records--but not the content of phone calls--both inside and outside the United States. A second NSA program intercepts the e-mails of non-U.S. persons outside the United States. Despite the claims of critics, these programs do not violate the Foreign Intelligence Surveillance Act (FISA), as recently amended by Congress, or the Fourth Amendment to the Constitution. Concerns about the proper balance between these surveillance programs and individual privacy may be appropriate, but these programs properly fall within the province of Congress and the President to set future national security policy.

Donahue is wrong – it's constitutional

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,

<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15,

P. 917-8

Another article in this Issue of the *Journal* challenges the constitutionality of the NSA's bulk collection program. In her article, Professor Laura Donohue calls into question the applicability of Smith v. Maryland to the NSA's bulk metadata collection. She argues that the telephone metadata system "is an entirely different situation" from that in Smith. In distinguishing *Smith* from the NSA's metadata program, Professor Donohue argues that, unlike the police placing a pen register on a single caller whom the police suspect of criminal behavior, "[t]he NSA is engaging in bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, almost all of the information obtained will bear no relationship whatsoever to criminal activity." In addition to questioning the applicability of *Smith*, Professor Donohue illustrates the recent tensions that have emerged between the Fourth Amendment and the government's ever-increasing

use of new technologies. Under the trespass doctrine, Professor Donohue argues that the NSA's metadata collection "amounts to a general warrant--the elimination of which was the aim of the Fourth Amendment." Therefore, as Professor Donohue concludes, the collection of bulk metadata is "a digital trespass on individuals' private spheres." **There are several flaws with Professor Donohue's analysis. Most notably, the Smith Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.** It makes no difference--notwithstanding Professor Donohue's argument--whether the government collects a single suspect's metadata, as in *Smith*, or thousands of callers' metadata, the vast majority of whom are not suspected of any wrongdoing. The point remains the same: **individuals lose their expectation of privacy the moment they voluntarily reveal information to third parties.** To use the words of Judge Eagan: "[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals **cannot result in a Fourth Amendment interest springing into existence ex nihilo.**" **Moreover**, though Professor Donohue is correct that tensions have emerged between the Fourth Amendment and the government's use of technology, she nevertheless misapplies the trespass doctrine to the NSA's metadata collection. **Unlike Jones, Kyllo, or Jardines, the government collection of individuals' metadata does not amount to a trespass or infringe onto their private digital sphere. Indeed, as the Court has emphasized in Katz and Smith, a digital trespass will not occur when one voluntarily turns his or her information over to third parties to see.**

Metadata collection is constitutional

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 916

A. Metadata Collection and Third-Party Doctrine

Even if Congress and the President have sufficient statutory authority to carry out the NSA programs, they may still violate the Constitution. A government decision may satisfy the structural provisions of the Constitution--such as the separation of powers and federalism--yet still run afoul of the Bill of Rights. This part measures the two NSA programs against the primary individual right at stake: the Fourth Amendment's protection against unreasonable searches and seizures. It concludes that both **the telephone metadata and the foreign e-mail collection programs**, as currently described by the Obama administration, **do not violate the Fourth Amendment.** The NSA's first program, which collects metadata on domestic phone calls, poses the fewest constitutional difficulties. Under existing judicial doctrine, **individuals have Fourth Amendment rights in the content of communications, but not in their addressing information. Privacy does not extend to the writing on the outside of envelopes deposited in the mail because the sender has voluntarily revealed the addresses to the post office for delivery. An identical principle applies to telecommunications. In Smith v. Maryland, the Supreme Court found calling information, such as the phone number dialed, beyond Fourth Amendment protection because the consumer had voluntarily turned over the information to a third party**

-- namely, the phone company -- for connection and billing purposes. Under the rubric of *Katz v. United States*, no one can have an expectation of privacy in records that they have handed over to someone else. In recent cases, however, the Court has turned a skeptical eye toward new search technologies. In *Kyllo v. United States*, for example, the Court held that

thermal imaging of homes qualified as a search under the Fourth Amendment, even though the police used the imaging device from a public street. In *United States v. Jones*, the Court found that the Fourth Amendment required a warrant for the installation of a global positioning service tracker on a car. These cases turn on the means by which the government conducts a search in a place protected by the Fourth Amendment. In *Kyllo*, the Court believed that thermal imaging verged on a physical search of a home, while *Jones* involved physical intrusion into a private car. Neither holding calls into doubt the loss of Fourth Amendment rights when an individual voluntarily hands over information to a third party. In other words, the information sought by the NSA programs would require a warrant to be searched if it remained within the home or personal computing devices. As a result, the Constitution does not require a warrant for a pen register because no electronic interception or surveillance of the content of the calls has occurred. Meanwhile, the data collected is potentially of enormous use in frustrating al Qaeda plots. If U.S. agents are pointed to members of an al Qaeda sleeper cell by a domestic phone number found in a captured al Qaeda leader's cell phone, call pattern analysis would allow the NSA quickly to determine the extent of the network and its activities. The NSA, for example, could track the sleeper cell as it periodically changed phone numbers. This could give a quick, initial, database-generated glimpse of the possible size and activity level of the cell in an environment where time is of the essence. A critic might respond that there is a difference between a pen register that captures the phone numbers called by a single person and a database that captures all of the phone numbers called by everyone in the United States. The Supreme Court, however, has never held that obtaining billing records would somehow violate privacy merely because of a large number of such records.

Surveillance State Frontline

The surveillance state is too pervasive. All branches and agencies, plus corporations, exercise biopower over the people; NSA only reform will fail.

Whitehead, 5-16-15 [John, constitutional and human rights attorney, and founder of the Rutherford Institute, "The NSA's Technotyranny: One Nation Under Surveillance," WashingtonsBlog, 5-16-15, <http://www.washingtonsblog.com/2015/05/the-nsas-technotyranny-one-nation-under-surveillance.html>]

The National Security Agency (NSA) has been a perfect red herring, distracting us from the government's broader, technology-driven campaign to render us helpless in the face of its prying eyes. In fact, long before the NSA became the agency we loved to hate, the Justice Department, the FBI, and the Drug Enforcement Administration were carrying out their own secret mass surveillance on an unsuspecting populace. Just about every branch of the government—from the Postal Service to the Treasury Department and every agency in between—now has its own surveillance sector, authorized to spy on the American people. Then there are the fusion and counterterrorism centers that gather all of the data from the smaller government spies—the police, public health officials, transportation, etc.—and make it accessible for all those in power. And of course that doesn't even begin to touch on the complicity of the corporate sector, which buys and sells us from cradle to grave, until we have no more data left to mine. The raging debate over the fate of the NSA's blatantly unconstitutional, illegal and ongoing domestic surveillance programs is just so much noise, what Shakespeare referred to as "sound and fury, signifying nothing." It means nothing: the legislation, the revelations, the task forces, and the filibusters. The government is not giving up, nor is it giving in. It has long since ceased to take orders from "we the people."

NSA surveillance isn't analogous to Foucault's Panopticon. At best, reactions to rather than applications of surveillance are comparable.

McGraw, '13 [Bryan, Associate Professor of Politics at Wheaton College, "How NSA Surveillance is NOT Like Foucault (but our reactions are)," Civitas Peregrina, June 11, 2013, <https://civitasperegrina.wordpress.com/2013/06/11/how-nsa-surveillance-is-not-like-foucault-but-our-reactions-are/>]

It's easy to see why we might then jump from the NSA's Prism program to Foucault. But here's what makes Foucault's argument interesting and not just some obtuse forerunner of the "X Files" (or any other conspiracy minded move/tv show). One of the panopticon's key features was that the tower where the guards resided was mirrored so that the prisoners could not tell if they were actually under observation at any particular moment. In fact, they need not be under observation at all for the tower to do its job. Foucault's view was that our liberal society was indeed one of deep disciplining, but it was not the case that there was a "them" that was doing the disciplining. Rather, we all are caught up and participate in our mutual disciplining. We are, to Foucault's mind, our own oppressors in that we impose a kind of "normalization" on one another. What the NSA=Foucault folks suppose is that Foucault had in mind a social order in which some small elite, armed with technologies and power, would herd the rest of us into docile compliance. Foucault's argument was actually much more worrisome: that all of us, armed with the ordinary technologies of communication and observation, would herd ourselves into docile submission. So the NSA program (whatever its merits and demerits) isn't Foucauldian. Rather, I would argue, it is our reactions—where commentators assume their expected positions, offer ritualized expressions of support or outrage, and punish (via dialogue) those who range outside the bounds of "proper" discourse—that reminds me of Foucault.

Alternative Causality: the modern Imperial Presidency is the root cause of Foucauldian biopower.

Smith, '13 [Reid, Freedom Works' staff writer and editor, "The Surveillance State in Your Head," The American Conservative, July 19, 2013,
<http://www.theamericanconservative.com/articles/the-surveillance-state-in-your-head/>]

With the fall of the Soviet Union, there was hope that the imperial presidency would be scaled back by Congress, but such optimism proved hollow. In The Cult of the Presidency, Gene Healy notes that while partisan rhetoric today is as acerbic as it has been in decades, Republicans and Democrats alike accept the bottomless depth of executive responsibility and the president's unique grasp on power. We've normalized dependence on his guidance and our subordination. The modern president has greatly exceeded, in size and scope, the few enumerated powers initially bestowed upon him and in the process has become a great deal more powerful—and potentially more dangerous. His powers of surveillance and social compulsion are virtually unmatched in human history. From a Foucauldian perspective, one might argue our president (Bush or Obama, it hardly matters) has staked his claim as our watchman. We become increasingly aware that all we do takes place under surveillance, and our dull surprise at this revelation suggests our submission to the system—the inevitable outcome of our assent to political power.

Foucauldian critique of NSA surveillance is impossible under modern capitalism. Current power structures are self-reinforcing.

Bruno, '14 [Zachary, BA, Critical Theory, Occidental College, "The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden," March 24, 2014,
<http://www.zachcbruno.com/academic/dd-preview/images/pdf/PrismProgramPanopticon.pdf>]

With this, Foucault would propose that critiquing the NSA's illicit surveillance program would first require deconstructing the structures of power and discursive claims making which surround it. In this regard, Reeves (2003) argues that a self-reinforcing dynamics exists, as it pertains to the discourses and power structures sustaining such governmental tools. In this regard, the difficulty of critiquing them, in the sense which Foucault (1995) intends, is related to the manner in which this power is self-reinforcing. Indeed, to garner a better understanding of the difficulties of critique in such a context, one need only examine Foucault's work on sexuality, repression, and biopolitics-based social control to understand the operation of these mechanisms. With the above in mind, what becomes most apparent, from considering Foucault's portrayal of the diffusion of normalizing power in contemporary society, is that it is impossible to resist the potency of this power from within modern society itself. Given that the latter is permeated with multiple structures of repression, often invisible to the human eye, or already internalized to such a degree that we are no longer capable of even recognizing their existence; it becomes clear that we live in a social context in which resistance through critique, within society, is at least temporarily impossible. If a social revolution were to ever undo the structures of normalizing power which currently permeate our social interactions, it might become possible to rebuild a society without the concentrations of capital, and thus power, which prevail today. In the interim, however, resisting and informally critiquing within the confines of organized modern capitalist society is a futile endeavor because of the all-too-deep entrenchment of those entities which regulate us, and force us to adopt certain behaviors in spite of our desires. Thus, because the entirety of our society has been permeated by these powerful exogenous forces, there is no true potential for resistance within society. Instead, because we cannot necessarily understand or confront all of the elements of our oppression, it is clear that resistance to the forces identified by Foucault must take place outside of mainstream society. On this basis, critique of the everyday colloquial variety is impossible simply because it necessitates that we accept and take for granted the imposed structures of meaning which emerge from society's most significant power bases.

The American populace cannot engage in Foucauldian critique of NSA surveillance because of disciplinary structures like the War on Terror.

Bruno, '14 [Zachary, BA, Critical Theory, Occidental College, "The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden," March 24, 2014, <http://www.zachcbruno.com/academic/dd-preview/images/pdf/PrismProgramPanopticon.pdf>]

Applied to the context of the NSA's surveillance Panopticon, the ultimate reality of the impossibility of critique is one wherein it is impossible for the American mass to understand the multiple structures of oppression inherent to the PRISM Program. Indeed, the apathy discussed by Zurchner (2014) is likely an embodiment of a context wherein the American population is blinded by the other disciplinary structures, like the purported threats of the War on Terror, which serve to maintain high levels of fear in American society. In this regard, the work of Lokaneeta (2010) suggests that these, associated with the notion of American governmentality, have preponderated in the post-9/11 context because of the visceral power of the discourse of threat which the Bush and Obama Administrations have spread.

Extension – Alt Causes to Panopticism

The Foucaldian Panopticon is inherent to a myriad of government agencies. Restricting NSA based surveillance is too narrowly based to succeed.

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

The Panopticon is real. It siphons billions of dollars each year from a federal budget in crisis. And it **is watching you** and your children. **Lost in the debate about NSA spying**, however — **and** even most public **resistance to it** — **have been** the various **other federal agencies** also **complicit in Fourth Amendment abuses**. Even **critics of domestic surveillance have** largely **failed to recognize how many government agencies spy on Americans**. A presidential review panel recently recommended substantial changes to FBI powers, including ending the authority to issue National Security Letters. NSLs are secret data requests used to circumvent both First and Fourth Amendment protections, demanding information about third parties and gagging the recipients. **The FBI’s pattern of abusing undercover infiltration** to disrupt First Amendment protected organizations, however, stretches back decades, threatens democracy even more deeply than NSLs, and **continues unabated**. **Beyond the NSA and FBI, many other agencies are** also **involved in domestic surveillance**. **And** all of them **continue to evade** public and congressional **scrutiny**.

Federal agencies other than NSA are complicit in maintaining the Panopticon.

A. Department of Homeland Security:

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

The Department of Homeland Security (**DHS**) is a sprawling behemoth, with nearly a quarter million employees scattered across nearly two dozen component agencies. **While purporting to protect the “homeland”** (a term with loaded connotations worth noting, but setting aside for now) from various threats, **DHS spies on Americans** in several disturbing ways. Some of **the most dystopian** piggyback on **programs** presented to the public as supporting immigration enforcement. Border security agencies, like Customs & Border Protection (CBP) and Immigration & Customs Enforcement (ICE), have **facilitated a record number of deportations** under the Obama administration, creating a domestic humanitarian crisis. Critics of the administration’s immigration crackdown have vocally challenged its failures. According to the New York Times, “**the department’s** continually shifting **strategies** against illegal immigration had two things in common. They **were ineffective and cruel**.”

B. Postal Service:

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

Nor are law enforcement agencies the only ones joining the intelligence agencies to spy on Americans. **Even the US Postal Service is getting in on the surveillance racket.** In July, the New York Times reported on the Mail Isolation Control and Tracking program, “in which **Postal Service computers photograph the exterior of every piece of paper mail** that is **processed in the United States** — about 160 billion pieces last year...” It concluded that “**postal mail is subject to the same kind of scrutiny that the National Security Agency has given to telephone calls and e-mail.**” Like the NSA’s ubiquitous electronic wiretapping, **postal surveillance carries disturbing implications,** particularly in terms of **enabling** the **suppression of political dissent.** Most astounding in the context of the controversy over NSA spying, however, is the sheer ignorance about the postal service’s monitoring practices.

C. State and local law enforcement:

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

DHS also erodes constitutional rights through its collaborations with local police. **State and local law enforcement agencies around the country collaborate with** a series of over **70 regional** DHS-funded **fusion centers** pursuing ambiguous missions at unknown costs. DHS leaders have praised fusion centers, but critics — extending from the libertarian CATO Institute and immigrant rights groups to FBI veterans — have described them as wasteful, duplicative, constitutionally offensive, and ineffective from a public safety standpoint. **Targeted surveillance**, of the sort abused by the FBI, **is also a problem across state & local departments.** For years, peace activists, Ron Paul supporters, environmentalists, and Muslims have been targeted for government spying in dozens of states—not only by the FBI, but also by state and local police. Until being shut down by the Governor in 2010, Pennsylvania state officials not only spied on environmental activists, but also shared its intelligence reports with their corporate targets, including mining companies. **DHS also facilitates** the **paramilitarization of local and state police agencies**, which around the country have sought DHS grants to buy everything from sophisticated listening devices to surveillance cameras, automated drivers license plate scanners developed originally for military uses, aerial surveillance drones, and even armored tanks.

A2: Authoritarianism

The claims about authoritarianism are hyperbolic and paranoid. All law enforcement practice might be used improperly, but accountability checks the worst practices.

Simon, 2014,

William H. Simon, Arthur Levitt Professor of Law at Columbia University, 10-20-2014, "Rethinking Privacy," Boston Review, <http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance>

The third trope of the paranoid style is the slippery slope argument. The idea is that an innocuous step in a feared direction will inexorably lead to further steps that end in catastrophe. As The Music Man (1962) puts it in explaining why a pool table will lead to moral collapse in River City, Iowa, "medicinal wine from a teaspoon, then beer from a bottle." In this spirit, Daniel Solove in Nothing to Hide (2011) explains why broad surveillance is a threat even when limited to detection of unlawful activity. First, surveillance will sometimes lead to mistaken conclusions that will harm innocent people. Second, since "everyone violates the law sometimes" (think of moderate speeding on the highway), surveillance will lead to over-enforcement of low-stakes laws (presumably by lowering the costs of enforcement), or perhaps the use of threats of enforcement of minor misconduct to force people to give up rights (as for example, where police threaten to bring unrelated charges in order to induce a witness or co-conspirator to cooperate in the prosecution of another). And finally, even if we authorize broad surveillance for legitimate purposes, officials will use the authorization as an excuse to extend their activities in illegitimate ways. Yet, slippery slope arguments can be made against virtually any kind of law enforcement. Most law enforcement infringes privacy. ("Murder is the most private act a man can commit," William Faulkner wrote.) And most law enforcement powers have the potential for abuse. What we can reasonably ask is, first, that the practices are calibrated effectively to identify wrongdoers; second, that the burden they put on law-abiding people is fairly distributed; and third, that officials are accountable for the lawfulness of their conduct both in designing and in implementing the practices.

Surveillance doesn't harm freedom or autonomy, because they aren't reliant on digital communication.

Sagar, 2015

Rahul, associate professor of political science at Yale-NUS College and the Lee Kuan Yew School of Public Policy at the National University of Singapore. He was previously assistant professor in the Department of Politics at Princeton University., "Against Moral Absolutism: Surveillance and Disclosure After Snowden," Ethics & International Affairs / Volume 29 / Issue 02 / 2015, pp 145-159.

The second harm Greenwald sees surveillance posing is personal in nature. Surveillance is said to undermine the very essence of human freedom because the "range of choices people consider when they believe that others are watching is . . . far more limited than what they might do when acting in a private realm."¹⁶ Internet-based surveillance is viewed as especially damaging in this respect because this is "where virtually everything is done" in our day, making it the place "where we develop and express our very personality and sense of self." Hence, "to permit surveillance to take root on the Internet would mean subjecting virtually all forms of human interaction, planning, and even thought itself to comprehensive state examination."¹⁷ This claim too seems overstated in two respects. First, it exaggerates the extent to which our self-development hinges upon electronic communication channels and other related activities that leave electronic traces. The arrival of the Internet certainly opens new vistas, but it does not entirely close earlier ones. A person who fears what her browsing habits might communicate to the authorities can

obtain texts offline. Similarly, an individual who fears transmitting materials electronically can do so in person, as Snowden did when communicating with Greenwald. There are costs to communicating in such “old-fashioned” ways, but these costs are neither new nor prohibitive. Second, a substantial part of our self-development takes place in public. We become who we are through personal, social, and intellectual engagements, but these engagements do not always have to be premised on anonymity. Not everyone wants to hide all the time, which is why public engagement—through social media or blogs, for instance—is such a central aspect of the contemporary Internet.

A2: Tyranny

The argument that NSA surveillance enables tyranny is wrong. The data exists inevitably and if you are concerned about the risk of a tyrant taking over, there are much bigger issues than privacy to be concerned about.

Etzioni, Professor of International Relations at the George Washington University, 2014

Amitai Etzioni , Intelligence and National Security (2014): NSA: National Security vs. Individual Rights, Intelligence and National Security, DOI: 10.1080/02684527.2013.867221

Part VI: The Coming Tyrant? A common claim among civil libertarians is that, even if little harm is presently being inflicted by government surveillance programs, the infrastructure is in place for a less-benevolent leader to violate the people's rights and set us on the path to tyranny. For example, it has been argued that PRISM 'will amount to a "turnkey" system that, in the wrong hands, could transform the country into a totalitarian state virtually overnight. Every person who values personal freedom, human rights and the rule of law must recoil against such a possibility, regardless of their political preference'.¹⁷⁷ And Senator Rand Paul (R-KY) has been 'careful to point out that he is concerned about the possible abuses of some future, Hitler-like president'.¹⁷⁸ A few things might be said in response. First, all of the data that the government is collecting is already being archived (at least for short periods – as discussed above) by private corporations and other entities. It is not the case that PRISM or other such programs entail the collection of new data that was not previously available. Second, if one is truly concerned that a tyrant might take over the United States, one obviously faces a much greater and all-encompassing threat than a diminution of privacy. And the response has to be similarly expansive. One can join civic bodies that seek to shore up democracies, or work with various reform movements and public education drives, or ally with groups that prepare to retreat to the mountains, store ammunition and essential foods, and plan to fight the tyrannical forces. But it makes no sense to oppose limited measures to enhance security on these grounds.

A2: State Abuses are morally objectionable

No Ethical abuse – ethical benefits to surveillance outweigh AND inherent safeguards check

Taylor 05

[In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance James Stacey Taylor Public Affairs Quarterly Vol. 19, No. 3 (Jul., 2005), pp. 227-246 Published by: University of Illinois Press on behalf of North American Philosophical Publications Stable URL: <http://www.jstor.org/stable/40441413> //duff

It must be admitted that, in practice, a system of constant State surveillance is likely to be abused to some extent.²⁰ However, if one adopts a rights-based understanding of claim (ii) above (i.e., if one holds that such a system of State surveillance is permissible as long as it does not in itself violate persons' moral rights), this objection can be readily rebutted. On such an understanding of claim (ii) one could first note that this abuse-based objection gets its force from the view that such abuse would violate persons' moral rights. The proponent of a rights-based understanding of claim (ii) would certainly agree with this underlying view, and would join with its advocates in condemning such abuse. However, the rights theorist who was in favor of such a system of State surveillance would also note that the condemnation of the abuse of State surveillance is not to condemn State surveillance itself. To condemn the use of x for the purposes of v, where y violates persons' rights (e.g., to privacy or autonomy) is not also to condemn the use of x for the purposes of z, where z does not violate persons' rights. Thus, a rights theorist who was a proponent of State surveillance could argue, to offer the possibility of abuse as an objection to constant State surveillance is to confuse the moral status of different possible uses of such surveillance. For such proponents of State surveillance, then, this first objection can be readily dismissed. If one adopts a consequentialist understanding of claim (ii), however, defending the use of constant State surveillance against this objection is more difficult. This is because the likelihood of such abuse together with the likelihood of such abuse causing harm must be weighed against the benefits (as outlined above) that such a system is likely to provide. And, given that such a system has not yet been implemented, such a weighing and balancing of its relative costs and benefits will be difficult to assess with certainty. Despite this, however, there is good reason to believe that little harm will accrue from the abuse of such a system of surveillance. Thus, given the likelihood that such a system of State surveillance will bring important benefits to the citizens of the State in which it is installed, the possibility of its abuse should not deter consequentialists from endorsing the above pro-surveillance argument. To show why there is good reason to believe that little harm would accrue from such a system of State surveillance its consequentialist proponents should first distinguish between major abuses of such a system and minor abuses of it. A major abuse of such a system would be one in which the State used its power together with its improved surveillance capabilities to persecute or oppress its citizens, either individually or as a whole. A minor abuse of the system would be one in which some of the agents of the State secured access to the information gathered by its surveillance devices for their own nefarious purposes, such as voyeurism or the mockery of the persons whose recorded actions they are viewing. The consequentialist proponent of constant and universal State surveillance need not be unduly concerned about the possibility of major abuses of the State surveillance system. If the State were prone to abuse its citizens in this way prior to the installation of such a system, this would provide good consequentialist grounds for resisting its introduction. The consequentialist proponent of constant State surveillance is thus only concerned with defending the introduction of such a surveillance system in those cases where the State was not prone to abusing its citizens in this way. This is not to say, however, that a State (or the agents of a State) that was not prone to persecuting or oppressing its citizens might not occasionally persecute individual citizens. In response to this the consequentialist proponent of constant State surveillance should note that given its power were the State (or its agents) to decide to persecute some of its citizens in this way it would not need a system of surveillance to do this effectively. Thus, although such a surveillance system might make it easier for the State (or its agents) to engage in the persecution that it had decided upon, this would not make things any worse for the person or persons thus persecuted. As such, then, the possibility of the major abuse of a system of constant and universal State surveillance by a State that was not prone to persecuting its citizens would not, for a consequentialist, be a significant objection to the introduction of such a system. What, then, of the concern that such a system of constant State surveillance would be subject to minor abuses? The most obvious response to this concern is to argue that if such a system of surveillance is introduced then it must be accompanied by a series of safeguards that would reduce the possibility that the information that

it gathers would be abused in this way. It might, for example, be that such a system should be accompanied by the requirement that only a very few persons have access to the information that it gathers, that such persons be screened carefully and supervised closely, and that they are subject to draconian penalties for any abuses that they might perpetrate. If they were severe enough such safeguards would be likely to reduce the possibility of the minor abuse of such a system of surveillance to a level whereby the harm that its abusers might cause would be outweighed by the advantages that it would provide to the State's citizens as a whole. However, the consequentialist proponent of State surveillance also has a second - and more philosophically interesting - response to the concern that such surveillance would be subject to minor abuse: that such abuse would not be harmful, and so would not detract from the advantages outlined above. This response is based on observing that given the penalties for abuse by which such a system would be accompanied (as outlined above) any such abuse would be perpetrated covertly. As such, its victims (e.g., persons subjected to the voyeuristic gaze of some of the agents of the State) would not know that they were victims. Yet even though this is so, the proponents of this second response to the above abuse-based objection do not use this observation to argue that, since such persons did not know that they were being watched, this watching did not harm them.²¹ This is because, as Joel Feinberg has persuasively argued, the mere fact that a person is ignorant of the frustration of her interests (e.g., her interest not to be the unwilling subject of voyeurism) does not mean that she has not thereby been harmed.²² Rather, this second consequentialist response to the above abuse-based objection conjoins this observation with the claim that for a person to be harmed her life must have been adversely affected in some way, whether she knew of this or not. To support this latter claim it will be useful to examine more closely Feinberg's argument against the view that a person can be harmed only if she knows that she has been harmed. This examination will serve two purposes. First, it will show why the consequentialist proponent of constant State surveillance should not claim that the unwitting victim of (e.g.) State voyeurism failed to be harmed by it owing to her ignorance of it. Second, it will support the claim that a person's life must be adversely affected for her to be considered harmed - the claim on which this second response rests.

EXT: No Abuse of Surveillance

The NSA is well-regulated and constrained by judicial oversight.

Cohen, 2015

Michael A. Cohen, 15, fellow at The Century Foundation. Previously, Michael served in the U.S. Department of State as chief speechwriter for U.S. Representative to the United Nations Bill Richardson and Undersecretary of State Stuart Eizenstat. , 6-3-2015, "NSA Surveillance Debate Drowned Out on Both Sides by Fear Tactics," World Politics Review, <http://www.worldpoliticsreview.com/articles/15905/nsa-surveillance-debate-drowned-out-on-both-sides-by-fear-tacticsa>

The arguments of NSA opponents have, for two years, relied on hypothetical, trumped-up fears of the government ransacking our private information. These concerns have been raised even though, from all appearances, the NSA's domestic surveillance activities are reasonably well-regulated and constrained by judicial oversight. NSA opponents like to point out that a recent court decision determined that the bulk records collection program was illegal, which ignores the many other court decisions that accepted its legality. More important, it ignores the decisions of the secret FISA Court, which ordered the NSA not to scrap collection programs that were determined to be operating unconstitutionally, but rather to make changes to them to get them in line with constitutional constraints.

There's no evidence of abuse of surveillance powers.

Simon, 2013,

David Simon, producer of HBO's The Wire, 7/3/13, "We are shocked, shocked..."
<http://davidsimon.com/we-are-shocked-shocked/>

I know it's big and scary that the government wants a data base of all phone calls. And it's scary that they're paying attention to the internet. And it's scary that your cell phones have GPS installed. And it's scary, too, that the little box that lets you go through the short toll lane on I-95 lets someone, somewhere know that you are on the move. Privacy is in decline around the world, largely because technology and big data have matured to the point where it is easy to create a net that monitors many daily interactions. Sometimes the data is valuable for commerce — witness those facebook ads for Italian shoes that my wife must endure — and sometimes for law enforcement and national security. But be honest, most of us are grudging participants in this dynamic. We want the cell phones. We like the internet. We don't want to sit in the slow lane at the Harbor Tunnel toll plaza. The question is not should the resulting data exist. It does. And it forever will, to a greater and greater extent. And therefore, the present-day question can't seriously be this: Should law enforcement in the legitimate pursuit of criminal activity pretend that such data does not exist. The question is more fundamental: Is government accessing the data for the legitimate public safety needs of the society, or are they accessing it in ways that abuse individual liberties and violate personal privacy — and in a manner that is unsupervised. And to that, the Guardian and those who are wailing jeremiads about this pretend-discovery of U.S. big data collection are noticeably silent. We don't know of any actual abuse. No known illegal wiretaps, no indications of FISA-court approved intercepts of innocent Americans that occurred because weak probable cause was acceptable. Mark you, that stuff may be happening. As happens the case with all law enforcement capability, it will certainly happen at some point, if it hasn't already. Any data asset that can be properly and legally invoked, can also be misused — particularly without careful oversight. But that of course has always been the case with electronic surveillance of any kind.

Ext - -No Significant NSA Information Gathering

Phone records of citizens not scrutinized

Stuart **Taylor, April 29, 2014**, The Big Snoop: Life, Liberty, and the Pursuit of Terrorists, <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.)

The NSA argues that it needs to comb through the coordinates of as many of these conversations as possible in the hunt for the rare but critically important phone call between a foreign terrorist and a collaborator in the United States. Although it is obvious that not all foreign terrorists' phone contacts are witting participants in a conspiracy, or even aware that there is a conspiracy, Keith Alexander, the former director of the NSA, is credited with what has become a pithy defense of the proposition that more access is better and total access is best: when searching for needles in a haystack, "you need the whole haystack." Brenner believes that the Alexander Doctrine is not a cover for spying on Americans. **NSA analysts are totally fixated on foreign targets**, he stresses, **and have no interest in the private lives of U.S. citizens whose phone records are gathered**. For this and other reasons, Brenner says, **the chance of a citizen's record being scrutinized is "infinitesimal—like winning the lottery."**

NSA only generates signals intelligence when it meets specific requirements

Asia Tribune, April 25, 2014, <http://www.asiantribune.com/node/79305>

NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. **Dissemination of information about U.S. persons in any NSA foreign intelligence report is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury**. Even if one or more of these conditions apply, NSA may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically "masks" the true identities of U.S. persons through use of such phrases as "a U.S. person" and the suppression of details that could lead to him or her being successfully identified by the context. Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report if the recipient has a legitimate need to know the identity. Under NSA policy, **NSA is allowed to unmask the identity only under certain conditions and where specific additional controls are in place to preclude**

its further dissemination, and additional approval has been provided by one of seven designated positions at NSA. Additionally, together DOL and ODNI review the vast majority of disseminations of information about U.S. persons obtained pursuant to Section 702 as part of their oversight process.

NSA privacy violations minuscule

The New York Times, August 17, 2013

N.S.A. Calls Violations Of Privacy 'Minuscule', http://www.nytimes.com/2013/08/17/us/nsa-calls-violations-of-privacy-minuscule.html?_r=0, p. 12

WASHINGTON -- The top National Security Agency official charged with making sure analysts comply with rules protecting the privacy of Americans pushed back on Friday against reports that the N.S.A. had frequently violated privacy rules, after the publication of a leaked internal audit showing that there had been 2,776 such "incidents" in a one-year period. The official, **John DeLong, the N.S.A. director of compliance, said that the number of mistakes by the agency was extremely low compared with its overall activities. The report showed about 100 errors by analysts in making queries of databases of already-collected communications data; by comparison, he said, the agency performs about 20 million such queries each month.** Mr. DeLong, speaking to reporters on a conference call, also argued that **the overwhelming majority of the violations were unintentional human or technical errors and that the existence of the report showed that the agency's efforts to detect and correct violations of the rules were robust. He said the number of willful errors was "minuscule," involving a "couple over the past decade."**

Ext -- No Greater than What Private Companies Do

Corporate privacy invasions

Danny Schechter edits Mediachannel.org and blogs at Newdissector.net. He is producing a TV documentary series on America's surveillance state, May 16, 2014, "Can we stop America's Surveillance State?" http://www.huffingtonpost.com/danny-schechter/can-we-stop-americas-surv_b_5334572.html?utm_hp_ref=politics&ir=Politics

American corporations are not just cooperating with the NSA but competing with it. And, not just with Google cars photographing every street in the world. Just ask Donald Sterling, the LA Clippers owner and jerk as he may be, about what non-government spying did to him. Who has been prosecuted in that eavesdropping incident? I spoke to Sam Antar who was wiretapped by the government as part of an investigation into illegal practices by the Crazy Eddy electronics chain years ago and who became a convicted felon. He says that spying has become a profitable business, that is bigger and even more insidious than the NSA.

Private sector collects a lot of data already

Los Angeles Times, May 5, 2014, <http://www.latimes.com/business/la-fi-lazarus-20140506-column.html>

I wrote recently about Verizon Wireless quietly downloading code into people's home computers that would transmit your online browsing to marketers, who could then target you with related ads on your smartphone or tablet. Such corporate spying is apparently legal and, experts say, will become increasingly common as businesses try to track consumers from device to device. And the more they share people's information among themselves — a shadowy industry of data brokers already exists — the more they'll amass digital dossiers containing intimate details about your life, including where you shop, how you pass your weekends and what medicines you take.

NSA surveillance no different than what private companies do

Allan Swarn, May 5, 2014, arnnet,
http://www.arnnet.com.au/article/544320/cebit_2014_privacy_about_more_than_compliance_it_vital_economy_ccu/

He said the post-Snowden revelations about NSA spying have been overblown. Much of that has been machine parsing of data, and that the NSA has at most a couple of hundred people attempting to read a given language, globally. It has larger numbers of people attempting to read all languages. But even the total number of NSA linguists is tiny compared to the total volume of global communications. The NSA's spying is mostly done by machines and algorithms - there simply aren't enough staff to 'human spy' on everyone. Borg compares the NSA surveillance to the same tracking Amazon, Facebook and Google do daily in our lives.

Private sector collects a lot of data already

Los Angeles Times, May 5, 2014, <http://www.latimes.com/business/la-fi-lazarus-20140506-column.html>

I wrote recently about Verizon Wireless quietly downloading code into people's home computers that would transmit your online browsing to marketers, who could then target you with related ads on your smartphone or tablet. Such corporate spying is apparently legal and, experts say, will become increasingly common as businesses try to track consumers from device to device. And the more they share people's information among themselves — a shadowy industry of data brokers already exists — the more they'll amass digital dossiers containing intimate details about your life, including where you shop, how you pass your weekends and what medicines you take.

NSA surveillance no different than what private companies do and with only a couple hundred people

Allan Swann, May 5, 2014, arnnet,
http://www.arnnet.com.au/article/544320/cebit_2014_privacy_about_more_than_compliance_it_vital_economy_ccu/

He said the post-Snowden revelations about NSA spying have been overblown. Much of that has been machine parsing of data, and that the NSA has at most a couple of hundred people attempting to read a given language, globally. It has larger numbers of people attempting to read all languages. But even the total number of NSA linguists is tiny compared to the total volume of global communications. The NSA's spying is mostly done by machines and algorithms - there simply aren't enough staff to 'human spy' on everyone. Borg compares the NSA surveillance to the same tracking Amazon, Facebook and Google do daily in our lives.

Ext – Not US Citizens

NSA does not engage in surveillance of citizens living in a foreign land

Asia Tribune, April 25, 2014, <http://www.asiantribune.com/node/79305>

The NSA document is very clear about data collection or surveillance of U.S. citizens living in foreign country. The NSA is aware that many American citizens living in foreign countries - most in their countries of birth - are engaged in areas that the American authorities are very much interested such as defense, national security or foreign affairs.

The NSA document very clearly states that such persons cannot be subject to its radar to extract information sensitive or not. The document notes: *NSA cannot intentionally use Section 702 authority to target any U.S. citizen, any other U.S. person, or anyone known at the time of acquisition to be located within the U.S.* The NSA analyst must review a sample of communications received from the selectors to ensure that they are in fact associated with the foreign intelligence target and that the targeted individual or entity is not a U.S. person (meaning a US citizen) and is not currently located in the U.S. If the NSA analyst discovers that NSA is receiving communications that are not in fact associated with the intended target or that the user of a tasked selector is determined to be a U.S. person or is located in the U.S., the selector must be promptly “detasked.” As a general rule, in the event that the target is a U.S. person or in the U.S., all other selectors associated with the target also must be detasked. If NSA discovers that it has tasked a selector that is used by a person in the U.S. or by a U.S. person, then NSA must cease collection immediately and, in most cases must also delete the relevant collected data and cancel or revise any disseminated reporting based on this data.

US law does not permit mass surveillance of non-US citizens

Report and Recommendations of the President’s Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

What, though, of non-United States persons who are outside the United States? We begin by emphasizing that, contrary to some representations, section 702 does not authorize NSA to acquire the content of the communications of masses of ordinary people. To the contrary, section 702 authorizes NSA to intercept communications of non-United States persons who are outside the United States only if it reasonably believes that a particular “identifier” (for example, an e-mail address or a telephone number) is being used to communicate foreign intelligence information related to such matters as international terrorism, nuclear proliferation, or hostile cyber activities. NSA’s determinations are subjected to constant, ongoing, and independent review by all three branches of the federal government to ensure that NSA targets only identifiers that meet these criteria.

Ext – Oversight Solves

Extensive oversight of surveillance now and no abuse

Report and Recommendations of the President’s Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Third, FISA put in place a system of oversight, review, and checks- and-balances to reduce the risk that elements of the Intelligence Community would operate outside of the law. We offer many recommendations to improve the existing procedures, but it is important to note that they now include a wide range of inspectors general, privacy oversight boards, minimization procedures, intensive training requirements, mandatory reviews by the Attorney General and the Director of National Intelligence, judicial oversight by the FISA Court, and regular reporting to Congress. Appendix C provides information on these oversight mechanisms.

Significantly, and in stark contrast to the pre-FISA era, the Review Group found no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity. This is of central importance, because one of the greatest dangers of government surveillance is the potential to use what is learned to undermine democratic governance. On the other hand, as discussed later in this Report, there have been serious and persistent instances of noncompliance in the Intelligence Community’s implementation of its authorities. Even if unintentional, these instances of noncompliance raise serious concerns about the Intelligence Community’s capacity to manage its authorities in an effective and lawful manner.

Extensive oversight of metadata queries

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through “queries” of the database. A query is a search for a specific number or other selection term within the database. Before any specific number is used as the search target or “seed” for a query, one of twenty-two designated NSA officials must first determine that there is a reasonable, articulable suspicion (“RAS”) that the number is associated with terrorism. Once the seed has been RAS-approved, NSA analysts may run queries that will return the calling records for that seed, and permit “contact chaining” to develop a fuller picture of the seed’s contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number (the “first hop”), but also numbers in contact with all first hop numbers (the “second hop”), as well as all numbers in contact with all second hop numbers (the “third hop”).

No abuse

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the program.²² Rather, the compliance issues were recognized by the FISC — and are recognized by the Board — as a product of the program's technological complexity and vast scope, illustrating the risks inherent in such a program.

Data collection is not indiscriminate

Report and Recommendations of the President's Review Group on Intelligence, December 2013, Liberty and Security in a Changing World, December 12, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Second, although recent disclosures and commentary have created the impression in some quarters that NSA surveillance is indiscriminate and pervasive across the globe, that is not the case. NSA focuses on collecting foreign intelligence information that is relevant to protecting the national security of the United States and its allies. Moreover, much of what NSA collects is shared with the governments of many other nations for the purpose of enhancing their national security and the personal security of their citizens.

Oversight does assure compliance with existing laws

Jeffrey Stone, April 23, 2014, The Daily Beast,
<http://www.thedailybeast.com/articles/2014/04/23/heres-who-should-watch-the-watchmen.html>

As a member of the President's Review Group on NSA surveillance, I had a rare opportunity last fall to observe and evaluate the various mechanisms our government uses to oversee the activities of our nation's intelligence agencies. At the structural level, I was impressed with the variety and range of oversight mechanisms in place.

The National Security Agency's activities, for example, are overseen by the NSA's Inspector General, the Director of National Intelligence, the Foreign Intelligence Surveillance Court, the Department of Justice, the Privacy and Civil Liberties Oversight Board, and the Senate and House Intelligence Committees. Each of these entities is responsible for reviewing various aspects of the NSA's operations.

Cumulatively, I found that these oversight mechanisms work reasonably well when it comes to ensuring that the NSA properly implements the authorities it has been given. In those instances in which the NSA overstepped its bounds, these entities were generally quick to respond.

To cite just one example, in 2009 the Foreign Intelligence Surveillance Court (the FISC) learned that the NSA had misapplied a legal standard, resulting in improper access to telephone metadata. Although finding

that the noncompliance had been unintentional, the FISC nonetheless prohibited “the government to access the data collected until such time as the government is able to restore the Court’s confidence that the government can... comply with [the] approved procedures for accessing such data.” The FISC finally lifted this restriction six months later, only after the NSA had demonstrated to the court’s satisfaction that the causes of the noncompliance had been corrected and that additional safeguards had been instituted.

This is but one example of this type of oversight, but it reflects the seriousness with which the various entities engaged in this process undertake their responsibilities. On balance, they seem to do a reasonable job of ensuring that the intelligence agencies comply with their legal authorities.

I was less impressed, though, with oversight of a different sort. Once the government, whether the Executive Branch, the Congress, or the FISC, authorizes the intelligence agencies to undertake certain types of surveillance, there is, in my judgment, insufficient attention to whether the programs instituted under those authorities can and should be refined and improved over time.

Extensive oversight of the NSA

Kate Bullington, January 22, 2015, IVN.us, “Who Watches the Watchman: How the NSA Gets Around Oversight,” <http://ivn.us/2015/01/22/us-citizens-are-in-a-fight-for-their-rights/> DOA: 1-24-15

Through legislation and executive orders, at least 12 actors provide oversight for the NSA program:

- The NSA itself is required under the [Protect America Act](#) to submit reports to the [Intelligence Oversight Board \(IOB\)](#) about discovered and reported illegal activities.
- The [House Permanent Select Committee on Intelligence \(HPSCI\)](#) and the [Senate Select Committee on Intelligence \(SSCI\)](#), receive reports and oversee compliance with laws and regulations. The congressional committees may receive whistle-blower information through congressional testimony.
- The [Department of Justice \(DOJ\)](#), including the [Office of Inspector General \(OIG\)](#), is responsible for inspections, audits, investigations and reports of NSA activity. The OIG is a venue that may also receive whistle-blower information.
- The [Office of General Counsel \(OGC\)](#) provides legal advice.
- The [Foreign Intelligence Surveillance Court \(FISC\)](#) is the secret court where the intelligence agents apply for warrants.
- The [Privacy and Civil Liberties Oversight Board, \(PCLOB\)](#) reviews and analyzes executive actions on terrorism; and considers liberty concerns on laws, regulations, and policies concerning terrorism. They are required to submit at least two reports per year to congress on their activities and conclusions.
- Employees of the NSA, who are supposed to “know, understand, and obey the full laws of the Nation.”
- Citizens of the U.S. can oversee NSA activity through Freedom of Information Act requests.
- The [Office of Compliance \(OOC\)](#) is also given the authority to oversee conformity to government standards and policies, and may receive complaints from federal employees.

Ext – It's Voluntary

Users don't care about shared data

Olivier Sylvain, 2014, Associate Professor, Fordham University School of Law, Summer Wake Forest Law Review, FAILING EXPECTATIONS: FOURTH AMENDMENT DOCTRINE IN THE ERA OF TOTAL SURVEILLANCE,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473101, DOA: 1-24-15, p. 485-6

Users, meanwhile, are of two minds about these data-sharing arrangements. On the one hand, polls suggest that users have serious concerns. On the other hand, the sheer pace of growth of the consumer market for networked services and devices strongly suggests that they are comfortable enough to share personal information about their identities, locations, and preferences. Users do not appear to be deterred by shifting privacy policies and long-worded terms of service that detail how much of their information will be traded. To the contrary, if consumer demand is any measure of interest, users appear to welcome innovations that track and even predict their tastes for new products and services. Users appear to expect that their personal data is the proverbial grist for today's networked information economy.

Users voluntarily disclose tons of information

Olivier Sylvain, 2014, Associate Professor, Fordham University School of Law, Summer Wake Forest Law Review, FAILING EXPECTATIONS: FOURTH AMENDMENT DOCTRINE IN THE ERA OF TOTAL SURVEILLANCE,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473101, DOA: 1-24-15, p. 489-90

Indeed, despite their misgivings, participation and upload rates at the top social networking sites and applications continue to grow. For example, over 1.2 billion users log in to their Facebook accounts at least every month. That is around one-third greater than the number of user accounts Facebook had just a year before. Of these, about 700 million are active daily users. users upload an average of more than 350 million photos every day, with a huge fraction of these pictures coming from smartphone cameras. Meanwhile, about 500 million people have active Twitter accounts from which they post nearly fifty-eight million tweets and photos every day. If these popular Internet-based applications are any indication of how willing users are to publicize their personal information, we can assume that, no matter how uneasy they may be about disclosing so much, users are still willing to do it.

A2: No Legislative Authority for Metadata Collection

The government has broad authority under Section 215 to collect telephone metadata

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

One reading of section 215 is that the phrase “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation” means that the order must specify with reasonable particularity the records or other things that must be turned over to the government. For example, the order might specify that a credit card company must turn over the credit records of a particular individual who is reasonably suspected of planning or participating in terrorist activities, or that a telephone company must turn over to the government the call records of any person who called an individual suspected of carrying out a terrorist act within a reasonable period of time preceding the terrorist act. This interpretation of “relevant” would be consistent with the traditional understanding of “relevance” in the subpoena context. In May 2006, however, the FISC adopted a much broader understanding of the word “relevant.” It was that decision that led to the collection of bulk telephony meta-data under section 215. In that decision, and in thirty-five decisions since, fifteen different FISC judges have issued orders under section 215 directing specified United States telecommunications providers to turn over to the FBI and NSA, “on an ongoing daily basis,” for a period of approximately 90 days, “all call detail records or ‘telephony meta-data’ created by [the provider] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.” The “telephony meta-data” that must be produced includes “comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.” The orders expressly provide that the meta-data to be produced “does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer,” nor does it include “cell site location information.” The orders also contain a nondisclosure provision directing that, with certain exceptions, “no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order.”

The FISC authorized the collection of bulk telephony meta-data under section 215 in reliance “on the assertion of the [NSA] that having access to all the call records ‘is vital to NSA’s counterterrorism intelligence’ because ‘the only effective means by which NSA analysts are able continuously to keep track of’ the activities, operatives, and plans of specific foreign terrorist organizations who “disguise and obscure their communications and identities” is “‘to obtain and maintain an archive of meta-data that will permit these tactics to be uncovered.’” The government has explained the rationale of the program as follows: One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist

attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States. By analyzing telephony meta-data based on telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. . . . In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.

A2: Scope of Collection is Too Broad

A broader collection of records is “relevant” for data collection purposes

General Counsel, Office of the Director of National Intelligence (ODNI), **July 31**, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hsl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

SEN. GRASSLEY: Mr. Litt, Section 215 contains a requirement that records collected under the program, Provision B, quote, unquote, "relevant to an authorized investigation." As a legal matter, how can you justify the assertion that phone records of millions of Americans who have nothing to do with terrorism are relevant to an authorized investigation under Section 215?

ROBERT LITT: So I'd begin by noting that a number of judges, repeatedly over the years, have found over the years that these records are, in fact, relevant. The reason is that the standard of relevance that we're talking about here is not the kind of relevance that you think about in the Perry Mason sense of a criminal trial. It's a much broader standard of relevance, and in a number of circumstances in the law, such as grand jury subpoenas or civil discovery, it's a -- it's a well-accepted concept that if you need to get a large group of records in order to find a smaller group of records that actually provides the information you need to move forward, that the larger group of records can be relevant.

That's particularly true in this case because of the kinds of controls that the deputy attorney general mentioned -- the fact that the queries are limited, the access to the data is limited, and for that reason, the FISA court has repeatedly found that these records are relevant.

SEN. GRASSLEY: Is there any legal precedent that supports such a broad definition of relevance to an investigation?

MR. LITT: I'd actually defer that to the deputy attorney general.

SEN. GRASSLEY: OK.

MR. COLE: Well, the legal precedent comes from the history of all the orders that have been issued, the courts having looked at this under the FISA law and under the provisions of 215 and making sure that under the provisions and the ability to get these records relevant to a -- rather, a foreign intelligence investigation. They have gone through the law that Mr. Litt has described on, as I said, I believe, 34 different occasions to do this analysis.

So those are -- that legal precedent is there.

Government Power Answers

Section 215 doesn't increase the power of the federal government

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,

<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 907

Section 215 does not contain a revolutionary grant of authority to the government. It authorizes something akin to a grand jury subpoena for financial, communication, or travel records as part of a criminal investigation. In fact, the statute additionally defines the records as those that can be obtained by a subpoena issued by a federal court as part of a grand jury investigation. Section 215 of the Patriot Act provides the authority for the NSA's collection of telephone billing records. The NSA collects the data containing the phone numbers on both ends of a call and the duration of every call made in the United States. But it does not intercept the content of the call, nor does it know the identity of the subscriber. It collects the information into a database of all calls in the nation, which did not exist previously because multiple telecommunications companies would delete their records. The NSA purges records that are more than five years old. A database allows the NSA to determine quickly the calling chain of any overseas numbers discovered to belong to al Qaeda operatives. Once the NSA tracks down the phone numbers called within the United States from a suspected al Qaeda phone number, it can then seek a warrant from the FISC to place the number under further surveillance and to collect other records, such as financial and travel information.

Phone Records Program Could Have Prevented 9/11

If the phone records program existed, 9/11 may not have happened

Stuart **Taylor, April 29, 2014**, The Big Snoop: Life, Liberty, and the Pursuit of Terrorists, <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.)

With respect to the phone records program, the disagreement between Senators Feinstein and Wyden has been especially stark, and it is reflected in a bipartisan debate underway over the past few months on the Hill. Feinstein believes if the phone records program had been up and running in 2001, it might have alerted the government that Khalid al-Mihdhar, a major al Qaeda operative from Saudi Arabia who was on NSA and FBI watch lists, was in San Diego, making calls to an al Qaeda safe house in Yemen. That information might have been a giveaway that the plan had “gone operational.” Instead, the NSA sleuths tracking terrorists thought al-Mihdhar was overseas. He was one of the five hijackers of American Airlines Flight 77, where 189 people (including the hijackers) were killed when it crashed into the Pentagon. Keith Alexander has posited the same counterfactual speculation. Playing it forward, he and Feinstein both believe that ending the phone records program would increase America’s vulnerability to another attack.

Answer to Negative Arguments

AT Circumvention

AT: Executive Circumvention

Executive will abide by the law

Prakash and Ramsey ‘12 (Saikrishna B, David Lurton Massee, Jr. Professor of Law and Sullivan and Cromwell Professor of Law, University of Virginia School of Law and Michael D, Professor of Law, University of San Diego School of Law, review of The Executive Unbound, Texas Law Review (2012) 90:973, <http://www.texaslrev.com/wp-content/uploads/Prakash-Ramsey-90-TLR-973.pdf>)

Yet we doubt the book’s central claim that we live in a post-Madisonian republic. First, the U.S. Executive is very much bound—by the Constitution, Congress’s laws, and the courts. Though we cannot peer into the many minds populating the Executive Branch, we do not believe that executive officials regard themselves as above the law and the courts, answerable only to the people via elections and polls. The Executive Branch does not act this way, and most of its actions are consistent with its own sense of what the law requires and forbids (although, like most actors, it often reads the law to maximize its discretion). To be sure, the Executive Branch takes advantage of gaps and ambiguities in the law, as well as its speed, decisiveness, and access to information, all as The Executive Unbound describes.⁵ But the Executive does not systematically disregard orders from Congress or the courts nor does it usually exercise core powers that the Constitution assigns elsewhere; the Executive does not impose criminal punishments, spend money without authorization, or rule by decree. Second, while we agree with Posner and Vermeule that public opinion colors Executive Branch decision making, we also believe that the public favors an executive bound by the law. So long as the public expects the law to constrain the Executive, the Executive will take into account this expectation and the public's sense of the law, even under Posner and Vermeule’s own light. In other words, the public has a taste for the rule of law, a taste that the Executive Branch ignores at its peril. We think the legal constraints on the modern Executive are so manifest that we wonder whether Posner and Vermeule’s real project is more aspirational than descriptive. Perhaps their ultimate objective is to persuade us that we should have an unbound executive, not that we already have one. We hedge here because the book seems of two minds. In keeping with the title, most of the book forcefully argues that the Executive faces no material legal constraints. For instance, Posner and Vermeule write that “the legally constrained executive is now a historical curiosity”⁶ and that the Madisonian separation of powers has “collapsed.”⁷ There is no equivocation here. Yet Chapter 6 argues that irrational fear of executive tyranny has prevented the Executive from obtaining powers needed to handle modern emergencies.⁸ Obviously this complaint assumes that there are constraints on the Executive. And the conclusion in particular appears to admit that the courts and Congress check the Executive—that the Executive is bound and that the Madisonian republic lives on.

AT circumvention – generic

No circumvention – prefer empirics and authoritative independent review

Bora 14 (Kukil Bora, International Business Times, “NSA Internet Surveillance Is Legal, A Presidential Privacy Board Concludes,” 7-2-2014, <http://www.ibtimes.com/nsa-internet-surveillance-legal-presidential-privacy-board-concludes-1617270>)

The NSA's current spying activities function under a provision known as Section 702, which has its roots in the Terrorist Surveillance Program implemented after the 9/11 attacks. It was added in 2008 to the Foreign Intelligence Surveillance Act of 1978 to allow the agency to collect and track electronic communications initiated by foreigners living outside the U.S. when their telephone calls, emails, web chats and text messages enter the country. Section 702 also covers the divisive PRISM program, which allows NSA to collect foreign communication data from technology companies, such as Google Inc. (NASDAQ:GOOGL), Facebook Inc (NASDAQ:FB), Microsoft Corporation (NASDAQ:MSFT) and Apple Inc. (NASDAQ:AAPL). The NSA is accused of also spying on communications made by Americans, in its effort to glean information on terrorist activities and foreign intelligence. After the unauthorized disclosure of classified documents by former NSA systems administrator Edward Snowden, many people expressed concerns, and criticized as unconstitutional, the practice of secretly collecting troves of data about Americans' communications over the Internet without their approval. However, the board, which consists of a Democratic federal judge, two privacy experts and two former Republican justice department officials, found that the NSA surveillance is legal and realistic. “Overall, the board finds that the protections contained in the Section 702 minimization procedures are reasonably designed and implemented to ward against the exploitation of information acquired under the program for illegitimate purposes,” the board said in the report. “The board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits.” The report also offered recommendations to help the government push NSA programs “into the sphere of reasonableness” to ensure that the agency can perform its duties while operating within Constitutional limits. However, according to Associated Press, exactly how the government would utilize the information obtained through Section 702, and the extent to which the information would help authorities investigate domestic law enforcement cases, remains unclear.

AT circumvention – intel-sharing

Foreign partners won't circumvent

Shane 13 (Scott Shane, New York Times, “Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance,” 6-21-2013, http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html?_r=0)

In the latest installment of the Snowden disclosures on Friday, The Guardian reported that the N.S.A.’s British counterpart has tapped into hundreds of fiber-optic communications lines and is sharing a vast quantity of e-mail and Internet traffic with American intelligence. Under a program called Tempora, the British agency, known as G.C.H.Q., has been able to tap into 200 of the approximately 1,600 high-capacity fiber cables in and out of Britain and aspires to be able to tap 400 lines at once, harvesting a staggering amount of information, the British newspaper reported. The documents said that G.C.H.Q., which has worked very closely with the N.S.A. for decades, may store the content of the communications flowing over the cables for three days and the so-called metadata — information about who is contacting whom at what time — for 30 days. During that time, analysts from both G.C.H.Q. and the N.S.A. are able to search the stored data for information of interest. The disclosures of the G.C.H.Q. initiative, called “Mastering the Internet,” immediately raised a question among privacy advocates: whether the N.S.A. might be able to obtain information about Americans from G.C.H.Q. that it is prohibited by law or regulations from collecting itself. An N.S.A.

spokeswoman, Judith Emmel, said the agency does not use foreign partners to evade American restrictions.

“Any allegation that N.S.A. relies on its foreign partners to circumvent U.S. law is absolutely false,” she said. “N.S.A. does not ask its foreign partners to undertake any intelligence activity that the U.S. government would be legally prohibited from undertaking itself.” Ms. Emmel said the N.S.A. is unwavering in its respect for U.S. laws and policies” and has “a rigorous internal compliance program” as well as oversight from Congress and the Foreign Intelligence Surveillance Court. One document released by Mr. Snowden lent some support for the Obama administration’s insistence that the N.S.A. is tightly controlled. In a confidential briefing, The Guardian reported, a G.C.H.Q. legal adviser declared: “We have a light oversight regime compared with the U.S.”

Tcircumvention – privates

Private sector won't circumvent

Tim Worstall, 13, "NSA's PRISM Sounds Like A Darn Good Idea To Me: This Is What Governments Are For," Forbes, <http://www.forbes.com/sites/timworstall/2013/06/07/nsas-prism-sounds-like-a-darn-good-idea-to-me-this-is-what-governments-are-for/>

There's been a joint investigation by the Washington Post and The Guardian into an NSA program called PRISM. The allegation is that the National Security Agency (NSA) has backdoor access to the systems and data of the major internet firms, Microsoft MSFT -0.77%, Google GOOG -0.68%, Apple AAPL -0.56%, Facebook FB +0.03% and so on, and they routinely use this to monitor what people are saying and doing. With one caveat this is in fact what governments are supposed to do so I'm at something of a loss in understanding why people seem to be getting so outraged about it. The WaPo piece is here, a couple from The Guardian here and here. It's worth pointing out that the companies themselves are vehemently denying that the NSA has such backdoor access to the data. However, senior executives from the internet companies expressed surprise and shock and insisted that no direct access to servers had been offered to any government agency. The top-secret NSA briefing presentation set out details of the PRISM program, which it said granted access to records such as emails, chat conversations, voice calls, documents and more. The presentation listed dates when document collection began for each company, and said PRISM enabled "direct access from the servers of these US service providers: Microsoft, Yahoo YHOO -2.43%, Google, Facebook, Paltalk, AOL AOL +0.06%, Skype, YouTube, Apple". Senior officials with knowledge of the situation within the tech giants admitted to being confused by the NSA revelations, and said if such data collection was taking place, it was without companies' knowledge. An Apple spokesman said: "We have never heard of PRISM. We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order," he said. Whether the claim of direct access is true or not is one thing. But the much larger point is that this sort of behaviour is not something that we should be shouting about government doing. It's something that we should be shouting about government not doing.

AT Circumvention (PDD 28)

Fiat solves circumvention – US fg including all relevant agencies will follow letter of the law for FAA section 702 and PDD 28 per plan mandates. Plan also sends international signal that bolsters trust – that's the Eoyang solvency.

PPD-28 is key to protecting the rights of non-US persons abroad

Edgar, 4/13/15 – (Timothy Edgar, visiting fellow at the Institute and adjunct professor of law at the Georgetown University Law Center Timothy. April 13, 2015. “The Good News About Spying” [<https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying>])HW

Beyond more transparency, Obama has also changed the rules for surveillance of foreigners. Until last year, privacy rules applied only to “U.S. persons.” But in January 2014, Obama issued Presidential Policy Directive 28 (PPD-28), ordering intelligence agencies to write detailed rules assuring that privacy protections would apply regardless of nationality. These rules, which came out in January 2015, mark the first set of guidelines for intelligence agencies ordered by a U.S. president—or any world leader—that explicitly protect foreign citizens’ personal information in the course of intelligence operations. Under the directive, the NSA can keep personal information in its databases for no more than five years. It must delete personal information from the intelligence reports it provides its customers unless that person’s identity is necessary to understand foreign intelligence—a basic rule once reserved only for Americans. The new rules also include restrictions on bulk collection of signals intelligence worldwide—the practice critics call “mass surveillance.” The NSA’s bulk collection programs may no longer be used for uncovering all types of diplomatic secrets, but will now be limited to six specific categories of serious national security threats. Finally, agencies are no longer allowed simply to “collect it all.” Under PPD-28, the NSA and other agencies may collect signals intelligence only after weighing the benefits against the risks to privacy or civil liberties, and they must now consider the privacy of everyone, not just U.S. citizens. This is the first time any U.S. government official will be able to cite a written presidential directive to object to an intelligence program on the basis that the intelligence it produces is not worth the costs to privacy of innocent foreign citizens

PPD-28 and USSID SP0018 safeguards civil liberties

Moultrie 1/12/15 (Ron Moultrie, former Signals Intelligence Director, Executive Agent for USSID. National Security Agency, January 12, 2015. “PPD-28 Section 4 Procedures” [https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf])HW

Presidential Policy Directive 28 (PPD-28) articulates principles to guide United States SIGINT activities for authorized foreign intelligence and counterintelligence purposes. In response to PPD-28 Section 4, NSA has developed Supplemental Procedures to United States Signals Intelligence Directive, USSID SP0018. USSID SP0018 implements the Attorney General-approved procedures contained in Department of Defense (DoD) Regulation 5240.1-R and its Classified Annex that govern NSA’s SIGINT activities. USSID SP0018 prescribes specific minimization policies and procedures for U.S. Persons, and assigns responsibilities to assure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. Persons. All personnel who are conducting E.O. 12333 SIGINT activities under the direction, authority, or control of the Director of the National Security Agency throughout the SIGINT lifecycle are responsible to protect the privacy of U.S. Persons. PPD-28 Section 4 directs the Intelligence Community

(IC) to establish policies and procedures for safeguarding personal information collected during signals intelligence activities. NSA's Supplemental Procedures are the guidance and procedures for implementing this direction from the President. Consistent with the requirements of Section 4.(a), NSA's Supplemental Procedures extend comparable safeguards currently provided for U.S. Persons to all persons, regardless of nationality. Section 4.(b) requires IC elements to issue procedures by 17 January 2015, one year after the President released PPD-28. As specified in section 4.(c), NSA worked with the White House in developing these policies and procedures to ensure the proper civil liberties and privacy safeguards are in place. The new Supplemental Procedures are entitled "USSID SP0018 Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information for Non-United States Persons." and implement the privacy and civil liberties protections afforded to non-u.s. persons in a manner that is comparable, to the extent consistent with national security, to the privacy protections afforded to U.S. persons. These new Supplemental Procedures are written as a guide to SIGINT professionals. Wherever possible, language in the Supplemental Procedures mirrors the terminology and structure of parallel provisions in USSID SP0018 and in PPD-28.

AT FBI Circumvention

FBI circumvention's irrelevant – NSA overreach causes international signal of distrust.

FBI will follow PPD-28

Giuliano 2/2/15 (Mark F. Giuliano- Deputy Director of the Federal Bureau of Investigation, making him the Bureau's second-highest-ranking official. "PRESIDENTIAL POLICY DIRECTIVE 28 POLICIES AND PROCEDURES" [<https://www.fbi.gov/about-us/nsb/fbis-policies-and-procedures-presidential-policy-directive-28-1>]) hw

Presidential Policy Directive 28 regarding signals intelligence activities (hereinafter "PPD-28"), issued January 17, 2014, articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. Specifically, section 4 of PPD-28 sets forth principles for safeguarding personal information collected from signals intelligence activities and requires Intelligence Community ("IC") elements to establish policies and procedures to apply such principles, consistent with technical capabilities and operational needs. As stated in PPD-28, all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. Although the FBI does not conduct "signals intelligence activities," the FBI is applying the relevant provisions of PPD-28 to information it collects pursuant to FISA section 702 to further these principles. Although the FBI does not conduct signals intelligence activities and does not have access to unevaluated, raw, or unminimized signals intelligence, it does receive from other IC elements engaged in such activities signals intelligence information that has been evaluated, minimized, or otherwise included in finished intelligence products. These policies and procedures also address the manner in which the FBI will handle signals intelligence information in these finished intelligence products.

AT: FISA surveillance only foreign

We meet – our aff stops the abuse of FISA exceptions that authorize domestic searches

Robertson, 15 - James Robertson served on the U.S. District Court for the District of Columbia from 1994 to 2010. He also served on the Foreign Intelligence Surveillance Court from 2002 to 2005 (“What went wrong with the FISA court”, Brennan Center for Justice at New York University School of Law, 2015)

And here is where concern about the Foreign Intelligence Surveillance Act comes in. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 established the rules for domestic government wiretaps. FISA, enacted ten years later, focused on foreign intelligence. But it is the use (or misuse) of FISA, and FISA's potential allowance of unreasonable domestic searches and seizures, that the reporting of James Risen and Eric Lichtblau and the disclosures of Edward Snowden have brought into sharp focus.

FISA's internationality requirement is vague and allows targeting purely domestic groups

Harper 14, University of Chicago Law School, U.S. Department of Justice, Civil Division, (Nick, “FISA’s Fuzzy Line between Domestic and International Terrorism”, University of Chicago Law Review; Summer2014, Vol. 81 Issue 3)//AK

Because foreign policy interests constitutionally distinguish international and domestic terrorist groups, FISA's internationality requirement, which attempts to sort these groups for Fourth Amendment purposes, must identify cases in which these interests are present. However, some interpretations of the nebulous FISA standard allow for the targeting of terrorist groups that should be considered domestic for Fourth Amendment purposes because they do not trigger foreign policy interests. This, in turn, permits the employment of certain FISA procedures against domestic groups that may violate the Fourth Amendment.

Abdul-Latif demonstrates how an expansive interpretation of FISA's internationality requirement¹⁷⁹ can permit the targeting of groups that do not implicate the two foreign affairs interests described above. In this case, the government engaged in FISA surveillance even though neither the target of the attack (a domestic military entrance processing station) nor Abdul-Latif's international YouTube activity risked creating a diplomatic crisis. Moreover, there is no available evidence indicating that Abdul-Latif may have been a link in a global chain of terror such that the government's duty to control international terrorism was triggered. Therefore, even if Abdul-Latif's conspiracy qualified as international terrorism under FISA—as the court seemed to think—the conspiracy still did not implicate the foreign policy interests necessary to merit such a designation under the Fourth Amendment.

Even assuming that such expansive interpretations of FISA's internationality requirement are rare, more limited interpretations that clearly satisfy FISA's language may similarly fail to trigger foreign policy concerns. To illustrate, a US citizen purchasing weapons from a friend in Mexico for use in a terrorist attack in the United States almost certainly qualifies as international terrorism under FISA. Such activity "transcend[s] national boundaries in terms of the means by which [the terrorist acts] are accomplished"¹⁸⁰ because the guns used to perpetrate the attack have a substantial international character. However, it is not readily apparent that such activity would cause a foreign affairs crisis or that it would trigger a domestic duty to control international terrorism. Thus, this activity should be seen as domestic terrorism for Fourth Amendment purposes.

The overinclusive nature of FISA's internationality requirement raises the important question whether FISA's procedures would violate the Fourth Amendment when applied to terrorist groups that should be considered domestic because they do not trigger the government's foreign policy interests. On one view, FISA's procedures are reasonable even when applied to domestic terrorist groups. As mentioned above, the Keith Court noted that in the domestic terrorism context, warrants for electronic surveillance need not be identical to Title III warrants.¹⁸¹ Rather, the warrants could utilize a less stringent standard of probable cause, have looser time and reporting requirements, and be sought at a specially designated court.¹⁸² FISA's procedures appear to roughly track these recommendations, as was noted by the FISCR in a rare published case upholding the constitutionality of FISA warrant procedures in the foreign-intelligence context.¹⁸³ Therefore, FISA proponents would argue, FISA warrants are reasonable under the Fourth Amendment regardless of whether domestic or international terrorist groups are targeted.

Although FISA's procedures generally track the recommendations made in Keith, there are at least two FISA procedures that seem inappropriate when applied in the domestic terrorism context, and which may render a FISA warrant unreasonable when applied to domestic groups. The most problematic of these is FISA's notice requirement. FISA does not require notice to the surveillance target unless the government intends to use the surveillance in a criminal proceeding,¹⁸⁴ and the Supreme Court has found such a lack of default notice to be a constitutionally significant factor in determining the reasonableness of a warrant.¹⁸⁵ The FISCR justified FISA's notice procedure in the foreignintelligence context by pointing to the conclusion in the FISA Senate report that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."¹⁸⁶ However, the Senate report from which the FISCR quotes concluded that FISA's stark departure from the standard notice requirement was reasonable only in the context of foreign counterintelligence investigations.¹⁸⁷ While the investigation of truly international terrorism might rise to the level of foreign counterintelligence due to the pseudopolitical nature of many foreign terrorist organizations, the same cannot be said of domestic terrorism investigations. Investigations of domestic terrorism simply do not require the same level of secrecy because there is no risk of injuring the foreign policy of the United States. As the Keith Court suggested, investigations of domestic groups might justify a looser notice requirement than Title III in sensitive cases or in cases involving long-term surveillance,¹⁸⁸ but there is no apparent justification for a no-notice default rule when FISA is applied to domestic terrorists.

FISA's minimization procedures also raise constitutional concerns when applied to domestic terrorists. The Supreme Court has forbidden warrant schemes that give an officer the ability to seize "any and all conversations" from a targeted device or facility.¹⁸⁹ In an effort to prevent

such broad information acquisition, FISA requires that the government adopt minimization procedures—“specific procedures” that limit the amount of information that the government can acquire, retain, and disseminate.¹⁹⁰ Although any suggested minimization procedures are subject to approval or modification by the FISC, the government has adopted standard procedures that, in practice, permit the initial acquisition of all information from a monitored device or facility.¹⁹¹ Title III, on the other hand, requires procedures that minimize the irrelevant information acquired in the first place.¹⁹² FISA does require further minimization of information that is retained and disseminated, but these additional safeguards likely do not provide a meaningful filter to the acquisition process because the standards of retention are extremely low.¹⁹³ Moreover, data acquisition can continue indiscriminately for weeks before further minimization procedures are applied.¹⁹⁴

FISA’s internationality requirement is blurring – allowing surveillance of purely domestic groups

Harper 14, University of Chicago Law School, U.S. Department of Justice, Civil Division, (Nick, “FISA’s Fuzzy Line between Domestic and International Terrorism”, University of Chicago Law Review; Summer2014, Vol. 81 Issue 3)//AK

The Foreign Intelligence Surveillance Act of 1978 (FISA) regulates, among other things, the government’s acquisition of electronic surveillance within the United States for foreign intelligence purposes. FISA allows a federal officer to seek an order from a judge at a specially designated court “approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.” As long as the requisite foreign nexus can be shown, FISA warrants are preferable to their possible substitutes because they are easier to obtain and allow for more secretive and penetrating investigations.

Consistent with FISA’s foreign focus, the government may use the statute to investigate members of international terrorist groups within the United States. However, the activities of purely domestic terrorist groups do not fall under FISA and must therefore be investigated using standard criminal investigative tools. Often, terrorists will easily be identified as international: members of designated “foreign terrorist organizations” operating within the United States are clearly international terrorists. But the proliferation of modern communication technologies has caused increasing slippage between the definitions of domestic and international terrorism. For example, many homegrown terrorists are inspired by international groups to commit attacks in the United States. In many cases, the government seems to classify these actors as international terrorists based on Internet activity that ranges from viewing and posting jihadist YouTube videos to planning attacks

with suspected foreign terrorists in chat rooms, thus using FISA's formidable investigatory weapons against them. The government is aided in this task by FISA's definition of international terrorism, which has an extremely vague and potentially loose internationality requirement. An expansive interpretation of this requirement could be used to subject what might properly be considered domestic terrorist groups to FISA surveillance.

One should be concerned about both the existence and the effects of an expansive interpretation of FISA's internationality requirement. Not only would subjecting domestic terrorist groups to FISA surveillance violate FISA itself, but such an application might also be unreasonable under the Fourth Amendment. Moreover, the FISA application and surveillance process is very secretive, lacks a true adversarial process, and is devoid of meaningful oversight. This setting offers an ideal environment for the government to push statutory and constitutional boundaries. Indeed, recent revelations from Edward Snowden offer confirmation that the government is more likely to cross constitutional lines in the name of national security when these institutional factors are present.

FISA's loose internationality requirement allows surveillance of domestic groups

Harper 14, University of Chicago Law School, U.S. Department of Justice, Civil Division, (Nick, “FISA’s Fuzzy Line between Domestic and International Terrorism”, University of Chicago Law Review; Summer2014, Vol. 81 Issue 3)//AK

FISA's definition of international terrorism permits the government to draw a fuzzy line between international and domestic terrorism. This uncertainty potentially allows the government to engage in FISA surveillance of terrorist groups that do not implicate the government's foreign policy interests. This, in turn, raises serious constitutional questions. To fashion a solution that avoids these constitutional issues, this Comment has identified the government interests that distinguish these groups for Fourth Amendment purposes and has proposed a more limited interpretation of FISA's internationality requirement. The proposed interpretation seeks to identify international terrorists by asking if they implicate these foreign policy interests. Beyond more accurately identifying terrorist groups, a more tailored internationality standard would give courts and defendants the tools necessary to counteract the distinct institutional advantage currently possessed by the government.

FISA is entirely about the use of foreign intelligence information within the United States

Sommer, 14 - The author is with ZwillGen PLLC in Washington, D.C.; a law firm that represented a telecomm provider against a FISA order (Jacob, “FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition” Litigation, Spring, Vol. 40 No. 3

http://www.americanbar.org/publications/litigation_journal/2013-14/spring/fisa_authority_and_blanket_surveillance_gatekeeper_without_opposition.html

FISA occupies an uneasy place. It resides where intelligence gathering meets the Fourth Amendment. FISA addresses the problem of how, and when, the government can conduct surveillance for intelligence-gathering purposes on United States soil. Over time, Congress has addressed this delicate balance by amending FISA to expand and contract surveillance capabilities. Today, FISA provides a comprehensive set of procedures for obtaining and using “foreign intelligence information” within the United States.

AT: 702 only foreign

702 governs collection within the US

Schneier, 15, fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Ch. 12)//AK

Section 702 of the FISA Amendments Act was a little different. The provision was supposed to solve a very specific problem. Administration officials would draw diagrams: a terrorist in Saudi Arabia was talking to a terrorist in Cuba, and the data was flowing through the US, but the NSA had to eavesdrop outside of the US. This was inefficient, it argued, and Section 702 allowed it to grab that conversation from taps inside the US.

None of their evidence assumes for incidental collection – the location of a source can't be determined until data is already gathered

PCLOB 14 - independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act ("Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 07/02/14, <https://www.pclob.gov/library/702-Report.pdf>)//GK p.6

Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired in a variety of ways. An example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is termed "incidental" collection. Another example is when two non-U.S. persons discuss a U.S. person. Communications of or concerning U.S. persons that are acquired in these ways may be retained and used by the government, subject to applicable rules and requirements. The communications of U.S. persons may also be collected by mistake, as when a U.S. person is erroneously targeted or in the event of a technological malfunction, resulting in "inadvertent" collection. In such cases, however, the applicable rules generally require the communications to be destroyed.

We meet – Section 702 gathers U.S. person data

Bates 14 – United States District Judge for the United States District Court for the District of Columbia, B.A. from Wesleyan University, J.D. from the University of Maryland School of Law (John, Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, 1/10/14, <http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf>)//JJ

Querying Section 702 Information: Section 702 of FISA concerns certain acquisitions of foreign intelligence information targeting non-U. S. persons who are reasonably believed to be outside the United States. Currently, the government may not target U.S. persons for acquisition under Section 702, see § 702(b)(1), (3), but information about U.S. persons may still be obtained (e.g., when a U.S. person communicates with a targeted non-U.S. person). Proposals have been made to generally prohibit querying data acquired under Section 702 for information about particular U.S. persons, with an exception for emergency circumstances and for U.S. persons for whom a probable cause showing has been made. These proposals would engender a new set of applications to the FISC. Decisions about querying Section 702 information are now made within the Executive Branch. As a result, the Courts do not know how often the government performs queries of data previously acquired under Section 702 in order to retrieve information about a particular U.S. person. It seems likely to us, however, that the practice would be common for U.S. persons suspected of activities of foreign intelligence interest, e.g., engaging in international terrorism, so that the burden on the FISC of entertaining this new kind of application could be substantial.¹

We meet – section 702 gathers communications of Americans
Kayyali 14 – B.A. from UC Berkeley and J.D. from UC Hastings, Community Outreach Editor for the Hastings Race and Poverty Law Journal (Nadia, The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why., Electronic Frontier Foundation, 5/7/14, <https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why>)//JJ

Even though it's ostensibly used for foreign targets, Section 702 surveillance sweeps up the communications of Americans. The NSA has a twisted, and incredibly permissive, interpretation of targeting that includes communications about a target, even if the communicating parties are completely innocent. As John Oliver put it in his interview with former NSA General Keith Alexander: "No, the target is not the American people, but it seems that too often you miss the target and hit the person next to them going, 'Whoa, him!'"

The NSA has confirmed that it is searching Section 702 data to access American's communications without a warrant, in what is being called the "back door search loophole." In response to questions from Senator Ron Wyden, former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers," for example email addresses associated with someone in the U.S.

Section 702 proves that US person data is under surveillance regardless of if the surveillance is domestic or foreign

Sanchez 15* Washington, D.C.–based writer, policy analyst, and journalist who covers the intersection of privacy, technology, and politics (Julian, “GOVERNMENT DISCRETION IN THE AGE OF BULK DATA COLLECTION: AN INADEQUATE LIMITATION?”, Federalist Edition Volume 2 p.32-35)//GK

Section 702 of the FISA Amendments Act permits blanket surveillance authorizations. Those are general warrants, plain and simple.⁵⁷ We are meant to feel reassured by the fact that Americans cannot be “targeted” under these authorizations,⁵⁸ even though our communications are intercepted.⁵⁹ But of course, no particular person is the specific target of any general warrant—that is what makes it a general warrant. That is not much of a consolation if your communications can nevertheless be intercepted, not pursuant to the order of a neutral magistrate but at the discretion of an NSA analyst.⁶⁰ The scale of collection under these authorities,⁶¹ makes it very likely the system for misuse of that data. It is also increasingly clear that the public’s initial understanding of how these programs operated was fundamentally inaccurate.⁶² Even the understanding of the Supreme Court, which formed the basis of the ruling in Clapper v. Amnesty International USA,⁶³ was grounded in a significant misunderstanding of how “targeting” under section 702 authorities operated.⁶⁴ Both the Court and most members of the public presumed that an American’s communications could be intercepted without a warrant, but only if they were in contact with a foreign surveillance target.⁶⁵ But, in fact, your communications could also be intercepted if your communication mentioned a “selector,” such as an e-mail address, that the NSA had tasked for collection.⁶⁶ So the NSA is essentially filtering all international communication, searching their contents by computer, and flagging those e-mails and other digital communications that reference a target, whether or not that target is actually a party to the conversation.⁶⁷ When we consider that a “target” as defined by FISA can also be a corporate entity⁶⁸—or an entire website, when the target is an entity like The Pirate Bay or WikiLeaks⁶⁹—the potential for large-scale interception of American communications is made fairly clear. Returning again to the question of “balancing,” what we should be asking is not what particular abuses we have found out about to date. Although the suggestion is disturbing in one set of leaked NSA documents that “radicalizers” who are not terrorists, but who speak critically about the U.S. and justify violence against it in writing, could be targeted for smear campaigns using signals intelligence about their private online sexual activity.⁷⁰ Rather, the question we need to ask is: If someone with the intentions of a Hoover once again gained his powerful position, what effective limits would there be on his ability to use this intelligence gathering architecture in anti-democratic ways? Are there, and can there be, appropriate and necessary limits on the mass collection of Internet communications? What about enormous collection of telephone, financial, and other types of data that can paint an incredibly detailed portrait of anyone’s life? There can be no meaningful guarantee of privacy—not “security” against unreasonable search—when this information is indiscriminately collected. Even if it is simply sitting in a database today,⁷¹ it remains waiting to be scrutinized and searched. Indeed, even if the initial “targeting” of NSA’s collection is limited to foreigners, those databases can subsequently be searched using “selectors” associated with U.S. persons.⁷² In other words, once that information is collected under a sweeping authority justified by the exigencies of foreign intelligence and counterterrorism, the NSA and the FBI are allowed to go in and search for an American’s name, even though they would have needed a particularized warrant to do initial collection targeting that person.⁷³ What are the practical constraints on the misuse of that vast store of data? Given that the FISA court has itself been repeatedly misinformed about the technical details of how these programs operate, in some cases for years at a time,⁷⁴ the only realistic answer is that there are not any. We are effectively relying on the probity of intelligence officials.⁷⁵ We can hope they have been deserving of that trust so far—but in the long run, hope is not an acceptable strategy.

We meet – Section 702 allows for mass surveillance of US persons

Wilhelm 14 – writer for TechCrunch (Alex, “Why Section 702 Reform Matters”, Techcrunch, 07/6/14, <http://techcrunch.com/2014/07/06/why-section-702-reform-matters/?ncid=rss>)//GK

A recent report in the Washington Post delved into the National Security Agency’s (NSA) Section 702 surveillance activities, and although it found that the program returns useful information to the agency, it also revealed broad use of the legal authority to collect data and communications from non-target parties. It also

indicated that “unmasked identities remain in the NSA’s files, and the agency’s policy is to hold on to ‘incidentally’ collected U.S. content, even if it does not appear to contain foreign intelligence.” In short under the legal purview of Section 702 of the Foreign Intelligence Surveillance Act (FISA), the NSA regularly collects — albeit in a roundabout fashion, and likely not one as robust and complete as it would like — data and communications of United States citizens that it hangs onto even if it has no immediate merit relating to national security. The Post did not go into too much detail on the “valuable” information the sweeps returned for national security reasons, but noted the searches provided the government with information about a secret overseas nuclear project and the identities of cyber hackers attacking U.S. networks. But the sweeps also provided the government agency with detailed information about the lives of more than 10,000 people who were not necessarily being targeted by the NSA. The Post report described the files, “determined as useless but nonetheless retained” as running the gamut from illicit sexual liaisons to financial anxieties. Pictures, including mothers kissing their infants and women modeling lingerie, were picked up in the broad searches. As we have recently seen, the NSA is unafraid to use its authority to search its pooled data — that it collects directly from technology companies and by tapping the core fiber cables of the Internet — with “selectors” that relate to United States persons. The Post report is damning in detailing the painful laxity that appears to pervade our national intelligence apparatus. In one example, it cites an analyst who inferred that every member of the chat friend list of a known foreigner to be foreign as well, a view so broad as to be almost ridiculous. The report also indicates that Section 702 authority is often used when traditional warrants expire: In an ordinary FISA surveillance application, the judge grants a warrant and requires a fresh review of probable cause — and the content of collected surveillance — every 90 days. When renewal fails, NSA and allied analysts sometimes switch to the more lenient standards of PRISM and Upstream. “These selectors were previously under FISA warrant but the warrants have expired,” one analyst writes, requesting that surveillance resume under the looser standards of Section 702. The request was granted. This matters as there has been action in the United States Congress to ban using so-called “backdoor” searches on United States persons. A backdoor search under Section 702 is when stored data is queried using search terms to find the communications of Americans. The NSA, under Section 702, cannot go out and try to collect the communications of a known United States person, but it can search what it picks up “incidentally.” Given the NSA’s own admitted broad use of Section 702, and that the FBI and CIA also use similar methods, and especially that the NSA’s incredibly broad interpretation of what it can collect under the rule, the amount of data and communications in its databases stemming from United States persons must be massive. And it has the authority to query that information without securing a warrant. The NSA and the executive branch do not view backdoor searches as outside the letter, or spirit, of the law, according to their recent comments appended to the data released concerning the use of such authority.

Section 702 is used to spy on U.S. citizens

Kayyali, J.D., 14 [Nadia, 2012 Bill of Rights Defense Committee Legal Fellow where they worked with grassroots groups to restrict the reach of overbroad national security policies. Nadia earned a B.A. from UC Berkeley, with a major in Cultural Anthropology and minored in Public Policy. Nadia received a J.D. from UC Hastings, ACLU of Northern California and Bay Area Legal Aid. , The Way the NSA Uses Section 702 is Deeply Troubling. Here’s Why., <https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why>] Schloss

The NSA has confirmed that it is searching Section 702 data to access American’s communications without a warrant, in what is being called the "back door search loophole." In response to questions from Senator Ron Wyden, former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers," for example email addresses associated with someone in the U.S.

AT Terrorism

AT Terrorism if no Surveillance

Surveillance doesn't solve terror

Cahall et al '14 [Bailey Cahall, research associate for the National Security Studies program at the New America Foundation, David Sterman, program associate at New America and holds a master's degree from Georgetown's Center for Security Studies, Emily Schneider is a senior program associate for the International Security Program at New America, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" January 13, <https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/>]

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined. Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it's unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government's investigations of these cases: <http://natsec.newamerica.net/nsa/analysis>). Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaa Moalin, a San Diego cabdriver who in 2007 and 2008 provided \$8,500 to al-Shabaab, al-Qaeda's affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to "connect the dots" faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA's phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it's unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin's calls, despite official statements that the bureau had Moalin's phone number and had identified him. This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues. Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange. In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used. We have also identified three additional plots that the government has not publicly claimed as NSA successes, but in which court records and public reporting suggest the NSA had a role. However, it is not clear whether any of those three cases involved bulk surveillance programs. Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

More data is not needed – all attacks accomplished by known terrorists

Matthias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Almost every major terrorist attack on Western soil in the past fifteen years has been committed by people who were already known to law enforcement. One of the gunmen in the attack on Charlie Hebdo, in Paris, had been sent to prison for recruiting jihadist fighters. The other had reportedly studied in Yemen with Umar Farouk Abdulmutallab, the underwear bomber, who was arrested and interrogated by the F.B.I. in 2009. The leader of the 7/7 London suicide bombings, in 2005, had been observed by British intelligence meeting with a suspected terrorist, though MI5 later said that the bombers were "not on our radar." The men who planned the Mumbai attacks, in 2008, were under electronic surveillance by the United States, the United Kingdom, and India, and one had been an informant for the Drug Enforcement Administration. One of the brothers accused of bombing the Boston Marathon was the subject of an F.B.I. threat assessment and a warning from Russian intelligence In each of these cases, the authorities were not wanting for data. What they failed to do was appreciate the significance of the data they already had. Nevertheless, since 9/11, the National Security Agency has sought to acquire every possible scrap of digital information—what General Keith Alexander, the agency's former head, has called "the whole haystack." The size of the haystack was revealed in June, 2013, by Edward Snowden. The N.S.A. vacuums up Internet searches, social-media content, and, most controversially, the records (known as metadata) of United States phone calls—who called whom, for how long, and from where. The agency stores the metadata for five years, possibly longer.

Ybarra 5-21-15 [Maggie, The Washington Times, "FBI admits no major cases cracked with Patriot Act snooping powers," <http://www.washingtontimes.com/news/2015/may/21/fbi-admits-patriot-act-snooping-powers-didnt-crack/?page=all>]

FBI agents can't point to any major terrorism cases they've cracked thanks to the key snooping powers in the Patriot Act. the Justice Department's inspector general said in a report Thursday that could complicate efforts to keep key parts of the law operating. Inspector General Michael E. Horowitz said that between 2004 and 2009, the FBI tripled its use of bulk collection under Section 215 of the Patriot Act, which allows government agents to compel businesses to turn over records and documents, and increasingly scooped up records of Americans who had no ties to official terrorism investigations. The FBI did finally come up with procedures to try to minimize the information it was gathering on nontargets, but it took far too long. Mr. Horowitz said in the 77-page report, which comes just as Congress is trying to decide whether to extend, rewrite or entirely nix Section 215. Backers say the Patriot Act powers are critical and must be kept intact, particularly with the spread of the threat from terrorists. But opponents have doubted the efficacy of Section 215, particularly when it's used to justify bulk data collection such as in the case of the National Security Agency's phone metadata program, revealed in leaks from former government contractor Edward Snowden. The new report adds ammunition to those opponents, with the inspector general concluding that no major cases have been broken by use of the Patriot Act's records-snooping provisions. "The agents we interviewed did not identify any major case developments that resulted from use of the records obtained in response to Section 215 orders," the inspector general concluded — though he said agents did view the material they gathered as "valuable" in developing other leads or corroborating information.

Intel-gathering won't stop terrorists- past attacks prove

Schwartz 1-26-15 [Mattathias covers national security issues for The New Yorker, "The Whole Haystack," <http://www.newyorker.com/magazine/2015/01/26/whole-haystack>]

Almost every major terrorist attack on Western soil in the past fifteen years has been committed by people who were already known to law enforcement. One of the gunmen in the attack on Charlie Hebdo, in Paris, had been sent to prison for recruiting jihadist fighters. The other had reportedly studied in Yemen with Umar Farouk Abdulmutallab, the underwear bomber, who was arrested and interrogated by the F.B.I. in 2009. The leader of the 7/7 London suicide bombings, in 2005, had been observed by

British intelligence meeting with a suspected terrorist, though MI5 later said that the bombers were “not on our radar.” The men who planned the Mumbai attacks, in 2008, were under electronic surveillance by the United States, the United Kingdom, and India, and one had been an informant for the Drug Enforcement Administration. One of the brothers accused of bombing the Boston Marathon was the subject of an F.B.I. threat assessment and a warning from Russian intelligence. In each of these cases, the authorities were not wanting for data. What they failed to do was appreciate the significance of the data they already had. Nevertheless, since 9/11, the National Security Agency has sought to acquire every possible scrap of digital information—what General Keith Alexander, the agency’s former head, has called “the whole haystack.” The size of the haystack was revealed in June, 2013, by Edward Snowden. The N.S.A. vacuums up Internet searches, social-media content, and, most controversially, the records (known as metadata) of United States phone calls—who called whom, for how long, and from where. The agency stores the metadata for five years, possibly longer.

Surveillance fails- even targeted operations haven’t involved attacks

Nakashima ’14 [Ellen Nakashima is a national security reporter for The Washington Post, “NSA phone record collection does little to prevent terrorist attacks, group says,” 1-12-14, http://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html]

An analysis of 225 terrorism cases inside the United States since the Sept. 11, 2001, attacks has concluded that the bulk collection of phone records by the National Security Agency has had no discernible impact on preventing acts of terrorism” In the majority of cases, traditional law enforcement and investigative methods provided the tip or evidence to initiate the case, according to the study by the New America Foundation, a Washington-based nonprofit group. The study, to be released Monday, corroborates the findings of a White House-appointed review group, which said last month that the NSA counterterrorism program “was not essential to preventing attacks” and that much of the evidence it did turn up “could readily have been obtained in a timely manner using conventional [court] orders.” Under the program, the NSA amasses the metadata — records of phone numbers dialed and call lengths and times — of virtually every American. Analysts may search the data only with reasonable suspicion that a number is linked to a terrorist group. The content of calls is not collected. The new study comes as President Obama is deliberating over the future of the NSA’s bulk collection program. Since it was disclosed in June, the program has prompted intense debate over its legality, utility and privacy impact. Senior administration officials have defended the program as one tool that complements others in building a more complete picture of a terrorist plot or network. And they say it has been valuable in knocking down rumors of a plot and in determining that potential threats against the United States are nonexistent. Director of National Intelligence James R. Clapper Jr. calls that the “peace of mind” metric. In an opinion piece published after the release of the review group’s report, Michael Morell, a former acting CIA director and a member of the panel, said the program “needs to be successful only once to be invaluable.” The researchers at the New America Foundation found that the program provided evidence to initiate only one case, involving a San Diego cabdriver, Basaaly -Moalin, who was convicted of sending money to a terrorist group in Somalia. Three co-conspirators were also convicted. The cases involved no threat of attack against the United States. “The overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don’t sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques,” said the report, whose principal author is Peter Bergen, director of the foundation’s National Security Program and an expert on terrorism.

FBI had plenty of data prior to 9-11 and didn’t act on it

Matthias Schwartz, January 26, 2015, The New Yorker, “The Whole Haystack,” <http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

In retrospect, every terrorist attack leaves a data trail that appears to be dotted with missed opportunities. In the case of 9/11, there was Mihdhar’s landlord, the airport clerk who sold Mihdhar his one-way ticket for cash, and the state trooper who pulled over another hijacker on September 9th. In August, 2001, F.B.I. headquarters failed to issue a search warrant for one of the conspirators’ laptops, despite a warning from the Minneapolis field office that he was “engaged in preparing to seize a Boeing 747-400 in commission of a terrorist act.” There was plenty of material in the haystack.

The government had adequate tools to collect even more. **The problem was the tendency of intelligence agencies to hoard information, as well as the cognitive difficulty of anticipating a spectacular and unprecedented attack.** The 9/11 Commission called this a “failure of the imagination.” **Finding needles, the commission wrote in its report, is easy when you’re looking backward, deceptively so.** They quoted the historian Roberta Wohlstetter writing about Pearl Harbor: It is much easier *after* the event to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear; we can now see what disaster it was signaling since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meanings.

Soo many other problems with the FBI – surveillance doesn’t solve

Sink and Wilber 15 — Justin, Del Quentin Bloomberg politics Lone Wolf Terrorists, Cyber Threats Put New Pressure on FBI
<http://www.bloomberg.com/politics/articles/2015-03-25/fbi-must-evolve-to-tackle-lone-wolf-online-threats-report-says>

(Bloomberg) — **The FBI urgently needs to accelerate intelligence-gathering capabilities at home and abroad to confront evolving terrorist threats,** a panel reviewing the bureau’s response since the Sept. 11 attacks said. Returning **foreign fighters, extremists acting alone,** and a **new breed of criminals in cyberspace mean the agency needs to build up its domestic intelligence operation,** the yearlong review of the Federal Bureau of Investigation found. **The FBI has not yet met its potential** — or its mandate from the president and Congress — **to develop a ‘specialized and integrated national security workforce’** that can serve as the hub of America’s domestic intelligence agency,” according to the report, which was presented to FBI Director James Comey. The review was undertaken at the request of Congress, which sought an update on how the FBI is fulfilling its mission since the 2001 terrorist attacks in New York and Washington. It was led by Edwin Meese, attorney general under President Ronald Reagan, former Representative Tim Roemer, an Indiana Democrat, and Georgetown University counterterrorism expert Bruce Hoffman. The report was released during a press conference with Comey and members of the panel Wednesday at FBI headquarters in Washington. Counterterrorism Priority The panel found that the FBI had largely succeeded at transforming itself after Sept. 11, developing a workforce attuned to the importance of intelligence-gathering and putting a priority on counterterrorism. **The FBI needs to do more to support, train and equip agents and analysts with the latest technologies to combat the changing nature of threats from jihadist groups such as Islamic State,** it said. “Some **things are necessary, we feel, to keep pace with the accelerating threat we find around the world.**” Meese said. “So there has to be an acceleration, obviously, in the amount of effort and the changes being made to bring the FBI” up to date, he said. Comey said that he generally agrees with the report’s findings, including the recommendation that the agency must change further. **Leadership at the agency isn’t “unified or consistent in driving cultural change,”** partially because of frequent turnover, according to the report. **An office dedicated to countering violent extremism is underfunded** and should be moved under the Department of Homeland Security, and the agency’s efforts to counter cyberthreats aren’t integrated well enough with other agencies, according to the report. Intelligence Integration **The FBI needs to invest more in collaborative relationships** with foreign partners as it seeks to combat terrorist threats. In the U.S., **the FBI isn’t “sufficiently integrated” into the intelligence community,** to the detriment of its own criminal investigations, according to the report. Regional FBI leaders were found to often give competing interests priority over intelligence-collection and coordination with other agencies. The panel urged Comey to work more closely with Director of National Intelligence James Clapper to help the U.S. national security community. **FBI agents and analysts should also participate in interagency collaboration and training assignments,** according to the panel. “The FBI must better use its strategic processes to drive the intelligence cycle for its law enforcement and intelligence missions,” according to the review. More Pressure Pressure the FBI to combat terrorism within the U.S. has intensified since the Islamic State emerged, with top administration officials repeatedly warning that the terror group could target the U.S. homeland. Last month, the White House hosted a summit on countering violent extremism, and President Barack Obama has pushed efforts at the United Nations to target foreign fighters. The panel recommended that FBI leaders communicate to Congress the value of laws integral to several successful investigations since 2008, such as the USA Patriot Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act. Privacy advocates and some companies are opposed to some provisions of those laws. The FBI showed lax communication, coordination, collaboration and use of human intelligence in five case studies analyzed by the review commission. Those included U.S. Army Major Nidal Hasan and the Fort Hood shooting, Faisal Shahzad and the bungled Times Square car-bomb attack, and Tamerlan and Dzhokhar Tsarnaev and the Boston Marathon bombing. **The FBI will fulfill its domestic intelligence role when its analysts and collectors, like its special agents, are grounded in criminal investigation; have ready access to state-of-the-art technology; continuously exploit the systems, tools, and relationships of the national intelligence agencies,**” the report concluded.

Mass surveillance **doesn’t prevent terrorism.**

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation’s Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Felix Macherez, 2015 (“This Security Expert Reckons Mass Surveillance Doesn’t Stop Terror Attacks,” *Vice*, June 26th, Available Online at

https://www.vice.com/en_uk/read/bruce-schneier-mass-surveillance-wont-stop-terror-876, Accessed 07-12-2015)

Is there any proof that the omnipresent surveillance that exists in the US – on the internet, with phone conversations – has actually helped to stop terrorist attacks in the past?

No. It's now a clear fact that the mass surveillance performed in the US has never stopped a single attack. On several occasions, the government was asked to justify its surveillance methods, and they have failed to ever do so. Sometimes, they provide scenarios and vague plans, but the data never withstands any test.

Are there better ways of stopping terrorist attacks then in your opinion?

What works and has proven efficient several times in the US, is to use "conventional" detective techniques – just following the clues. However there's an important caveat here: no method of surveillance or inquiry will ever stop a lone gunman.

There are simply never enough hints to stop the aggressor before he acts in such cases. Individuals such as the Fort Hood shooter, or Anders Behring Breivik , or the Charlie Hebdo attackers in France, will always be a problem. Early intervention aimed at identifying and helping troubled individuals before they become murderers is the only real solution here.

Mass surveillance can't stop terrorism — too much data.

Schneier 15 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Felix Macherez, 2015 ("This Security Expert Reckons Mass Surveillance Doesn't Stop Terror Attacks," *Vice*, June 26th, Available Online at https://www.vice.com/en_uk/read/bruce-schneier-mass-surveillance-wont-stop-terror-876, Accessed 07-12-2015)

VICE: The NSA uses the metaphor "connecting the dots" to justify its surveillance activities. However the US government actually struggles to ever connect those dots. Why is that?

Bruce Schneier: There is too much external noise when you do mass surveillance. The problem is that "connecting the dots" is neither the right method nor the right metaphor. When you look at a child's colouring book, connecting the dots is very easy because they are all visible – they are all on the same page and they have numbers written on them. All you have to do is move the lead of your pencil across your page, from one dot to the other, and there you go – the drawing is done.

In reality, those "dots" can only be seen and connected after things have occurred – so after each terrorist attack, if you want. When you look, it's easy to make the link between, say, an information request coming from Russia, a visit abroad, and other potential information gathered elsewhere. So with hindsight, we know who the terrorists are. That's why we're able to chase after them, but not stop them. Before an event occurs, there is an extremely huge number of potential "human dangers," and an even greater number of possible scenarios. There are so many variables to take into account that it's impossible to rely on a single potential course of events.

You're saying that mass surveillance cannot really stop terrorist attacks in the US. Would you say the same for France?

Mass surveillance is unreliable for statistical reasons, not for cultural or linguistic reasons. That analysis is valid for all countries, including France.

AT NSA Surveillance Key to stopping terrorism

NSA doesn't aid in detection efforts – surveillance has a negligible impact

Benkler 13 -- Yochai Benkler is a law professor and director of the Berkman Center for Internet & Society at Harvard University. "Fact: the NSA gets negligible intel from Americans' metadata. So end collection" <http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadatasurveillance-intelligence>

Congress may be on the verge of prohibiting the NSA from continuing its bulk telephony metadata collection program. Two weeks ago, the Senate national security dissenters: Wyden, Udall, Paul, and Blumenthal proposed prohibition. Last week, the move received a major boost from a bipartisan proposal by core establishment figures: Senator Patrick Leahy, and Representatives Jim Sensenbrenner and John Conyers. It's a prohibition whose time has come.

Dragnet surveillance, or bulk collection, goes to the heart of what is wrong with the turn the NSA has taken since 2001. It implements a perpetual "state of emergency" mentality that inverts the basic model outlined by the fourth amendment: that there are vast domains of private action about which the state should remain ignorant unless it provides clear prior justification. And all public evidence suggests that, from its inception in 2001 to this day, **bulk collection has never made more than a marginal contribution to securing Americans from terrorism, despite its costs**.

In a 2 October hearing of the Senate judiciary committee, Senator Leahy challenged the NSA chief, General Keith Alexander: Would you agree that **the 54 cases that keep getting cited by the administration were not all plots, and that of the 54 only 13 had some nexus to the US?** Would you agree with that, yes or no? Alexander responded: Yes. Leahy then demanded that

Alexander confirm what his deputy, Christopher Inglis, had said in the prior week's testimony: that **there is only one example where collection of bulk data is what stopped a terrorist activity**. Alexander responded that Inglis might have said two, not one. Advertisement In fact, what Inglis had said the week before was that there was one case "that comes close to a but-for example and that's the case of Basaly Moalin". So, who is Moalin, on whose fate the NSA places the entire burden of justifying its metadata collection program? Did his capture foil a second 9/11? A cabby from San Diego, Moalin had immigrated as a teenager from Somalia. In February, he was convicted of providing material assistance to a terrorist organization: he had transferred \$8,500 to al-Shabaab in Somalia. After the Westgate Mall attack in Nairobi, few would argue that al-Shabaab is not a terrorist organization. But al-Shabaab is involved in a local war, and is not invested in attacking the US homeland. The indictment against Moalin explicitly stated that al-Shabaab's enemies were the present Somali government and "its Ethiopian and African Union supporters". Perhaps, it makes sense for prosecutors to pursue Somali Americans for doing essentially what some Irish Americans did to help the IRA; perhaps not. But this single successful prosecution, under **a vague criminal statute, which stopped a few thousand dollars from reaching one side in a local conflict in the Horn of Africa, is the sole success story for the NSA bulk domestic surveillance program**.

At the hearing, perhaps trying to bolster Alexander's feeble defense of the program's effectiveness, Director of National Intelligence James Clapper complained that "plots foiled" should not be the metric. He said: There's another metric I would use; let's call it the "peace of mind metric". In the case of the Boston Marathon bomber, we were able to use these tools to determine whether there was, or was not, a subsequent plot in NYC. Clapper actually used the clearest example that his program offers Americans little real security – its failure to pick up the Tsarnaev brothers before they attacked – as a way of persuading us that we should use an amorphous and unmeasurable "peace of mind" metric; peace of mind we should gain from knowing that the same system that failed to detect the Boston bombers also detected no bombers in New York. One is left picturing Inspector Clouseau: I did not know the bank was being robbed because I was engaged in my sworn duty as a police officer. The admissions Leahy forced out of the NSA heads and DNI Clapper that they have been systematically overstating the effectiveness of bulk collection are consistent with the only other official assessments of bulk collection. The sole publicly available FISC opinion (pdf) that assesses the impact of bulk collection from 2004 to 2009 was unimpressed that: [T]he government's submission cites three examples in which the FBI opened three new preliminary investigations of persons in the US based on tips from the BR metadata program. Judge Walton wrote that this achievement "does not seem particularly significant". Perhaps most damning are the results of the consensus report authored by the five inspectors general of the Departments of Defense and Justice and the CIA, NSA, and Office of DNI, mandated by Congress as part of the Fisa Amendments Act of 2008. That report provides the most detailed official assessment of the effectiveness of bulk collection, from inception as the President's Surveillance Program (PSP) in the fall of 2001 until 2007. It is revealing about both the NSA and its bulk collection program. **The NSA's inspector general only reported the agency's top brass beliefs; his report merely quoted then NSA Director Michael Hayden in his view that there were "no communications more important to NSA efforts to defend the nation". Other inspectors general were more skeptical. The Department of Justice "concluded that although PSP-derived information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts**". The CIA reported: [W]orking-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP reporting. Officials also stated that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP. The inspector general of the DNI reported that "National Counterterrorism Center analysts characterized the PSP information as being a useful tool, but noted that the information was only one of several valuable sources of information available to them", and "not of greater value than other sources of intelligence". It is hardly surprising that supporters of bulk collection fervently believe it is critical to national security. No psychologically well-balanced person could permit herself to support a program that compromises the privacy of tens of millions of Americans, costs billions of dollars, and imposes direct and articulable harm to cyber security by undermining the security of commercial products and public standards without holding such a belief truly and honestly. But the honest faith of insiders that their bureaucratic mission is true and critical is no substitute for credible evidence. **A dozen years of experience has produced many public overstatements and much hype from insiders, but nothing to support the proposition that the program works at all, much less that its marginal contribution is significant enough to justify its enormous costs in money, freedom, and destabilization of internet security. No rational cost-benefit analysis could justify such a leap of faith. If the NSA cannot show real, measurable evidence of its effectiveness, evidence that doesn't collapse as soon as it is examined and isn't a vague appeal to amorphous, measurement-free "peace of mind", its bulk collection program has to go.**

AT Surveillance Stopped 54 Attacks

The 54 number has been thoroughly discredited. So has “it stopped 9/11.”

Cohn 14 — Cindy Cohn, Executive Director and former Legal Director and General Counsel of the Electronic Frontier Foundation, holds a J.D. from the University of Michigan Law School, and Nadia Kayyali, Activist at the Electronic Frontier Foundation, holds a J.D. from the University of California-Hastings, 2014 (“The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible,” Electronic Frontier Foundation, June 2nd, Available Online at <https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible>, Accessed 07-12-2015)

1. The NSA has Stopped 54 Terrorist Attacks with Mass Spying

The discredited claim

NSA defenders have thrown out many claims about how NSA surveillance has protected us from terrorists, including repeatedly declaring that it has thwarted 54 plots. Rep. Mike Rogers says it often. Only weeks after the first Snowden leak, US President Barack Obama claimed: “We know of at least 50 threats that have been averted” because of the NSA’s spy powers. Former NSA Director Gen. Keith Alexander also repeatedly claimed that those programs thwarted 54 different attacks.

Others, including former Vice President Dick Cheney have claimed that had the bulk spying programs in place, the government could have stopped the 9/11 bombings, specifically noting that the government needed the program to locate Khalid al Mihdhar, a hijacker who was living in San Diego.

Why it’s not credible:

These claims have been thoroughly debunked. First, the claim that the information stopped 54 terrorist plots fell completely apart. In dramatic Congressional testimony, Sen. Leahy forced a formal retraction from NSA Director Alexander in October, 2013:

"Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S.?" Leahy said at the hearing.
"Would you agree with that, yes or no?"

"Yes," Alexander replied, without elaborating.

But that didn’t stop the apologists. We keep hearing the “54 plots” line to this day.

As for 9/11, sadly, the same is true. The government did not need additional mass collection capabilities, like the mass phone records programs, to find al Mihdhar in San Diego. As ProPublica noted, quoting Bob Graham, the former chair of the Senate Intelligence Committee:

U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al Mihdhar, long before 9/11 and had the ability find him, but they failed to do so.

"There were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar," says former Senator Bob Graham, the Florida Democrat who extensively investigated 9/11 as chairman of the Senate's intelligence committee.

Moreover, Peter Bergen and a team at the New America Foundation dug into the government's claims about plots in America, including studying over 225 individuals recruited by al Qaeda and similar groups in the United States and charged with terrorism, and concluded:

Our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading...

When backed into a corner, the government's apologists cite the capture of Zazi, the so-called New York subway bomber. However, in that case, the Associated Press reported that the government could have easily stopped the plot without the NSA program, under authorities that comply with the Constitution. Sens. Ron Wyden and Mark Udall have been saying this for a long time.

Both of the President's hand-picked advisors on mass surveillance concur about the telephone records collection. The President's Review Board issued a report in which it stated "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks." The Privacy and Civil Liberties Oversight Board (PCLOB) also issued a report in which it stated, "we have not identified a single instance involving a threat to the United States in which [bulk collection under Section 215 of the Patriot Act] made a concrete difference in the outcome of a counterterrorism investigation."

And in an amicus brief in EFF's case First Unitarian Church of Los Angeles v. the NSA case, Sens. Ron Wyden, Mark Udall, and Martin Heinrich stated that, while the administration has claimed that bulk collection is necessary to prevent terrorism, they "have reviewed the bulk-collection program extensively, and none of the claims appears to hold up to scrutiny."

Even former top NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US and at most, helped catch one guy who shipped about \$8,000 to a Somalian group that the US has designated as a terrorist group but that has never even remotely been involved in any attacks aimed at the US.

Don't trust NSA's numbers *even though* some info is classified.

Van Dongen 13 — Teun van Dongen, National Security Expert and a Ph.D. Candidate in Counterterrorism Studies at Leiden University, former Analyst at The Hague Centre for Strategic Studies where he worked for the Dutch National Coordinator for Security and Counterterrorism, 2013 ("The NSA Isn't Foiling Terrorist Plots," *Foreign Policy In Focus*, October 8th, Available Online at <http://fpif.org/nsa-isnt-foiling-terrorist-plots/>, Accessed 07-09-2015)

What about the NSA?

Admittedly we do not know how all terrorist plots have been detected. But going by what we do know, the conclusion is simple: terrorist plots have been foiled in all sorts of ways, few of which had anything to do with mass digital surveillance. True, in the case of the dismantlement of the Sauerland Cell in Germany in 2007, NSA information played a role. But whether the authorities got this information from "digital dragnet surveillance" or from more individualized and targeted monitoring is hard to tell.

It might be tempting to give the NSA the benefit of the doubt, given that the organization speaks on the basis of information that we do not have. But such dubious claims about the effectiveness of the digital surveillance programs fit seamlessly into a pattern of misinformation and deceit.

The U.S. government acknowledged the existence of PRISM only after Edward Snowden had leaked details about it to The Guardian. Moreover, when the news broke, President Obama and Director of National Intelligence James Clapper tried to downplay the scale of the digital data gathering, even though we know now that the NSA is essentially making a back-up of pretty much all conceivable forms of online communication. President Obama further promised that “nobody is listening to your phone calls,” but it later became clear that the NSA can access the content of phone calls and e-mails if it so desires. Congressional oversight is poor, privacy rules are frequently broken, and the NSA liberally shares data with other intelligence agencies and foreign governments.

Against this background of disputed or outright false government claims, the public is wise to be skeptical of the NSA’s claims about the effectiveness of the digital surveillance programs. The recent revelations may be mind-boggling in their technological, legal, and procedural complexities, but the bottom line is quite simple: The first credible piece of evidence that these programs are doing any good in the fight against terrorism has yet to surface. Until such evidence is provided, the Obama administration is only eroding the trust of the citizens it is claiming to protect.

IT Benjamin Wittes — General

Wittes is an NSA propagandist — ignore him.

Gosztola 15 — Kevin Gosztola, journalist, author, and documentary filmmaker known for work on whistleblowers, WikiLeaks, national security, secrecy, civil liberties, and digital freedom, has written for *The Nation*, *Salon*, and *OpEdNews*, 2015 (“Former NSA Director’s Favorite Blogger Was Invited to Give Constitution Day Speech at NSA,” *Firedoglake*—a progressive news site, February 25th, Available Online at <http://dissenter.firedoglake.com/2015/02/25/former-nsa-directors-favorite-blogger-was-invited-to-give-constitution-day-speech-at-nsa/>, Accessed 07-12-2015)

The National Security Agency marked Constitution Day in September by inviting one of the United States national security state’s most favorite bloggers, Benjamin Wittes, who is the editor-in-chief of Lawfare, to give a speech.

The address was made even more remarkable by the fact that Wittes had intended to post his unclassified speech soon after but was stymied by the very secrecy, which he has relentlessly pilloried NSA whistleblower Edward Snowden for challenging through his disclosures. So, until February 21, he was unable to post audio of the speech.

For those unfamiliar with Wittes, he is a senior fellow in Governance Studies at the Brookings Institution, a major Beltway think tank. He also is on the Hoover Institution’s Task Force on National Security and Law. More importantly, he is someone who former NSA director Keith Alexander and Hillary Clinton like to read and is popular among officials in US intelligence agencies because his blog focuses on the “hard national security choices” US intelligence agencies have to make each day.

Wittes testified before the Senate Select Committee on Intelligence on September 23, 2013, that Snowden’s “disclosures show no evidence of any intentional, unlawful spying on Americans or abuses of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures. They show earnest and serious efforts to keep the Congress informed—including members not on this committee or its counterpart in the House of Representatives. And they show an ongoing dialogue with the Foreign Intelligence Surveillance Court (FISC) about the parameters of the agency’s legal authorities and a commitment both to keeping the court informed of activities and to complying with its judgments as to their legality.” [PDF]

He is just the type of person the NSA would want to address its analysts or officers because he reflects and champions the exact agency thinking, which has directly come under scrutiny as a result of Snowden.

Now, before proceeding, Wittes preemptively responded to critics (“NSA foes”), who would write posts like this one:

It was an honor and pleasure to give this speech before an agency in whose work I believe and whose workforce has taken a huge and largely unfair beating. I hope my comments stimulated thought and challenged people at the agency. And while people are free, of course, to decide that either the fact of the speech or its contents confirm whatever they already believed about me and NSA, I would hope they might instead—or in addition—engage some of the ideas I put forth.

Let's engage a few ideas in the Constitution Day speech and then return to the best part about all this, which is that Wittes had to wait about five months for the NSA to declassify an unclassified speech before he could post the audio of it.

Wittes opens his speech by noting that it was "moving" to him that he would be invited to speak at a time of "stress" and "unwanted publicity" for the NSA. He then proceeds to call Constitution Day an "odd day" and a "weird event." He notes that Democratic Senator Robert Byrd was largely responsible for the institution of the day and that every educational institution that gets federal funds must observe Constitution Day. Without really any evidence whatsoever, he suggests this is burdensome for small colleges to observe primarily because they have to invite people like him. But colleges do not have to invite expensive speakers to do events and can distribute literature about the Constitution or observe the day in other ways.

Most of the speech to the NSA is committed to contemplating how the NSA should handle a political reality, where there is this cloud of suspicion about what it does as an agency. But Wittes does not specifically highlight the Constitution and whether the NSA adheres to it through its operations nor does he use the multiple legal challenges to NSA surveillance in courts to make specific arguments about the constitutionality of US intelligence operations. He instead opts to rationalize the suspicion the public has toward the NSA as something wholly inadequate and invalid.

The result is a speech that reinforces the siege mentality that the agency does not deserve to be under so much public criticism—and here is what can be done to survive this moment.

Wittes argues that the intelligence community may do "ugly stuff" but so do other federal government agencies. The government can threaten to kill you or put you in "a small box" for the rest of your life. "The fact that there is ugly stuff done in the intelligence community is both true and utterly inadequate as an explanation for this kind of deep reservoir of suspicion." It is a race to the bottom kind of argument. Why be suspicious of agencies like the NSA when other agencies can commit gross abuses of power too? (Pretty nuts.)

To him, secrecy is not a legitimate argument for why people are suspicious of intelligence operations. He suggests "a huge amount of what the government does is functionally secret, if only because nobody happens to [submit Freedom of Information Act (FOIA) requests for] it or because it would be subject—if not classified—it would be subject to some FOIA exemption or another. And parts of the government we, in fact, trust a great deal have huge levels of secrecy that we don't really mind all that much. Or, we kind of fight about the appropriate levels of secrecy, but we do it without developing a deep, deep suspicion of the day-to-day operations."

It is unclear how Wittes happens to know what the public seeks when submitting FOIA requests. However, generally speaking, the amount of FOIA requests for government records has been increasing each year and more Americans than under President George W. Bush are filing lawsuits to force the government to comply with FOIA.

Wittes' argument can be demolished simply by stating the fact that certain material being kept secret through FOIA exemptions does not invalidate or delegitimize suspicion of security agencies. It reinforces suspicion, especially when there is increased awareness of the "state secrets privilege" being abused in courts.

The Supreme Court is not subject to FOIA, Wittes notes. However, that does not help one argue that secrecy cannot explain suspicion toward security agencies. If anything, one might say the institutional secrecy of the highest court in the US accentuates the perceived corruption of US intelligence agencies.

The most entralling part of his speech is when Wittes attempts to explain the distrust of NSA and other clandestine agencies by suggesting that the Constitution is incompatible with their operations. For example, people who cooperate with agents are heralded as assets or heroes while those who turn against agencies are traitors or criminals. Wittes acknowledges that former NSA director Michael Hayden cheerfully admitted that the agency steals secrets. If he stole secrets, it would be criminal, but the NSA is able to get away with doing it.

Wittes proudly defends this dynamic, even going so far to say that he does not feel like a hypocrite when confessing that he opposes what Edward Snowden did but would be thrilled if there was a hypothetical Chinese Edward Snowden. But he appears to at least understand that some of the more egregious activities revealed by Snowden suggest an agency that does not adhere to principles all citizens are expected to uphold. To NSA employees in the audience, that is okay.

He discusses transparency as one possible prescription for smoothing over relations with citizens. He makes it clear that he does not mean transparency through the release of documents or even copies of the policies or interpretations of the law, which NSA employs to justify operations. Rather, he advocates a “transparency of values,” such as “reasons why we have this building.” Wittes favors NSA not being apologetic about why NSA headquarters exists.

In other words, he favors the exact kind of so-called transparency former NSA director Keith Alexander and Director of National Intelligence James Clapper favor. It is the transparency the NSA urged personnel to employ at Thanksgiving dinners in 2013, when confronted with family critical of the agency.

Officials and think tankers like Wittes favor the proud declaratory expression of agency values as a way of helping citizens understand the stakes of what the national security state is allegedly up against to shift attention from unspeakable conduct. This is propaganda, not transparency.

And now that I have engaged parts of Wittes’ speech, as he wanted critic/foes to do rather than simply mock and laugh at him, let’s appreciate the poetic justice of the ordeal Wittes went through trying to get this speech posted online.

“I had meant to post the speech back then, except that it being NSA and all, I wasn’t allowed to bring my own recording equipment into the building and thus had to wait until the NSA folks released the audio of my own speech to me. This took a while—a long, long while, as it turned out,” according to Wittes.

“For reasons still unclear to me, my speech had to go through a lengthy review before it could be released, even to its author. This was particularly odd, since the event was unclassified, since I am not cleared to receive classified information in any event, since I was free at any time in the interim to give exactly the same speech somewhere else, and since I requested only my own words—not the words of any NSA official or any of the Q&A.”

Is Wittes pretending to be ignorant or does he seriously not understand the secrecy regime of an agency he champions and how it seeks to control all information that ever comes into its grasp?

Didn't part of his speech talk about how they are able to do things other people in democratic society are not supposed to do? Isn't classifying even the most innocuous information like his own speech one of those things?

Once Wittes gave his speech, it became property of NSA. It was theirs to classify so the public would not pick apart Wittes' speech and use it to further criticize NSA personnel. It did not matter how many concessions he made to the minions, who guard anything reflexively stamped secret. If agency wanted it to be public, it would be public when the public would care about it the least.

Though, it is not as if Wittes bothered to fight it. He did not write a post about what he said and complain about NSA secrecy while they were frustrating him. He sycophantically waited because he has staked his reputation over the past 18 months on defending the NSA and some laws that have become deeply unpopular because they grant them authorities that are abused or abusive. He is like an NSA groupie.

The NSA basically owns him at this point and, when someone at NSA says jump, Wittes says what time.

Wittes is a hack for NSA. Disregard his arguments.

Greenwald 12 — Glenn Greenwald, lawyer and journalist who published reports based on classified documents disclosed by Edward Snowden, Contributor to *Salon* and *The Guardian*, Recipient of the 2014 Pulitzer Prize for Public Service, holds a J.D. from New York University School of Law and a B.A. in Philosophy from George Washington University, 2012 ("The Brookings Institution demands servile journalism," *The Guardian*, October 15th, Available Online at <http://www.theguardian.com/commentisfree/2012/oct/15/drones-brookings-media>, Accessed 04-20-2015)

The very idea that government assertions are entitled to a presumption of truth even when they are shrouded in secrecy, subject to no accountability, and unaccompanied by proof, is the mindset of a servile government propagandist. It's astonishing that, even after what happened in the run-up to the Iraq War - when media outlets placed themselves in the supine posture exemplified by Wittes - that anyone is willing to stand up in public and advocate this model of government-subservient "journalism".

Then again, there should be nothing surprising about any of this given that both Brookings and Wittes are classic examples of that sprawling strain of Washington think tank culture that exist for little reason other than to serve and justify government power. They are pure expressions of the courtier Beltway mentality that demands that everyone else be as reverent of royal court prerogatives as they are.

Brookings, of course, was one of the leaders in persuading Americans, especially many American liberals, to support the attack on and eight-year occupation of Iraq, and it remains vocally in the lead in the fear-mongering campaign against Iran. Its national security "experts" have been lavishly funded by billionaire mogul Haim Saban, who has described himself as a "total hawk" and said: I'm a one-issue guy and my issue is Israel."

Wittes is not only a reflexive defender of the use of US military force, including drones, but recently supplied one of the creepier and more revealing episodes when he gathered with a former Bush Homeland Security official and their children to simulate "drone warfare" for fun, all while NPR giggled, watched and reported:

"It started as trash talk between two contributors to a national security blog. They decided to host a drone smackdown to see if one guy's machine could take down another. . . .

"The first contestant was a drone with interlocking black loops to protect the rotors, shaped like the burners on your stove top. The machine, nicknamed Stux2bu, belonged to [Ben] Wittes, co-founder of Lawfare, the blog that sponsored the contest. . . .

"They pointed out the name of their drone derived from the word Stuxnet, the infamous real-world computer virus discovered in June 2010 that targeted Iran's nuclear enrichment efforts."

This is what people do who spend their lives cheering for American military force and violence and killing but refuse to get anywhere near the fighting they adore: they play-act as tough-guy warriors, having some nice Sunday fun playing with weapons that routinely kill innocent people, including children, as they provide the intellectual justification and apologia from a safe distance. (After describing all of the fun drone festivities, NPR justified itself by adding on as a cursory afterthought: "To a lot of people, drones are no laughing matter. U.S. machines equipped with deadly missiles have killed al-Qaida leaders in Pakistan and Yemen. They've also killed some innocent civilians").

Although it may seem repellent, the view that media outlets should dutifully amplify rather than "aggressively challenge" government claims is quite pervasive, especially among establishment journalists themselves. Indeed, that is more or less what it means to be an "establishment journalist", and it is this mindset, more than any other, that explains how the attack on Iraq was able to be launched based on a mountain of falsehoods.

In 2004, Guardian columnist George Monbiot wrote: "the falsehoods reproduced by the media before the invasion of Iraq were massive and consequential: it is hard to see how Britain could have gone to war if the press had done its job." In a 2004 Guardian Op-Ed on the role played by the western media in enabling that attack, David Edwards and David Cromwell traced the last century's structural history of journalism in order to argue that mindlessly conveying government claims is no longer an abandonment of the purpose of modern journalism but rather a core fulfillment of it.

Edwards and Cromwell quoted ITV News political editor, Nick Robinson - responding to criticisms of his pre-war reporting - this way: "It was my job to report what those in power were doing or thinking . . . That is all someone in my sort of job can do." Countless American journalists, including the most influential ones, have expressed similar sentiments.

Those who believe that media institutions should serve as an adversarial check on government power will find Sullivan's column utterly uncontroversial and obvious. About Wittes' attack on Sullivan, the ACLU's Jameel Jaffer said this morning to Lawfare: "Now you are parodying yourselves."

But for those who devote themselves to serving, venerating and justifying the acts of those in power - like the Brookings Institution's Wittes - Sullivan's view is "very strange" indeed, even

offensive. To them, the very idea that government claims should be "aggressively challenged" is virtually blasphemous, a total contradiction of the goals to which they are devoted. As Kade Crockford put it today: "'aggressively challenging' the government on its claims has a way of helping the facts come out." That's precisely why Wittes and friends find it so distasteful.

The drone program is popular in part because US media outlets parrot US governments assertions and thus reflexively claim that the victims are "militants" - even though they have no idea who was actually killed, even though the term itself is wildly propagandistic, even though the Obama administration refuses to disclose basic evidence, and even though there is ample evidence proving how unreliable those claims are. Only by having media outlets refrain from "aggressively challenging" government claims can those claims, and thus support for drone attacks, be sustained. That's why Sullivan's call - made in the pages of the New York Times itself - is so threatening to some.

There really is no point in having media outlets that do anything other than "aggressively challenge" the claims of those in power. Actually, there is a point in having that: it allows government assertions to be glorified as true even when there is no evidence that they are. That is why so many power-serving Washington mavens are so eager to defend that model and demand adherence to it. And their success in that mission is why so many destructive government falsehoods are able to flourish without real scrutiny.

Wittes is an NSA apologist — his args are political doublespeak.

Masnich 14 — Mike Masnick, Founder and Chief Executive Officer of Floor64—a software company, Founder and Editor of *Techdirt*, 2014 (“Orwell Would Be Proud: NSA Defender Explains How Even Though NSA Spies On Americans, It’s OK To Say They Don’t,” *Techdirt*, February 6th, Available Online at <https://www.techdirt.com/articles/20140205/22492826105/orwell-would-be-proud-nsa-defender-explains-how-even-though-nsa-spies-americans-its-ok-to-say-they-dont.shtml>, Accessed 07-05-2015)

Benjamin Wittes of the Brooking Institution has become the go-to non-government NSA apologist. One of his most recent articles is a true work of rhetorical artistry, in which he tries to explain why saying "the NSA doesn't spy on Americans" is acceptable shorthand for the fact that the NSA spies on pretty much every American. It's a master class in political doubletalk. First, it's the law's fault. The law, you see, is too complicated for mere mortals not working for the NSA to understand, so that makes it okay to lie:

The law is so dense and so complicated that it cannot be accurately summarized at a level a citizen can reasonably process.

Any effort to summarize the relevant law necessarily ignores themes sufficiently important to its architecture that the reductionism will partake of serious inaccuracy. The person who told my friend that NSA does not spy on Americans was not lying. He or she was highlighting a crucially-important limitation on NSA’s authority vis a vis US persons. The law and the relevant regulations all contain significant territorial restrictions and significant protections for US persons overseas as well—all designed to separate the foreign intelligence mission of NSA from both domestic intelligence and domestic law enforcement. It’s a sincere and pervasive effort. “We don’t spy on Americans” is a

common shorthand for a wealth of law and practice that really and meaningfully keeps the agency out of the business of being a covert domestic intelligence agency.

Got that? Because there are some limitations on all the spying they do on Americans, and it's too complicated to understand those limitations, so it's okay to lie and say they don't spy on Americans. Of course, in the very next paragraph, Wittes tries to effectively brush away the massive amount of surveillance done on Americans.

NSA, after all, does spy on individual Americans with an order from the FISC. It does, moreover, capture all domestic telephony metadata. And most importantly, it does routinely capture communications between Americans and the targets of its surveillance and incidentally capture other material its systems scoop up overseas—subject to rules that limit the retention and processing of US person information. In other words, to say that NSA does not spy on Americans emphatically does not mean, as a reasonable student or citizen might expect it to mean, that the agency does not regularly acquire and process the communications of Americans.

Of course, as Jameel Jaffer from the ACLU points out, this is all nonsense because it's a simple fact that the NSA does do surveillance on Americans, and to claim otherwise is not acceptable shorthand. It's a lie. And while Wittes then tries to obfuscate things even more by trying and purposely failing to come up with a concise way of summarizing what the NSA does, Jaffer helps out with a few workable suggestions:

This is nonsense. Perhaps Ben's right that it's difficult to come up with a single sentence, or even a single paragraph, that clearly and comprehensively describes the nature and extent of the NSA's surveillance of Americans. (Can you describe any federal agency's functions in a single, comprehensive paragraph?) But it's not difficult to come up with a sentence more accurate than "The NSA doesn't spy on Americans." Try this one: "The NSA spies on Americans." Or this one: "The NSA collects a huge amount of information about Americans' communications and in many contexts it collects the communications themselves." Or this one: "The NSA is sometimes described as a foreign-intelligence agency but this label should not obscure the fact that a large part of the agency's energy is dedicated to collecting and analyzing information about Americans."

Jaffer further points out that Wittes's suggestion that those who claim the NSA doesn't spy on Americans are really trying to tell the truth through shorthand, is actually misleading. As Jaffer points out:

Any official who says the NSA isn't spying on Americans is seeking to mislead.

And anyone defending that statement is trying to support that fundamental attempt to mislead.

IT Benjamin Wittes — “Glenn Greenwald Bad”

Wittes uses “civility” as an excuse not to engage Greenwald’s substantive arguments about policy.

Greenwald 11 — Glenn Greenwald, lawyer and journalist who published reports based on classified documents disclosed by Edward Snowden, Contributor to *Salon* and *The Guardian*, Recipient of the 2014 Pulitzer Prize for Public Service, holds a J.D. from New York University School of Law and a B.A. in Philosophy from George Washington University, 2011 (“Brookings’ ‘centrist’ opposition to the rule of law,” *Salon*, January 14th, Available Online at http://www.salon.com/2011/01/14/lawlessness_4/, Accessed 04-20-2015)

UPDATE: I neglected to mention Wittes’ trite invocation of this platitude: this is about “the criminalization of policy differences — nothing more or less.” Anyone who dismisses as a mere “policy difference” the creation of a worldwide torture regime — featuring tactics the U.S. had long prosecuted and condemned when used by others and which were the signatures of history’s most brutal tyrannies — is exhibiting some truly warped thinking: not just legally and politically warped, but morally warped.

UPDATE II: The Brookings Scholar responds by explaining why he won’t respond: you see, as a defender of torturers, he’s much too high-minded and civil to engage those who aren’t. Leaving aside the fact that everything I wrote here was purely substantive, few people are in greater need of reviewing this satirically profane though brilliantly insightful post explaining the distinction between (a) decency and (b) shallow notions of civility: for the record, I value the former infinitely more than the latter. Bill Kristol and John Yoo are both extremely “civil” in the sense that Wittes means this — all while they advocate indecent and repellent ideas. That, by itself, demonstrates the irrelevance of these vapid notions of “civility” to which Wittes and most DC denizens cling as a means of justifying what they’re actually advocating (we may be defending repulsive and destructive ideas — we’re cheering on wars and insisting on legal immunity for torturers — but at least we’re doing it in a soft-spoken manner while sitting in plush think tank conference rooms with name plates and pitchers of water, which entitles us to respect and deference).

Wittes is a foot soldier for the status quo — that’s how he makes a living.

Greenwald 11 — Glenn Greenwald, lawyer and journalist who published reports based on classified documents disclosed by Edward Snowden, Contributor to *Salon* and *The Guardian*, Recipient of the 2014 Pulitzer Prize for Public Service, holds a J.D. from New York University School of Law and a B.A. in Philosophy from George Washington University, 2011 (“Brookings’ ‘centrist’ opposition to the rule of law,” *Salon*, January 14th, Available Online at http://www.salon.com/2011/01/14/lawlessness_4/, Accessed 04-20-2015)

Like many other self-proclaimed “scholars” of the Brookings Institution, Benjamin Wittes never tires of branding himself a “centrist.” But like Brookings itself, this so-called centrism is devoid of any coherent worldview and instead has one overarching purpose: to defend Beltway elite prerogatives and specifically the bipartisan orthodoxies of the National Security State. That’s why Brookings is so lavishly funded and why it exists, and that — in almost every instance — is what D.C. denizens mean when they talk about “centrism”: subservient defenders of the status quo.

Dutifully fulfilling his function, Witten has spent the last several years joining with former Bush OLC lawyer Jack Goldsmith to defend indefinite detention without charges as well as the creation of “national security courts” to allow “preventive detention.” He scorned those who objected to Bush’s illegal, warrantless eavesdropping programs as simplistic, ignorant partisans. When Congress drastically expanded Bush’s eavesdropping powers with the 6-month enactment of the Protect America Act, Witten went to The New Republic to (of course) defend the new powers, prompting Matt Yglesias to say that Witten was merely fulfilling “his appointed role as ‘liberal who agrees with conservatives about all the topics he writes about.’” Witten was recently held up as the face of “American exceptionalism” by international law professor Kevin Jon Heller for explicitly justifying America’s right to impose double standards in light of its objective superiority. Behold Reasonable Sober Serious Centrism!

Witten can’t claim the moral high ground: he’s an apologist for torture.

Kaye 11 — Jeff Kaye, Practicing Psychologist and Clinician at Survivors International—a program of the University of California-San Francisco/San Francisco General Hospital Trauma Recovery Center that provides psychological, social service, and medical services to victims of torture, withdrew his membership in the American Psychological Association because of that organization’s complicity with U.S. torture practices, holds a Ph.D. in Psychology from The Wright Institute and a B.A. in History from the University of California-Berkeley, 2011 (“Benjamin Witten Responds: ‘Happy to be a government proxy’,” *Firedoglake*—a progressive news site, July 24th, Available Online at <http://firedoglake.com/2011/07/24/benjamin-witten-responds-happy-to-be-a-government-proxy/>, Accessed 07-12-2015)

In an arrogant riposte to an earlier posting of mine, Lawfare blogger and member of the Hoover Institute Task Force on National Security and the Law, Benjamin Witten, proclaimed he is “Happy to be a government proxy.”

Witten’s tongue may seem somewhat in cheek, but he really means it. “Government proxy” how? In my earlier article criticizing both Witten and Adweek columnist Alex Koppelman for their poorly resourced and vituperative articles attacking Scott Horton’s investigation of the 2006 deaths of three Guantanamo detainees, published by Harper’s Magazine in January 2010. Department of Defense investigations had labeled all three deaths suicides.

Moreover, when both Koppelman and Witten were cited in a footnote to a Department of Justice brief (PDF) defending numerous government officials against a lawsuit brought by parents of the dead detainees — Koppelman and Witten’s stories were cited as examples of “numerous articles addressing serious flaws with the HARPER’S MAGAZINE story”— I noted that the two authors “wittingly or not” had become “government proxies in the matter of the Guantanamo suicides controversy.”

Witten replied, sarcastically, “Wow, I’m Verklempt.” He continued:

Turns out that DOJ, in a footnote in a brief before the D.C. Circuit, cited this post of mine from some time back – in which I expressed dismay that Scott Horton and Harpers had received a National Magazine award for a feature article devoted to the spurious suggestion that U.S. service personnel had tortured three Guantanamo detainees to death. The passing citation in the brief prompted this howl of rage from a new blogger over at Firedoglake named Jeff Kaye, who had earlier written a defense of the Harpers article....

Happy to be a government proxy on this one. Robert Loeb and Barbara Herwig, who filed the brief, hereby have my blessing to use any Lawfare post their hearts may desire in defending this suit. I'll live with myself quite happily, thank you.

Wittes, who saved his strongest complaint for a typo of his name in the post, repeats the lie that Horton's article claimed the three Guantanamo detainees — Salah Ahmed Al-Salami, Mani Shaman Al-Utaybi, and Yasser Talal Al-Zahrani — were “tortured to death” by “U.S. service personnel.” In fact, Horton never makes any such claim in the article. It is true that the Al-Zahrani’s father is quoted in the article as asserting his son was tortured and killed, but that is very different than Horton coming to such a conclusion. Instead, Horton built a case, based upon contradictions in the government’s investigations, eye-witness testimony, independent autopsy, and revelations concerning a CIA (or JSOC?) black site at Guantanamo, that the deaths were “possible homicides.”

By claiming Horton implicated “service personnel” in torture or possible homicide, Wittes means to tar Horton with irresponsible attacks against rank-and-file U.S. servicemen and women who have sacrificed much to serve their country. If suspicion falls on anyone, it is on interrogators or agents for the CIA or JSOC. Since writing the story, Horton has been calling, as have the parents, for an independent investigation.

Wittes’ portrayal of the DoJ citation of his work is strangely spurious as well. He says that the citation in the brief filed with the D.C. Circuit came from a “post of mine some time back.” In fact, the post was dated May 23, 2011, the same day as Koppelman’s Adweek screed. The brief, signed by government attorneys in DoJ’s Civil Appellate Division, Robert Loeb and Barbara Herwig, as well as by Assistant Attorney General Tony West, was filed on July 13, a mere seven weeks after the Koppelman/Wittes articles. Perhaps we should allow for the subjectivity of time sense and grant Wittes his belief that his article had appeared “some time back” in relation to the government brief. My subjective sense of the affair is that it was quite contemporaneous.

I have very little patience for academic apologists for torture like Wittes. I suppose some, including Wittes himself, might take umbrage at such labels, but an apologist is what he is, no matter how even-handed and reasonable — a man who supposedly takes no extreme positions — he presents himself. Take, for instance, his defense of his friend William Haynes’ approval of torture techniques at Guantanamo. In an article for The New Republic last year, Wittes defended Bush administration attorneys like Haynes, Jack Goldsmith, John Yoo and Jay Bybee, castigating “the vilification of government lawyers involved in the war on terror.”

Admittedly, Wittes said, Haynes was a friend of his “about whom I do not pretend to be neutral.” But rather than forgo comment because of his personal connection (Jack Goldsmith, too, is a personal friend and a professional collaborator, having written articles with Wittes; Goldsmith also is one of two other major contributors, with Wittes, to the blog Lawfare), he defends Haynes’s actions, and apologizes for torture.

Wittes in TNR:

Haynes’s long tenure at the Defense Department was a complicated affair. He made mistakes, mistakes I probably would have made too had I been in his shoes. He also behaved very admirably at important junctures.

The memo for which he has been pilloried is also the reason that the military, unlike the CIA, never waterboarded anybody. [Djamel Ameziane might disagree with that assertion.] Haynes recommended approval of certain modestly coercive techniques—the use of which later spun out of control—but he drew the line at several highly-coercive techniques, waterboarding included. Though they might be legal, he wrote, the military was trained in a tradition of restraint and shouldn't use them. In other words, he behaved exactly the way the Left often criticizes the CIA for not behaving; even in a crisis setting, he refused to let the criminal law define military interrogation policy. Why is that fact not even part of the conversation about him?

And what were the “certain modestly coercive techniques” Haynes approved? In a November 27, 2002 memo from Haynes to then-Secretary of Defense Donald Rumsfeld, Haynes approved all “Category I and II” “counter-resistance techniques” that had been requested by Major General Mike Dunleavy, Commander of Task Force 170, Guantanamo. He also approved one of the “Category III” techniques. But as Wittes notes, he did not approve some others, including a version of waterboarding, and the making of death threats.

The actual techniques, derived from SERE torture training conducted by DoD, were described by Dunleavy’s staff intelligence director, Lieutenant Commander Jerald Phifer, in a memo that accompanied Dunleavy’s request, and which Haynes approved, in large part.

What techniques did Haynes approve? From the Phifer memo, they included all these “Category II” techniques:

- (1) The use of stress positions (like standing), for a maximum of four hours.
- (2) The use of falsified documents or reports
- (3) Use of the isolation facility for up to 30 days. Request must be made to through the OIC [Officer in Charge], Interrogation Section, to the Director, Joint Interrogation Group (JIG). Extensions beyond the initial 30 days must be approved by the Commanding General. For selected detainees, the OIC, Interrogation Section, will approve all contacts with the detainee, to include medical visits of a non-emergent nature.
- (4) Interrogating the detainee in an environment other than the standard interrogation booth.
- (5) Deprivation of light and auditory stimuli
- (6) The detainee may also have a hood placed over his head during transportation and questioning. The hood should not restrict breathing in any way and the detainee should be under direct observation when hooded.
- (7) The use of 20 hour interrogations.
- (8) Removal of all comfort items (including religious items).
- (9) Switching the detainee from hot rations to MREs.
- (10) Removal of clothing.
- (11) Forced grooming (shaving of facial hair, etc...)

(12) Using detainees individual phobias (such as fear of dogs) to induce stress.

According to Benjamin Wittes, these techniques are “modestly coercive.” I wonder if Wittes himself were to be subjected to these, under conditions of indefinite detention, no less, he might not find himself truly “verklempt,” or something far worse.

Famously, Donald Rumsfeld scribbled on the bottom of the Haynes memo, “However I stand for 8-10 hours a day. Why is standing limited to 4 hours?” In Wittes’ world, I suppose Haynes is to be congratulated for holding stress positions to only four hours maximum at a time.

But then, I suppose for the Wittes, the intrepid scholar, this post of mine is just another “howl of rage from a new blogger over at Firedoglake.” Referencing my notice of Wittes’ peculiar sense of time above, I should note I’ve been writing at Firedoglake since April 2009, a year longer than “Lawfare” has been in business.

Wittes is wrong about everything.

Greenwald 7 — Glenn Greenwald, lawyer and journalist who published reports based on classified documents disclosed by Edward Snowden, Contributor to *Salon* and *The Guardian*, Recipient of the 2014 Pulitzer Prize for Public Service, holds a J.D. from New York University School of Law and a B.A. in Philosophy from George Washington University, 2007 (“How the super-smart, insider experts opine,” *Unclaimed Territory*—Glenn Greenwald’s blog, February 5th, Available Online at <http://glenngreenwald.blogspot.com/2007/02/how-super-smart-insider-experts-opine.html>, Accessed 07-12-2015)

The New Republic has published an article by Benjamin Wittes, a "Guest Scholar" at the Brookings Institution, which argues that the issues surrounding the Bush administration's warrantless eavesdropping activities are so complex and sophisticated, and raise such grave matters of national security, that not even the most brilliant and well-informed insider-experts -- such as Wittes -- could possibly form an opinion about whether the Bush administration did anything wrong. Only blind, ignorant partisans would claim that President Bush acted wrongfully or illegally here.

Wittes' article is the perfect textbook illustration of how the above-it-all, very-serious, super-smart, self-anointed pundit-experts churn out empty, cliched decrees -- which, though totally devoid of substance, nonetheless enable the Bush movement's worst excesses. Wittes executes this formula perfectly. First comes the Broder-ish tactic of equating and then dismissing both "extremes" in the debate in order to establish one's nonpartisan, elevated, detached objectivity:

Many liberals are convinced that the program represented a deep affront to the rule of law, though they don't know quite what the program was. Many conservatives are no less certain of the program's absolute necessity. And, though they don't know quite what it was either, they are sure as well that President Bush had the authority to implement it-- whatever federal law on the subject may happen to say.

Right at the start we learn how very clever and objective Wittes is: both "liberals" and "conservatives" have formed strong opinions about the NSA scandal despite knowing nothing. Thus, those who object to the President's law-breaking are exactly the same as those who defend it: merely loud-mouth partisan extremists -- opposite sides of the same shrill, lowly coin -- who

can be scornfully dismissed away as know-nothing hysterics. Such blind ignorance, of course, stands in stark contrast to the very high-minded and insider expertise of Wittes:

Unlike many of these oh-so-confident commentators, I actually know something about the Foreign Intelligence Surveillance Act. I am one of the very few journalists--to my knowledge, in fact, the only one--who ever physically set foot inside the super-secret Foreign Intelligence Surveillance Act (FISA) Court. FISA has been a particular interest of mine since the mid-'90s, when I was a young reporter at a legal trade paper and the court it created was the most obscure corner of the federal judiciary. Precisely because nobody knew anything about it, I studied it obsessively. I talked to the judges who heard the government's surveillance requests and to the Justice Department lawyers who advanced these applications. I learned, in some detail, the contours, value, and the limitations of FISA at a time when very few people cared about it.

So what is my assessment of the Terrorist Surveillance Program, informed by my decade of watching the court and the law that underlies it?

I don't know.

Just preliminarily, do The New Republic editors really not realize how adolescent this all sounds? "I actually know something about the Foreign Intelligence Surveillance Act." "I am one of the very few journalists--to my knowledge, in fact, the only one--who ever physically set foot inside the super-secret Foreign Intelligence Surveillance Act (FISA) Court." "I studied it obsessively." "I learned, in some detail, the contours, value, and the limitations of FISA at a time when very few people cared about it." To The New Republic, this sounds impressive, because they think it constitutes a persuasive (even necessary) foundation for someone to begin an argument by insisting, based on nothing, how much more knowledgeable they are than everyone else.

In fact, Wittes' insider credentials are so impressive that he can simply decree the truth about issues without even bothering to offer any rationale or facts at all. His entire article is devoid of any facts or arguments. He simply assures us that he knows so much more about FISA than you do, and because of how much he knows, he realizes that these matters are way too complicated even for him -- let alone for you -- to form an opinion about whether the President did anything wrong here. This is his whole "argument":

I don't know what the program is. I don't know whether it was lawful before the recent change. Truth be told, I don't even understand what the change announced in Gonzales's letter really means. I can arrange the facts in the public record so as to describe a program that would, in my view, offend the Constitution. And I can arrange the facts in the public record so as to describe a program that would not, in my view, offend the Constitution. I can imagine a program outside of FISA that the law should be amended to accommodate. And I can imagine a program that violates the FISA precisely because it involves the kind of warrantless surveillance the law was passed to prevent. What's more, the more I learn about this program, the less I understand it.

For the eager-to-please, self-styled Beltway insider-experts, a failure to form a clear political opinion is the mark of both intellectual and moral superiority, of emotional maturity, and is the hallmark of that most coveted Washington virtue -- seriousness. Unlike you, who has formed one of those dirty opinions that the President has no right to break the law, Wittes understand that these matters are much, much more complex and sophisticated than that -- after all, this involves

computers and national security threats and data and things you cannot possibly begin to understand -- and it is only your ignorance, your extremely unserious partisanship, that has enabled you to think that you are in a position to oppose or condemn what George Bush has done here (TNR's Jason Zengerle long ago pronounced that "some of the outrage [over the NSA scandal] is in fact outrageous").

Like most of these pundits, Beltway journalists, and think-tank "fellows," Wittes wants the President's lawbreaking to implicate all sorts of murky and complex matters because, that way, the expertise which Wittes thinks he has would be needed. It would mean that only Wittes, but not you, is qualified to form judgments and that your obligation would be to listen to him and rely on what he says, rather than form your own views. So he asserts that there are all kinds of complicated issues (never identified) which only insiders can understand and which prevent any meaningful opinions to be formed by non-insiders (i.e., the masses).

As is so often true with articles like this one in The New Republic, and similar venues, Wittes' eager attempt to show how much more than everyone else he knows ends up revealing the precise opposite -- a profound ignorance regarding the issues about which he is purporting to enlighten us all. The FISA law, as intended, is one of the clearest laws in the U.S. Code, and the issues raised by the NSA scandal are everything but complicated or murky.

I think everyone other than Wittes and a handful of still-confused Bush followers understands now that the U.S. Code provides that "the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . may be conducted", and FISA itself provides that "A person is guilty of an offense if he intentionally (1) engages in electronic surveillance under color of law except as authorized by statute."

The administration admits that the eavesdropping it has been conducting outside of the FISA court -- whatever that might entail -- is precisely the type of eavesdropping for which the FISA law requires a court order. And the fact that the administration has now agreed to conduct this same eavesdropping under the purview of the FISA court by itself proves that this eavesdropping is the type covered by FISA (otherwise, the FISA judges would have no jurisdiction to supervise it). For that reason, Wittes' grand conclusion is completely bereft of logic and just factually wrong on every level:

For whatever it's worth, here's my best guess--and, I stress, it's only a guess--about what this NSA program was all about: I suspect it was an earnest attempt to address problems that the drafters of the FISA would have been mortified to learn they had created for the intelligence community. . . .

This hypothesis could be totally wrong. The point is that, without knowing the precise contours of the program, it is simply impossible to evaluate it against a complicated and subtle law written at a time when the computer age was still in its infancy. Some day, we will finally learn what the program really was and why it couldn't, and then could, be approved through the FISA Court. Details will leak, or the technology will become too obsolete to warrant continued protection. When that day comes, those who insist that no possible combination of technology, law, and national emergency could excuse bypassing the court may find themselves embarrassed. . . .

What facts could possibly emerge that make us all realize how Good and Right the President was to break the law, or for us to conclude that he didn't? Wittes doesn't bother to identify such possible facts, because none exist. By definition, none can exist.

FISA -- at least the parts relevant to the administration's lawbreaking -- is not a "complicated and subtle law" except to people who do not understand it or who want purposely to obscure it. And one does not need to know "precise contours of the program" in order to know that the President broke the law. That he engaged in the precise eavesdropping without warrants for which FISA requires warrants renders all of Wittes' very, very complicated and angst-ridden speculation completely irrelevant.

But this is how this sort of pompous, self-styled partisan-transcendence almost always operates. They think that things like emphatic beliefs and principles -- and especially stern criticism of our Serious National Security Leaders -- are for the lowly, anti-intellectual masses. The true guardians of wisdom and serious political thought in our society struggle endlessly with complex intellectual dilemmas and never reach any definitive conclusions because they are too smart and too serious for things like convictions or beliefs or things as shrill and irresponsible as accusations of wrongdoing against a sitting wartime President (the classic case illustrating this mindset was when The New Republic's Jonathan Chait chided those whom he revealingly labelled as "partisan hysterics" -- meaning those who objected to his magazine's defense of Ann Coulter and thus, unlike the complex and thoughtful Chait, failed to appreciate what a "clever, interesting, very well-executed" intellectual achievement it was).

The impact of this petty, self-regarding mentality is hard to overstate. In the run-up to the invasion of Iraq, it manifested as endless condemnation against war opponents on the ground that war opponents were simply too shrill and emphatic and failed to grapple with all of the fascinating, multi-layered, theoretical challenges which any serious, complex political thinker had to confront when pondering Iraq.

And the same thing is occurring now with Iran. Only "partisan hysterics" would take the position that a military attack on Iran is unwarranted, unnecessary, and insane. More sophisticated, trans-partisan, serious thinkers understand that the issue is far more complex than that and cannot be reduced to such crass partisan certainties.

This really illustrates the core of why our pundit class and Beltway opinion-making mechanisms are so corrupt and worthless, but also so destructive. The whole point -- the only objective -- of Wittes' article, and of columns and articles from most of our establishment pundits, is to establish their own special place of wisdom and insight. To achieve that, they reduce all political matters to nothing more than grand intellectual puzzles, and equate any real beliefs with primitive ignorance. That is what they mean by heinous, lowly "partisanship" -- genuine political convictions.

There is no place for hard-core beliefs or passion and especially not for anger. Such emotions are just the misguided stirrings of the masses. And thus, a President and his political movement start disastrous wars, are provoking still new ones, systematically and deliberately break the law, destroy U.S. credibility, and introduce a whole array of radical and destructive measures. But those are all just fascinating intellectual matters which we should ponder with delicacy and civility and mild, restrained discourse. None of them warrants any strong reactions or condemnations.

And so the super-smart, insider pundit class merrily buzzes along, never forming a definitive thought or opinion about anything other than to haughtily condemn those who object to what the President and his political movement have done and plan to do. Regarding the destruction which this President is wreaking on the country, Wittes summarizes how the truly smart, sober, non-partisan experts (as opposed to the partisan hysterics) should react: "I don't know' seems like a good place to me."

IT Benjamin Wittes — “Nothing To Hide”

Wittes is wrong about “nothing to hide” — there is a substantial chilling effect.

Masnich 14 — Mike Masnick, Founder and Chief Executive Officer of Floor64—a software company, Founder and Editor of *Techdirt*, 2014 (“Saying That You’re Not Concerned Because The NSA Isn’t Interested In You Is Obnoxious And Dangerous,” *Techdirt*, July 16th, Available Online at <https://www.techdirt.com/articles/20140703/18113427778/saying-that-youre-not-concerned-because-nsa-isnt-interested-you-is-obnoxious-dangerous.shtml>, Accessed 07-05-2015)

One of the more common responses we’ve seen to all of the revelations about all of that NSA surveillance, is the response that “Well, I don’t think the NSA really cares about what I’m doing.” A perfect example of that is long-time NSA defender Ben Wittes, who recently wrote about why he’s not too worried that the NSA is spying on him at all, basically comparing it to the fact that he’s confident that law enforcement isn’t spying on him either:

As I type these words, I have to take on faith that the Washington D.C. police, the FBI, the DEA, and the Secret Service are not raiding my house. I also have to take on faith that federal and state law enforcement authorities are not tapping my various phones. I have no way of knowing they are not doing these things. They certainly have the technical capability to do them. And there’s historical reason to be concerned. Indeed, there is enough history of government abuse in the search and seizure realm that the Founders specifically regulated the area in the Bill of Rights. Yet I sit here remarkably confident that these things are not happening while my back is turned—and so do an enormous number of other Americans.

The reason is that the technical capability for a surveillance event to take place does not alone amount to the reality—or likelihood—of that event’s taking place....

For much the same reason as I am not rushing home to guard my house, I have a great deal of confidence that the National Security Agency is not spying on me. No doubt it has any number of capabilities to do so. No doubt those capabilities are awesome—in the wrong hands the tools of a police state. But there are laws and rules that protect me, and there are compliance mechanisms that ensure that the NSA follows those laws and rules. These systems are, to be sure, different from those that restrain the D.C. cops, but they are robust enough to reassure me.

Julian Sanchez has a blistering response to that, appropriately entitled Check Your Privilege, which highlights that while Wittes, a well-paid, white, DC-based policy think tank worker, may be confident of those things, plenty of other folks are not nearly so confident, and that the NSA has made it pretty clear that they shouldn’t be so confident.

In a democracy, of course, the effects of surveillance are not restricted to its direct targets. Spying, like censorship, affects all of us to the extent it shapes who holds power and what ideas hold sway. Had the FBI succeeded in “neutralizing” Martin Luther King Jr. earlier in his career, it would hardly have been a matter of concern solely for King and his family—that was, after all, the whole point.

Instead of a couple wonks comfortably ensconced in D.C. institutions, let’s instead ask a peaceful Pakistani-American who protests our policy of targeted killings, perhaps in

collaboration with activists abroad; we might encounter far less remarkable confidence. Or, if that seems like too much effort, we can just look to the survey of writers conducted by the PEN American Center, finding significant percentages of respondents self-censoring or altering their use of the Internet and social media in the wake of revelations about the scope of government surveillance. Or to the sworn declarations of 22 civil society groups in a lawsuit challenging bulk phone records collection, attesting to a conspicuous decline in telephonic contacts and members expressing increased anxiety about their association with controversial or unpopular organizations.

As Sanchez notes, it's not just whether or not any of us are direct targets, but the overall chilling effects of how the system is used. And, I should note, that while Wlettes is confident that he's safe -- there are a growing number of folks who have good reason to believe that they are not immune from such surveillance. The recent revelation that Tor users are labeled as extremists who get extra-special scrutiny seems like a major concern. Similarly, the story from earlier this year that the NSA targeted the Pirate Bay and WikiLeaks as part of some of its surveillance efforts is a major concern. In the process of doing journalism, I've communicated with folks associated with some of those and other similar organizations. In the past, I probably would have similarly noted that I doubted the NSA cared at all about what I was doing, but as each of these stories comes out, I am increasingly less sure. And, more importantly, even if the NSA is not at all concerned with what I happen to be doing, just the fact that I now have to think about what it means if they might be certainly creates a chilling effect, and makes me think twice over certain people I contact, and what I say to them.

It's easy to claim that you're not worried when you're the one out there supporting those in power. It becomes a lot trickier when you're either criticizing those in power, or communicating with those who challenge the power structure. Suddenly, it's not so easy to sit on the sidelines and say "Meh, no one's going to care about me..." And that should be a major concern. The way we keep a strong democracy is by having people who are able and willing to challenge the status quo and those in power. And yes, the US is much more forgiving than many, many other countries to such people, but there are clear biases and clear cases where they are not at all accepting of such things. And the more of a chilling effect the government creates around those things, the more dangerous it becomes to stand up for what you believe in.

Wlettes is wrong about “nothing to hide” — he’s super privileged.

Sanchez 14 — Julian Sanchez, Senior Fellow specializing in technology, privacy, and civil liberties at the Cato Institute, former Washington Editor for *Ars Technica*, holds a B.A. in Philosophy and Political Science from New York University, 2014 (“Check Your Privilege,” *Cato at Liberty*—a Cato Institute blog, July 3rd, Available Online at <http://www.cato-unbound.org/2014/07/03/julian-sanchez/check-privilege>, Accessed 06-29-2015)

Ben Wlettes begins his essay by observing that, just as he takes on faith that government agencies are not currently raiding his house, he is “remarkably confident” that the NSA is not illicitly wiretapping him. As someone who occasionally corresponds with Guardian editors and human rights activists outside the United States, I am frankly not nearly so confident that none of my communications have been “incidentally” collected, but how either of us is personally affected is rather beside the point. I’m also, after all, confident that, as a person of pallor, I could have

strolled through Brooklyn at any time over the past few years without being subject to a humiliating “stop and frisk.” That is, in a sense, the problem.

I dwell on what Ben no doubt intended mostly as a rhetorical flourish because concerns about surveillance so frequently evoke blasé responses to the effect of: “Well, I’m sure they’re not interested in me, so I don’t really care; I have nothing to hide.” Privileged folks like Ben and I may well be right to think the laws, rules, and institutional priorities governing the intelligence community will protect us—a fortiori if we happen to be vocal advocates of that community—but the test of a just system is not how it treats the privileged. That doesn’t mean a privileged perspective is necessarily wrong, but it does mean we ought to be cautious about any inference from “this is not a problem I worry about” to “this is not a problem.”

In a democracy, of course, the effects of surveillance are not restricted to its direct targets. Spying, like censorship, affects all of us to the extent it shapes who holds power and what ideas hold sway. Had the FBI succeeded in “neutralizing” Martin Luther King Jr. earlier in his career, it would hardly have been a matter of concern solely for King and his family—that was, after all, the whole point.

Instead of a couple wonks comfortably ensconced in D.C. institutions, let’s instead ask a peaceful Pakistani-American who protests our policy of targeted killings, perhaps in collaboration with activists abroad; we might encounter far less remarkable confidence. Or, if that seems like too much effort, we can just look to the survey of writers conducted by the PEN American Center, finding significant percentages of respondents self-censoring or altering their use of the Internet and social media in the wake of revelations about the scope of government surveillance. Or to the sworn declarations of 22 civil society groups in a lawsuit challenging bulk phone records collection, attesting to a conspicuous decline in telephonic contacts and members expressing increased anxiety about their association with controversial or unpopular organizations.

What’s important to keep in mind here is that even if Ben were well justified in his belief that government is unlikely to ever again misuse its powers against any peaceful citizens, the panoptic chilling effect these systems exert on many who lack his (let us suppose) superior understanding would still inflict a real cost in the currency of democratic engagement. Some people, no doubt, will be unreasonably paranoid regardless of the facts about the government’s powers and capabilities, while others now anxious may be reassured once articulate folks like Ben and Carrie explain the rules already in place. At least some, however, may be reassured only if the law is tightened in appropriately reassuring ways. If so, and if members of marginalized groups have sound historical reason to fear mistreatment by government, then folks like Ben and I should be cautious of generalizing too quickly from the fact that we don’t personally share those fears.

I2 Benjamin Wittes — “Surveillance Debates Bad”

Wittes is an apologist for the government and an enemy of democracy.

Friedersdorf 14 — Conor Friedersdorf, Staff Writer for *The Atlantic*, 2014 (“Exposing the NSA: A Public Service Worthy of a Pulitzer Prize,” *The Atlantic*, April 16th, Available Online at <http://www.theatlantic.com/politics/archive/2014/04/exposing-the-nsa-a-public-service-worthy-of-a-pulitzer-prize/360723/>, Accessed 07-12-2015)

NSA apologists spoke out too. Max Boot of Commentary absurdly compares the Pulitzer board's praise for reporting on the NSA to giving an award to articles "whitewashing the evils of Stalinist Russia." At Lawfare, Benjamin Wittes objects to the characterization of the Washington Post's reporting as authoritative. And while he acknowledges that The Guardian sparked debate, he isn't much impressed by that achievement.

Let's focus there.

"If sparking a debate is enough to earn the Pulitzer's coveted public service medal, then sure. Congrats," Wittes writes. "I would note, however, that merely sparking a debate is an exceedingly low standard." He proceeds to recall past award-winners in the Pulitzer's public-service category, winners that he much preferred:

They passed a test much higher than the “sparked a debate” test, a test that the Westboro Baptist Church and the Church of Scientology, I might add, pass with some regularity, and they were not merely transit stops for leaks from others.

The Westboro Baptist Church is an anti-gay congregation that protests at military funerals to attract media attention. If it did not exist, Americans would be no less aware of the ongoing, transparent debate about public policy affecting gays. Wittes reveals a blind spot when he conflates the value of the debate Westboro sparks with the value of the debate sparked by Snowden and various reporters. The latter is a tremendous public service: When public policy is shrouded in secrecy, sparking debate is synonymous with enabling the practice of democracy. Without debate, representative government as we know it is extinguished.

Snowden and the Pulitzer Prize committee understand this. Unlike Wittes, they appreciate that informing citizens about public policy has inherent value and is a prerequisite for meaningful civic participation. That's especially true when what's being hidden includes repeated violations of the Constitution, national-security figures lying to Congress, woefully underinformed legislators, and mass surveillance.

The benefits of reporting on the NSA aren't just theoretical.

As a direct result of articles written by Glenn Greenwald, Laura Poitras, Barton Gellman, and others, President Obama and multiple members of Congress have changed their positions on surveillance policy. Expert executive-branch panels have criticized the status quo. The White House and legislators have suggested multiple reforms. Article III judges have concluded the NSA's behavior is needless and illegal. That these significant actions occurred only after the Snowden leaks is evidence that prior secrecy retarded the whole civic process.

Back then, public policy lacked democratic legitimacy. Recent reform efforts are due to the fact that, when Americans learned about the status quo, they wouldn't tolerate it.

Treating the spark for a debate that informs policy as no more a public service than anti-gay protests at military funerals isn't just myopic. It's consistent with the anti-democratic, anti-transparency ideology that prevails at Lawfare. Wittes and others believe that the public has no proper role in judging the propriety of most NSA actions, because the information needed to render judgments is properly classified. And they're not troubled by the ways in which the NSA and the FISA court have twisted the law so that it hardly resembles what Congress passed.

If they had their way, we'd all be more ignorant.

Their preferences are antithetical to the role the press is supposed to play in America. When the Founders ratified the First Amendment, journalism like the stories sourced to Edward Snowden is exactly the sort of thing that they were hoping to protect: articles that give the public the truth about their government, truth that governing elites would be tempted to suppress if they were allowed to do it. Put another way, the Framers expected there to be an adversarial relationship between the government and the press. And Wittes is on the other side. No wonder he doesn't like the work journalism organizations select for awards. As long as he allies himself with people who think that they're justified in suppressing basics like what the law is, he'll hold valuable journalism in contempt.

NSA surveillance does not prevent terrorism — NAF study.

Bergen et al. 14 — Peter Bergen, Director of the National Security Program at the New America Foundation, Professor of Practice at the School of Politics and Global Studies and Co-Director of the Center on the Future of War at Arizona State University, Research Fellow at the Center on National Security at Fordham University, National Security Analyst for CNN, has taught at the John F. Kennedy School of Government at Harvard University and the School of Advanced International Studies at Johns Hopkins University, holds an M.A. in Modern History from New College (Oxford), et al., with David Sterman, Research Assistant at the New America Foundation, holds an M.A. in Security Studies from Georgetown University and a B.A. in Political Science and Government from Dartmouth College, Emily Schneider, Research Assistant at the New America Foundation, holds a J.D. in National Security and Counterterrorism Law from Syracuse University College of Law, an M.A. in English from the University of Rochester, and a B.A. in English from Penn State University, and Bailey Cahall, Research Associate at the New America Foundation, holds an M.A. in Global Security and Foreign Policy from the Maxwell School of Citizenship and Public Affairs at Syracuse University and a B.A. in History from West Virginia University, 2014 (“Do NSA's Bulk Surveillance Programs Stop Terrorists?,” New America Foundation, January 13th, Available Online at http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists, Accessed 04-20-2015)

On June 5, 2013, the Guardian broke the first story in what would become a flood of revelations regarding the extent and nature of the NSA's surveillance programs. Facing an uproar over the threat such programs posed to privacy, the Obama administration scrambled to defend them as legal and essential to U.S. national security and counterterrorism. Two weeks after the first leaks by former NSA contractor Edward Snowden were published, President Obama defended the NSA surveillance programs during a visit to Berlin, saying: “We know of at least 50 threats that have

been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved.” Gen. Keith Alexander, the director of the NSA, testified before Congress that: “the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world.” Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that “54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives.”

However, our review of the government’s claims about the role that NSA “bulk” surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda’s ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA’s bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.

Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it’s unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government’s investigations of these cases: <http://natsec.newamerica.net/nsa/analysis>).

Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens’ telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided \$8,500 to al-Shabaab, al-Qaeda’s affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to “connect the dots” faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA’s phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it’s unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin’s calls, despite official statements that the bureau had Moalin’s phone number and had identified him. This undercuts the government’s theory that the database of Americans’ telephone metadata is necessary to expedite the investigative process, since it clearly didn’t expedite the process in the single case the government uses to extol its virtues.

Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange.

NSA surveillance hasn't stopped any terror attacks — White House Panel.

Wright 13 — Dan Wright, News Desk Reporter at *Firedoglake*—a progressive news site, citing Geoffrey Stone, Professor of Law at the University of Chicago and Member of the White House Panel investigating NSA bulk surveillance, 2013 (“NSA Program Stopped No Terrorist Attacks,” *Firedoglake*—a progressive news site, December 20th, Available Online at <http://news.firedoglake.com/2013/12/20/nsa-program-stopped-no-terrorist-attacks/>, Accessed 07-12-2015)

Remember when those NSA officials and President Obama claimed they needed to spy on Americans because it would prevent terrorist attacks? Even saying it already had prevented attacks and “saved lives”? Yeah, about that, actually not true. Obama, NSA, and friends were lying.

According to NBC News one of the White House Panel members on the committee to reform the NSA has disclosed that not one-single-solitary-attack was stopped from the NSA surveillance program.

A member of the White House review panel on NSA surveillance said he was “absolutely” surprised when he discovered the agency’s lack of evidence that the bulk collection of telephone call records had thwarted any terrorist attacks.

“It was, ‘Huh, hello? What are we doing here?’” said Geoffrey Stone, a University of Chicago law professor, in an interview with NBC News. “The results were very thin.”

So the NSA has been caught in yet another lie. Will we ever believe them again? Should we?

But it is hard to believe – given we live in such a dangerous world – that there is not at least some evidence the program may have helped protect the country. That by vacuuming up all that data at least something came out of it to help protect the country from terrorist attacks.

While Stone said the mass collection of telephone call records was a “logical program” from the NSA’s perspective, one question the White House panel was seeking to answer was whether it had actually stopped “any [terror attacks] that might have been really big.”

“We found none,” said Stone.

So when Obama said “lives have been saved” he was not only wrong, but he knew he was wrong. And when the NSA claimed 13 attacks had been thwarted they knew that wasn’t true.

AT Section 215 Specific -- Frontline

No Link -- Metadata collection hasn't stopped a single attack

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 9-1-14

The threat of terrorism faced today by the United States is real. The Section 215 telephone records program was intended as one tool to combat this threat — a tool that would help investigators piece together the networks of terrorist groups and the patterns of their communications with a speed and comprehensiveness not otherwise available. However, we conclude that the Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.

The Board's review suggests that where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways: by offering additional leads regarding the contacts of terrorism suspects already known to investigators, and by demonstrating that foreign terrorist plots do not have a U.S. nexus. The former can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. The latter can help the intelligence community focus its limited investigatory resources by avoiding false leads and channeling efforts where they are needed most. But with respect to the former, our review suggests that the Section 215 program offers little unique value but largely duplicates the FBI's own information gathering efforts. And with respect to the latter, while the value of proper resource allocation in time-sensitive situations is not to be discounted, we question whether the American public should accept the government's routine collection of all of its telephone records because it helps in cases where there is no threat to the United States.

Link turn – Section 215 slows investigators down by eating up resources and generating useless leads

Matthias Schwartz, January 23, 2015, The New Yorker, "Who Can Control NSA Surveillance?" The New Yorker, DOA: 1-23-15, <http://www.newyorker.com/news/news-desk/can-control-n-s-surveillance> DOA: 1-26-14

There isn't much evidence to suggest that Section 215 helps catch the most dangerous terrorists, like those who committed the attacks in Paris two weeks ago. It may even slow investigators

down, by eating up resources and generating extraneous leads. (I wrote about Section 215's track record in this week's magazine.)

Turn – Widespread business records surveillance undermines cooperation with industry that is needed to prevent terrorism

Washington Post, 10-10, 13, http://www.washingtonpost.com/world/national-security/nsa-tries-to-regain-industrys-trust-to-work-cooperatively-against-cyber-threats/2013/10/09/93015af0-2561-11e3-b3e9-d97fb087acd6_story.html

A drop in Americans' trust in the government is making the difficult task of public-private cooperation against cyber-threats even more difficult. And that has officials such as Gen. Keith B. Alexander, director of the National Security Agency, scrambling to shore up confidence in his agency, whose image has taken a beating in the wake of leaks about its surveillance programs by former NSA contractor Edward Snowden. At public hearings and in speeches, Alexander, who also heads the U.S. Cyber Command, is warning that cyberattacks on such critical and technology-dependent industries as energy, finance and transportation can be prevented only if those industries work with the government. **But companies are wary of partnering with an agency that has been revealed to be conducting far-reaching domestic data collection in the name of thwarting terrorism.** “**Industry is critical to resolving our problems**” in cybersecurity, Alexander said at the Billington Cybersecurity Summit last month at the National Press Club. Toward that end, he said, Congress needs to pass “cyber-legislation” to encourage private companies to share data on cyber-threats. A bipartisan bill the House passed in April would provide immunity from civil lawsuits or criminal prosecution to companies that give the Department of Homeland Security network data that might contain evidence of such threats. DHS would pass the data on to relevant agencies, such as the NSA. Alexander said the protected data would be limited to technical material indicating vulnerabilities in systems and hackers’ tracks. “We’re not talking about sharing our private information,” he assured the summit audience. **But there is wide recognition within and outside the government that the Snowden leaks**, which began in June, **have created a deficit of trust. “It was tough enough to [pass the bill] when the waters were calm,**” Michael V. Hayden, Alexander’s predecessor as NSA director, said last week at The Washington Post’s Cyber Summit. **“Now [proponents are] trying to do it in whitewater rapids, and it’s not going to happen.”** Even before the Snowden revelations, the White House threatened to veto the bill on grounds it lacked adequate safeguards for Americans’ privacy, among other things. Now, experts say, it is increasingly unlikely that the House version will emerge from the Senate. “I don’t think anybody thinks it’s realistic to put the NSA in the middle of domestic cybersecurity at this point,” said Michelle Richardson, legislative counsel at the American Civil Liberties Union. **One of the most consequential Snowden leaks was a classified court order whose publication forced the government to acknowledge that the NSA had obtained secret court permission in 2006 to gather the phone records of virtually all Americans — billions of calls — to search for clues to terrorist plots.** Another leak detailed how nine Internet companies — including Yahoo, Google and Microsoft — cooperated, under court order, with the NSA to collect e-mails and other digital data from lawful foreign targets.

Section 215 hasn't stopped any terror attacks

Dustin Volz, January 21, 2015, National Journal, "Snowden: France's 'Intrusive' Surveillance Failed to Stop Paris Attacks," <http://www.nationaljournal.com/tech/snowden-france-s-intrusive-surveillance-laws-failed-to-stop-paris-attacks-20150121> DOA: 1-25-15

"When you look at the United States, the Patriot Act, the mass surveillance that's been debated and criticized since 2013, the White House did two independent investigations into its effectiveness and found that despite monitoring the phone calls for everyone in the United States every time they pick up the phone, it hadn't stopped a single attack," Snowden said in his NOS interview. "We see the same thing in London. It didn't stop the attacks in Spain. It didn't stop the attacks in Boston," he continued. "The problem with mass surveillance is that you're burying people under too much data." Snowden has repeatedly referenced the 2013 Boston Marathon bombing to suggest mass surveillance may in fact undermine the mission of intelligence agencies. Dzhokar and Tamerlan Tsarnaev were pointed out by Russian intelligence to U.S. officials before the bombings in 2013, which killed three and left hundreds more wounded.

AT 44 Examples of Section 215's Effectiveness

Only one weak instance of Section 215 effectiveness – one person (Moalin) was caught funneling \$8500 to a terrorist group

Matthias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Section 215 is just one of many legal authorities that govern U.S. spy programs. These authorities are jumbled together in a way that makes it difficult to separate their individual efficacy. Early in the metadata debate, the fifty-four cases were sometimes attributed to Section 215, and sometimes to other sections of other laws. At a Senate Judiciary Committee hearing in October, 2013, Senator Patrick Leahy, of Vermont, called the fifty-four-plots statistic "plainly wrong . . . these weren't all plots, and they weren't all thwarted." He cited a statement by Alexander's deputy that "there's only really one example of a case where, but for the use of Section 215 bulk phone-records collection, terrorist activity was stopped." "He's right," Alexander said. The case was that of Basaaly Moalin, a Somali-born U.S. citizen living in San Diego. In July, 2013, Sean Joyce, the F.B.I.'s deputy director at the time, said in Senate-committee testimony that Moalin's phone number had been in contact with an "Al Qaeda East Africa member" in Somalia. The N.S.A., Joyce said, was able to make this connection and notify the F.B.I. thanks to Section 215. That February, Moalin was found guilty of sending eighty-five hundred dollars to the Shabaab, an extremist Somali militia with ties to Al Qaeda. "Moalin and three other individuals have been convicted," Joyce continued. "I go back to what we need to remember, what happened in 9/11." At the same hearing, Senator Dianne Feinstein, of California, talked about "how little information we had" before 9/11. "I support this program," she said, referring to Section 215. "They will come after us, and I think we need to prevent an attack wherever we can. In the thirteen years that have passed since 9/11, the N.S.A. has used Section 215 of the Patriot Act to take in records from hundreds of billions of domestic phone calls. Congress was explicit about why it passed the Patriot Act—despite concerns about potential effects on civil liberties, it believed that the law was necessary to prevent another attack on the scale of 9/11. The government has not shown any instance besides Moalin's in which the law's metadata provision has directly led to a conviction in a terrorism case. Is it worth it?

Information provided by section 215 in these cases was available elsewhere and it's not even clear it played an important role in the Somali case.

Julian Sanchez, January 16, 2015, Just Security, "Decrypting John Boehner on the Capitol Hill Bomber" <http://thehill.com/policy/defense/229990-gop-headed-for-battle-over-the-patriot-act>
DOA: 1-20-15

If, as I suspect, Boehner's claim ultimately collapses under scrutiny, it would fit a pattern we've observed time and again with respect to controversial intelligence programs, and the §215 program in particular: Dramatic claims are made to the effect that warrantless wiretapping or

fusion centers have proven essential tools in the war on terror, saving lives and foiling terror plots—only to be debunked, sometimes years later, and typically with far less fanfare. When the NSA's bulk collection of telephony metadata was first disclosed by *The Guardian*, intelligence officials and their nominal overseers in Congress were quick to respond with evidence of the program's utility: Along with collection under §702 of the FISA Amendments Act, Americans were told that the telephony program had helped to thwart “dozens” of terror plots. Some members of Congress, fortunately, were not so credulous, and eventually forced officials to concede that, in fact, while the telephony database had been queried in about a dozen of those cases, in only one—involving monetary contributions to the Somalian group Al Shabaab—had it even arguably provided essential evidence. A thorough report by the Privacy and Civil Liberties Board subsequently examined the program's supposed success stories, and confirmed that in every other case, telephone numbers “tipped” to the FBI from the NSA database merely duplicated information the Bureau had already obtained using ordinary targeted authorities. Even in the case of the Al Shabaab donor, PCLOB concluded that there was “no indication that speed or Section 215’s five-year depth of records were important to the discovery.”

Obama commission couldn't identify a single case where it stopped a terror attack

David Sanger, The New York Times, June 30, 2014

Sky Isn't Falling After Scandal, N.S.A. Chief Says, p. 1

Admiral Rogers has taken command of the agency just as its power to collect and retain "telephone metadata" -- the records of numbers dialed and the duration of calls -- is being stripped from the agency. Mr. Obama defended the program last summer, after the initial round of revelations. But he had a change of heart, fueled by his commission's conclusion that it could not find a case in which the program had definitively halted a potential terrorist attack.

Their examples are flawed -- NSA surveillance programs fail to disrupt terrorism

Bergen, et al, September 2013, Jihadist Terrorism: A Threat Assessment,
http://bipartisanpolicy.org/sites/default/files/Jihadist%20Terrorism-A%20Threat%20Assesment_0.pdf

Peter Bergen is the author of four books about al-Qaeda, three of which were *New York Times* best sellers. The books have been translated into 20 languages. He is the director of the National Security Program at the New America Foundation in Washington, D.C.; a fellow at Fordham University's Center on National Security; and CNN's national security analyst. He has held teaching positions at the Kennedy School of Government at Harvard University and at the School of Advanced International Studies at Johns Hopkins University.¶ Bruce Hoffman is a professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where he is also the director of both the Center for Security Studies and the Security Studies Program. He previously held the corporate chair in counterterrorism and counterinsurgency at the RAND Corporation and was the scholar-in-residence for counterterrorism at the CIA between 2004 and 2006.¶ Michael Hurley is the president of Team 3i LLC, an international strategy company, and advises the Bipartisan Policy Center's Homeland Security Project. He led the 9/11 Commission's counterterrorism policy investigation, as well as CIA personnel in Afghanistan immediately after the 9/11 attacks. He retired from the CIA following a 25-year career and has served as director on the National Security Council staff.¶ Erroll Southers is the associate director of research transition at the Department of Homeland Security's National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California, where he is an adjunct professor in the Sol Price School of Public Policy. He is a former FBI special agent and was President Barack Obama's nominee for the Transportation Security Administration, as well as Governor Arnold Schwarzenegger's deputy director for the California Office of Homeland Security

and the chief of homeland security and intelligence for the LAX Police Department. He is the author of *Homegrown Violent Extremism*.)

Earlier this year, it was revealed that the National Security Agency (NSA) has been collecting phone-records metadata from Americans for many years and that it had secured^[1] the right to access overseas Internet traffic and content from every U.S. Internet service.³¹⁷ This sparked a debate between those who saw an overly expansive government fishing expedition that infringed Americans' privacy and those who pointed out that the NSA programs were carefully managed to protect the rights of American citizens. Beyond the privacy issues that the NSA programs raise: How successful have these programs been in interrupting terrorist plots? So far the evidence on the public record suggests that the programs have been of far less utility than recent U.S. government claims about their ability to disrupt terrorist plots.[¶] Sometime in late 2007, Basaaly Saeed Moalin, a cabdriver living in San Diego, began a series of phone conversations with Aden Hashi Ayrow, one of the leaders of al-Shabaab. He had no idea the NSA was listening in. In one of those 3 phone calls, Ayrow urged Moalin to send money to al-Shabaab, telling him that he urgently needed several thousand dollars. At one point, Ayrow told Moalin that it was "time to finance the jihad" and at another: "You are running late with the stuff. Send some and something will happen." Over several months in 2008, Moalin transferred thousands of dollars to al-Shabaab. He even told Ayrow that he^[1] could use his house in Mogadishu, and "after you bury your stuff deep in the ground, you would, then, plant the trees on top."³²⁰ U.S. prosecutors later asserted that Moalin was offering his house to al-Shabaab as a place to hide weapons, and earlier this year, he was convicted of conspiracy to provide material support to al-Shabaab and of money laundering for the terrorist organization.³²¹ However, there is nothing on the public record to suggest he was planning an attack in the United States. Another terrorist financier detected by NSA surveillance^[1] was Khalid Ouazzani, a Moroccan native and naturalized American living in Kansas City, Missouri. Sometime in 2008, Ouazzani swore an oath of allegiance to al-Qaeda and sent around \$23,000 to the group before he was arrested two years later.³²² In June 2013, at a hearing for the House Select Committee on Intelligence on the NSA surveillance programs, FBI Deputy Director Sean Joyce testified that Ouazzani also had some kind of a "nascent" plan to attack the New York Stock Exchange. Ouazzani's attorney denied that claim and court documents in his case do not mention any such plan. At the same hearing, Joyce and other top government officials pointed to these two cases as examples of the kinds of terrorist conspiracies NSA surveillance has disrupted^[1] in recent years, but they gave no new public information^[1] to substantiate a claim made by General Keith Alexander, NSA's director, a week earlier that "dozens of terrorist events" had been averted both in the United States and abroad.³²⁴ Alexander said he would provide members of the House Intelligence Committee with additional information about the some 50 other terrorist plots that had been averted as a result of NSA surveillance, but this would be behind closed doors as the details of these plots remain classified. Speaking at Black Hat, an information-security conference, a month later, General Alexander provided more specific numbers, saying that NSA surveillance had prevented 54 terrorist-related activities worldwide, including 13 terrorist activities within the United States. The public record suggests that few of these plots involved attacks within the United States, because traditional law enforcement methods have overwhelmingly played the most significant role in foiling terrorist attacks. According to a survey by the New America Foundation, jihadist extremists based in the United States have mounted 47 plots to conduct attacks within the United States since 2001.³²⁶ Of those plots, nine involved an actual terrorist act that was not prevented by any type of government action, such as the 2009 shooting spree at Fort Hood, Texas. Of the remaining 38 plots, the public record shows that at least 33 were uncovered by using

standard policing practices such as informants, undercover officers, and tips to law enforcement.

At the House Intelligence Committee hearing, the FBI's Sean Joyce also pointed to the 2009 plots by Najibullah Zazi as well as David Coleman Headley's plan to attack a Danish newspaper as attacks that were also disrupted by NSA monitoring. As Joyce explained, the plot by Zazi to attack the New York subway system around the eighth anniversary of the 9/11 attacks was "the first core al-Qaeda plot since 9/11" that was directed from Pakistan inside the United States.³²⁷ There is no doubt that it was a serious plot, but if it was the only such plot on U.S. soil that the government averted as^[T] a result of the NSA's surveillance monitoring, the public^[T] will have to decide whether it justifies the large-scale government surveillance programs—no matter how carefully they are run.

The only cited example of a successful call log program is Somalia and Bergen just answered this

New York Times, 9-26, 13, http://www.nytimes.com/2013/09/27/us/politics/senators-push-to-preserve-nsa-phone-surveillance.html?_r=0

Officials have struggled to identify terrorist attacks that would have been prevented by the call log program, which has existed in its current form since 2006. The clearest breakthrough attributed to the program was a case involving several San Diego men who were prosecuted for donating several thousand dollars to a terrorist group in Somalia.¹ Mr. Wyden pressed General Alexander about whether the N.S.A. had ever collected, or made plans to collect, bulk records about Americans' locations based on cellphone tower data.¹ General Alexander replied that the N.S.A. is not doing so as part of the call log program, but that information pertinent to Mr. Wyden's question was classified.

NSA Telephone tracking hasn't disrupted terrorism and could be significantly abused

Peter Bergen, 9-10, 13, She is the director of the Homeland Security Project at the Bipartisan Policy Center, Jihadists Terrorism: A Threat Assessment, Political Transcript Wire, Peter Bergen is the author of four books about al-Qaeda, three of which were *New York Times* best sellers. The books have been translated into 20 languages. He is the director of the National Security Program at the New America Foundation in Washington, D.C.; a fellow at Fordham University's Center on National Security; and CNN's national security analyst.

BERGEN: Well, one way of answering that is -- I've -- talking about the NSA, obviously there's a debate, I mean, the vote was very close in House -- in -- in Congress, on this issue. And one of the -- one of the points we make in the report is, as far as we can tell from the public record, only one case -- what is controversial in the United States is, the telephone metadata; Americans care less about overseas e-mail traffic. As far as we can tell, only one case of the 212 cases since 9/11 came out of the telephone program, and it's a rather trivial case. It was a guy in San Diego who was sending money to Al-Shabaab, a few thousand dollars -- the Somalia al-Qaeda affiliate. Now, you know, sending money to Al-Shabaab is not something one -- one would want to encourage, but if the price of finding this one case is the government having access to all your phone records for the past five years, no matter how carefully they manage that

program, who's to say that some future administration, five years down the road, doesn't have quite the same view of the way the -- the data should be handled. So, I mean, that -- that would be question one, is are we in a situation -- I mean, I was astonished by this New York Times story where, you know, essentially every -- any program you use in the United States on a computer has a mandated back door into it that the NSA can basically get into. Is not -- **it seems a sort of fundamentally kind of un-American concept**, that basically everything that you -- and obviously, the people involved in this are well- intentioned. So I think we're doing a lot of the right things. We've had a long time over the last 12 years to get our counterterrorism policy right. We make some recommendations in the report, but I don't think there's some huge sort of magic wand that needs to be waved over the situation, but personally, and like a lot of other Americans, I am concerned about what seems to be this huge kind of grab of executive power on the issue of our private communications. Which, by the way, **it would be one thing if you could say, "Hey, all these NSA -- every terrorism case that we've found in this country was because of NSA surveillance."** As we say in the report, in fact, almost every case that is made is based on the typical things that make any criminal case: a suspicious activity report in 9 percent of these cases, a tip from a family or community member in 33 percent of these cases, an undercover cop or -- or an informer in about half of these cases. That's how these cases are made.

Meta data collection has not stopped a single terrorist attack

Nathaniel Mott, PandoDaily, June 30, 2014

Did the Snowden leaks make the US more vulnerable to terrorists? New NSA director is all, 'Nah we got this.'

Michael Rogers, the new director of the National Security Agency, said in an interview published today in the New York Times[1] that Edward Snowden's decision to leak information about the agency's surveillance programs hasn't led him to believe that the sky is falling. Have terrorists changed their habits since the programs were revealed?

Yes. Have they referenced information learned from news reports based on the documents Snowden leaked? Rogers said that they have. But have those changes stopped the NSA from surveilling those terrorists? Nope, they haven't. It seems that one of the greatest lies spread after Snowden's leaks might finally be put to rest. Countless people have argued that Snowden's decision to reveal the existence of the NSA's surveillance programs will allow terrorists to evade the agency and carry out plots, leaving the United States powerless to stop them. **So far as an argument for keeping those programs secret goes, it's a pretty good one -- or at least it would have been had the people making it been able to provide a single shred of evidence proving that these programs prevented a single terrorist attack when their claims were questioned. The New America Foundation skewered those claims[2] with a report studying the effect these bulk surveillance programs have had on the government's ability to prevent terrorist attacks. It concluded that there's no evidence supporting those claims, and that the single case provided by the government actually makes the bulk surveillance programs less defensible than before: Surveillance of American phone metadata has had no discernible**

impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program [...] calls into question the necessity of the Section 215 bulk collection program. [...] This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues. But the publication of this report -- and others that produced no evidence supporting claims that bulk surveillance programs have prevented terrorist attacks -- didn't stop people from claiming that Snowden's whistleblowing had compromised the US's ability to defend itself. As former Pando writer David Sirota explained in a blog post on the subject[3] written for Salon: These are the inconvenient truths that NSA defenders do not want the public to know because they threaten to ignite a powerful backlash against the surveillance state. Thus, without countervailing facts of their own, the agency's defenders are resorting to an age-old public relations trick: They are trying to scream a scary motto (in this case, 'national security!') as often and as loudly as possible to either distract everyone's attention or fully drown out any fact-based discourse. Rogers appears to be taking a different tack. Instead of pretending that one of the world's largest intelligence agencies has been crippled by the efforts of a lone whistleblower, he said in his interview with the Times that the NSA is adapting to the shifting landscape faster than its targets are using the information revealed by Snowden. That doesn't excuse the agency for its systematic erosion of personal liberty, but at least Rogers isn't going to hide behind the drumbeat of 'the terrorists will win!' like so many others have. [illustration by Brad Jonas]

AT Stopped Somali Funding

It's was an insignificant amount of \$ that didn't impact the groups' funding

Nathaniel Mott, PandoDaily, June 30, 2014

Did the Snowden leaks make the US more vulnerable to terrorists? New NSA director is all, 'Nah we got this.'

Michael Rogers, the new director of the National Security Agency, said in an interview published today in the New York Times[1] that Edward Snowden's decision to leak information about the agency's surveillance programs hasn't led him to believe that the sky is falling. Have terrorists changed their habits since the programs were revealed? Yes. Have they referenced information learned from news reports based on the documents Snowden leaked? Rogers said that they have. But have those changes stopped the NSA from surveilling those terrorists? Nope, they haven't. It seems that one of the greatest lies spread after Snowden's leaks might finally be put to rest. Countless people have argued that Snowden's decision to reveal the existence of the NSA's surveillance programs will allow terrorists to evade the agency and carry out plots, leaving the United States powerless to stop them. So far as an argument for keeping those programs secret goes, it's a pretty good one -- or at least it would have been had the people making it been able to provide a single shred of evidence proving that these programs prevented a single terrorist attack when their claims were questioned. The New America Foundation skewered those claims[2] with a report studying the effect these bulk surveillance programs have had on the government's ability to prevent terrorist attacks. It concluded that there's no evidence supporting those claims, and that the single case provided by the government actually makes the bulk surveillance programs less defensible than before: Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program [...] calls into question the necessity of the Section 215 bulk collection program. [...] This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues. But the publication of this report -- and others that produced no evidence supporting claims that bulk surveillance programs have prevented terrorist attacks -- didn't stop people from claiming that Snowden's whistleblowing had compromised the US's ability to defend itself. As former Pando writer David Sirota explained in a blog post on the subject[3] written for Salon: These are the inconvenient truths that NSA defenders do not want the public to know because they threaten to ignite a powerful backlash against the surveillance state. Thus, without countervailing facts of their own, the agency's defenders are resorting to an age-old public relations trick: They are trying to scream a scary motto (in this case, 'national security!') as often and as loudly as possible to either distract everyone's attention or fully drown out any fact-based discourse. Rogers appears to be taking a different tack. Instead of pretending that one of the world's largest intelligence agencies has been

crippled by the efforts of a lone whistleblower, he said in his interview with the Times that the NSA is adapting to the shifting landscape faster than its targets are using the information revealed by Snowden. That doesn't excuse the agency for its systematic erosion of personal liberty, but at least Rogers isn't going to hide behind the drumbeat of 'the terrorists will win!' like so many others have. [illustration by Brad Jonas]

Moalin data not worth it

Matthias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Does the Moalin case justify putting the phone records of hundreds of millions of U.S. citizens into the hands of the federal government? "Stopping the money is a big deal," Joel Brenner, the N.S.A.'s former inspector general, told me. Alexander called Moalin's actions "the seed of a future terrorist attack or set of attacks." But Senator Leahy contends that stopping a few thousand dollars, in one instance, over thirteen years, is a weak track record. The program "invades Americans' privacy" and "has not been proven to be effective," he said last week. The Moalin case, he continued, "was not a 'plot' but, rather, a material-support prosecution for sending a few thousand dollars to Somalia."

Metadata didn't help with the Basaaly Molan investigation

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 9-1-14

The investigation of Basaaly Moalin is the only case in which Section 215 records demonstrably contributed to the identification of an unknown terrorism suspect. In 2007, the NSA provided the FBI with information showing an indirect connection between a telephone number in Somalia, which the NSA was tracking because of its association with the Al Shabaab terrorist organization, and an unknown telephone number in San Diego. The NSA reported this information to the FBI, which realized that the telephone number was linked to pending FBI investigations. Based on the NSA's report and the link between this telephone number and pending investigations, the FBI opened a preliminary investigation into the number.

Using a national security letter and database checks, the FBI identified the user of the San Diego telephone number as Basaaly Moalin, the subject of a previous FBI investigation that was closed several years earlier for lack of sufficient information. The FBI reopened the case, and through subsequent investigation it learned that Moalin and three others were providing material support to Al Shabaab. All four men were convicted in 2013 of providing funds to the terrorist organization. The NSA's report was the catalyst that prompted the FBI to investigate Moalin's San Diego number. Even without the NSA's tip-off, however, FBI agents may well have discovered that the number was a common link among pending FBI investigations. Moreover, given that the NSA's tip came from monitoring a specific foreign number it was tracking, it is not clear to us that bulk collection of telephone records was necessary to discovering the connection between this number and Moalin's. Conventional techniques may have been less likely to discover it, or at least more time-consuming. But we know of no indication that speed or Section 215's five-year depth of records were important to the discovery. In addition, we believe it worthy of note that Moalin and his associates were not charged or convicted of involvement in planning or executing any specific terrorist plots.

Their crime was sending money to Al Shabaab. While there is a critical value in cutting off funds to deadly foreign terrorist organizations such as this one, we find it significant that in the seven-year history of the NSA's Section 215 program, this material-support prosecution remains the only time that the program has directly contributed to the identification of an unknown terrorism suspect. And even in this instance, as noted, Moalin was not entirely unknown to law enforcement, but rather was the subject of a previous FBI investigation and was the user of a telephone number already linked to pending FBI investigations. In our view, therefore, it is telling that the Moalin case represents perhaps the strongest success story produced by the NSA's Section 215 program. Like the other three cases discussed above, the Moalin investigation shows that the program does provide some demonstrable value in supporting the government's counterterrorism efforts. But it also starkly illustrates the limits of what the program has accomplished, and perhaps what it is capable of accomplishing.

AT Section 215 Stopped NY Stock Exchange Attacks

Telephone records did not make operation WIFI possible

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 9-1-14

Our analysis of another 2009 case, which involved an early stage plot to attack the New York Stock Exchange, also fails to demonstrate that the Section 215 program has offered significant added value to the government's counterterrorism efforts. While conducting Internet surveillance of an extremist based in Yemen, the NSA discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA provided information about this connection to the FBI. In the course of its investigation, the FBI subsequently identified the unknown person as an individual named Khalid Ouazzani, and it discovered that he was in communication with other individuals located in the United States who were in the very initial stages of devising a plan to bomb the New York Stock Exchange. All of these individuals eventually were convicted for their roles in the nascent plot. After the FBI discovered the plot and identified the individuals involved, the NSA queried telephone numbers associated with those individuals using Section 215, providing additional telephone numbers as leads to the FBI. Those numbers simply mirrored information about telephone connections that the FBI developed independently using other authorities. Thus, while Section 215 was used in the Operation Wi-Fi investigation, we are aware of no indication that bulk collection of telephone records was necessary to the investigation, or that the information produced by Section 215 provided any unique value.

AT Section 215 Was Critical to Catch the Capitol Bomber

A targeted phone records search may have helped to catch the capitol bomber, not bulk data collection

Julian Shanchez, January 16, 2015, Just Security, “Decrypting John Boehner on the Capitol Hill Bomber” <http://thehill.com/policy/defense/229990-gop-headed-for-battle-over-the-patriot-act> DOA: 1-20-15

As *The Guardian's* Spencer Ackerman notes, however, this seems conspicuously at odds with the FBI's own account of how alleged plotter Christopher Cornell was identified. According to the criminal complaint, it was an informant hoping to reduce his own criminal sentence who brought Cornell to the Bureau's attention. Nor, indeed, was Cornell particularly subtle: Under the Twitter handle ISBlackFlags, he pseudonymously voiced support for the Islamic State and violent jihad. If that's true, then while it would hardly be surprising if Cornell's phone records were reviewed at some point in the investigation, it's hard to see how a bulk telephone database could have been essential to identifying him. Once Cornell had been identified, of course, traditional targeted intelligence or law enforcement authorities would have been sufficient to allow investigators access to his metadata—or, for that matter, his online communications.

Surveillance not responsible for preventing the Capitol attacks

Julian Hattem, January 20, 2015, The Hill, “GOP Faces PATRIOT Act Choice,” <http://thehill.com/policy/defense/229990-gop-headed-for-battle-over-the-patriot-act> DOA: 1-20-15

“I'm going to say this one more time because you're going to hear about it for months and months to come as we attempt to reauthorize the FISA program,” he added. “Our government does not spy on Americans, unless they are Americans who are doing things that frankly tip off our law enforcement officials to an imminent threat.” Critics of the spy agency were quick to question Boehner's take on the Capitol plot. The FBI said it relied on Twitter messages and an undercover source to gather information about the suspect, Christopher Cornell — not wiretaps or call records. “[T]here is every reason to be extremely skeptical of the implication that the [Section] 215 database, or indeed, any novel FISA authorities, played an essential role in the investigation of Cornell,” Julian Sanchez, a senior research fellow at the libertarian Cato Institute, wrote in a blog post on Friday.

AT Section 215 Key to David Coleman Headley Investigation

Telephone records not key to the David Coleman Headley investigation

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 9-1-14

In October 2009, Chicago resident David Coleman Headley was arrested and charged for his role in plotting to attack the Danish newspaper that published inflammatory cartoons of the Prophet Mohammed. He was later charged with helping orchestrate the 2008 Mumbai hotel attack, in collaboration with the Pakistan-based militant group Lashkar-e-Taiba. He pled guilty and began cooperating with authorities. Headley, who had previously served as an informant for the Drug Enforcement Agency, was identified by law enforcement as involved in terrorism through means that did not involve Section 215. Further investigation, also not involving Section 215, provided insight into the activities of his overseas associates. In addition, Section 215 records were queried by the NSA, which passed on telephone numbers to the FBI as leads. Those numbers, however, only corroborated data about telephone calls that the FBI obtained independently through other authorities. Thus, we are aware of no indication that bulk collection of telephone records through Section 215 made any significant contribution to the David Coleman Headley investigation.

Ext – Examples Stopped Through Other Means

Examples of prevented terror attacks would have been stopped through other means

Shaina Kalanges, Summer 2014, Kalanges is a second-year law student at the Northern Illinois University College of Law with a Bachelor of Arts from the University of Illinois Urbana-Champaign. Modern Private Data Collection and National Security Agency Surveillance: A Comprehensive Package of Solutions Addressing Domestic Surveillance Concerns, Northern Illinois University Law Review

http://www.niu.edu/law/organizations/law_review/pdfs/full_issues/34_3/Kalanges_FINAL%206.pdf, DOA: 1-20-15, p. 653

While Judge Pauley reasoned that any issues with noncompliance were weeded out of the current surveillance process, one legislative proposal, which gained nearly eighty-five sponsors, reacts to this issue quite differently and suggests that more may be done to insure American civil liberties. Additionally, Judge Leon in Klayman picked apart the examples of metadata collection that the government provided to demonstrate the metadata program's progress in preventing terrorist attacks. The Klayman court discerned that any uncovered terrorists were already found with other evidence that the metadata program merely corroborated.

AT Section 215 Increases the Speed of Terror Investigations

Metadata doesn't increase the speed and efficiency in which terrorism can be prevented

Richard Leon, US District Judge, December 13, 2013, Klayman v Obama,
<http://legaltimes.typepad.com/files/obamansa.pdf>,
957 F. Supp. 2d 1; 2013 U.S. Dist. LEXIS 176925; 59 Comm. Reg. (P & F) 825, p. 107-10

The Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose" of "identifying unknown terrorist operatives and preventing terrorist attacks. Govt.'s Opp'n at 51—an interest that everyone, including this Court, agrees is "of the highest order of magnitude," *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *see also Haig v. Agee*, 453 U.S. 280, 307, 101 S. Ct. 2766, 69 L. Ed. 2d 640 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)).⁶⁶ **A closer examination of the record, however, reveals that the Government's interest is a bit more nuanced—it is not merely to investigate potential terrorists, but rather, to do so faster than other investigative methods might allow. Indeed, the affidavits in support of the Government's brief repeatedly emphasize this interest in speed. For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the Government to quickly analyze past connections and chains of communication," and "increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations.** Shea Decl. ¶ 46 (emphases added); *see also id.* ¶ 59 ("Any other means that might be used to attempt to conduct similar analyses would require *multiple, time-consuming steps* that would frustrate needed *rapid* analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis." (emphases added)). FBI Acting Assistant Director of the Counterterrorism Division Robert J. Holley echoes Director Shea's emphasis on speed: "It is imperative that the United States Government have the capability to *rapidly* identify any terrorist threat inside the United States." Holley Decl. ¶ 4 (emphasis added); *see also id.* ("[T]he *agility* of querying the metadata collected by NSA under this program allows for more *immediate* contact chaining, which is significant in *time-sensitive* situations The *delay* inherent in issuing new national security letters would necessarily mean losing *valuable time*. . . . [A]gggregating the NSA telephony metadata from different telecommunications providers enhances and *expedites* the ability to identify chains of communications across multiple providers." (emphases added)). **Yet, turning to the efficacy prong, the Government does not cite a single instance in which analysis [**110] of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency.** In the first example, the FBI learned of a terrorist plot still "in its early stages" and investigated that plot before turning to the metadata "to ensure that all potential connections were identified. Assistant Director Holley does not say that the metadata revealed any new information—much less time-sensitive information—that had not already come to light in the investigation up to that point. *Id.* In the

second example, it appears that the metadata analysis was used only after the terrorist was arrested "to establish [his] foreign ties and put them in context with his U.S. based planning efforts. And in the third, the metadata analysis "revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists." Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only *sometimes* provides information earlier than the FBI's other investigative methods and techniques." (emphasis added).⁶⁴ Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.⁶⁵ See *Chandler*, 520 U.S. at 318-19 ("Notably lacking in respondents' presentation is any indication of a concrete danger demanding departure from the Fourth Amendment's main rule."). **Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.**⁶⁶

No evidence

NSN 1-17 (National Security Network,- non-profit foreign policy organization headquartered in Washington, D.C., United States, that focuses on international relations, global affairs and national security. Characterizing itself as "progressive," the NSN's mission statement asserts the group aims to "build a strong progressive national security and counter conservative spin." with 2,000 members and experts represent the emerging generation of foreign policy leaders. With a wealth of experience in government service, the private sector and the non-profit sector "The National Security Benefits of NSA Reform")

Counterterrorism value of NSA metadata to preventing terrorist attack open to question, yet to be demonstrated by government. **Senior officials have justified the value of the metadata or "bulk" collection programs in terms of their ability to rapidly turn around counterterrorism intelligence in response to a time-sensitive need. However, DC District Court Judge Richard Leon who presided over a challenge to the metadata collection program last year, writes that "Given the limited record before me at this point in the litigation — most notably the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics — I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism."** Importantly, during court proceedings, **the government shared only limited evidence with the court and did not provide additional evidence when invited to do so, leaving the issue of justification open.** [Richard Leon via USA Today, 12/16/13] Additionally, **a report by New America Foundation's Peter Bergen et al. concluded that "in-depth analysis" of 225 terrorism cases related to "the government's claims about the role that NSA 'bulk' surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading," adding that "the contribution of NSA's bulk surveillance programs to these cases was minimal."** [Peter Bergen et al., 1/14]

AT Section 215 Would Have Stopped 9-11 if it Existed Then

Section 215 metadata collection would not have stopped 9-11

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

Some have suggested that if the NSA's calling records program were in place before 9/11, it could have alerted the government that one of the future airplane hijackers was in the United States, and perhaps have led to the prevention of the attacks. For several years, beginning in the late 1990s, the NSA intercepted telephone calls to and from a prominent Al Qaeda safe house in Yemen. A number of calls were made in early 2000 between this safe house and a person named Khalid, who after 9/11 was identified as hijacker Khalid al-Mihdhar. Although the NSA was able to listen to these conversations, it did not have the telephone number that was calling the safe house, and thus it did not know that Mihdhar made the calls from San Diego, California. Had the NSA known this information, it is argued, the government could have identified Mihdhar as the caller and been aware of his presence in the United States, perhaps leading to his apprehension and the identification and detention of other hijackers. **For two reasons, we do not believe the Mihdhar example supports continuance of the NSA's Section 215 program. First, the failure to identify Mihdhar's presence in the United States stemmed primarily from a lack of information sharing among federal agencies, not of a lack of surveillance capabilities.** As documented by the 9/11 Commission and others, this was a failure to connect the dots, not a failure to collect enough dots. **Second, in order to have identified the San Diego telephone number from which Mihdhar made his calls, it was not necessary to collect the entire nation's calling records.** As explained by the 9/11 Commission Report, the joint inquiry into the 9/11 attacks by the House and Senate intelligence committees, and a Department of Justice Inspector General report, **the government had ample opportunity before 9/11 to pinpoint Mihdhar's location, track his activities, and prevent his 2001 reentry into the United States. By early 2000, the CIA was** aware of Mihdhar and knew that he had a visa enabling him to travel to the United States. Yet despite having information that Mihdhar and fellow hijacker Nawaf al-Hazmi "were traveling to the United States," **the CIA "missed repeated opportunities to act based on the information in its possession."** The agency **did not advise the FBI of what it knew or "add their names to watchlists."** Furthermore, at the time that Mihdhar and Hazmi were in San Diego in early 2000, when the calls to Yemen were made, they were living with "a long-time FBI asset." Mihdhar left the United States in June 2000, and he was able to return in 2001 because he still had not been placed on any watchlists. And "[o]n four occasions in 2001, the CIA, the FBI, or both had apparent opportunities to refocus on the significance of Hazmi and Mihdhar and reinvigorate the search for them." Yet these opportunities were missed. **It is argued**, however, **the NSA's bulk telephone records program could have made up for these intelligence lapses** and failures of information sharing. Knowledge that the telephone calls from "Khalid" to the Yemen safe house were made from San Diego theoretically could have led the government to discover Mihdhar's presence in the United States. **But obtaining this knowledge did not require a bulk telephone records program. The NSA knew the telephone number of the Yemen safe house. If the telephone calls with Mihdhar were deemed suspicious at the time, the government could have used existing legal authorities to request from U.S. telephone companies the records of any calls made to or from that Yemen number.** Doing so could have identified the San Diego number on the other

end of the calls. Thus we do not believe that a program that collects all telephone records from U.S. telephone companies was necessary to identify Mihdhar's location in early 2000, nor that such a program is necessary to make similar discoveries in the future.

9-11 argument is just speculation and proves the terrorism link is unsupported

USA Today, 10-20, 13, <http://www.usatoday.com/story/opinion/2013/10/20/nsa-surveillance-privacy-editorials-debates/3115167/> DOA: 1-15-15

Until Snowden's revelations made headlines, most lawmakers knew little about these collections. Now Congress is considering whether to curtail or kill the phone records program — the most expansive of the initiatives that have been exposed and a test of where to draw the line between what the government wants and what it actually needs. In that debate, the burden should be on the NSA to prove that the program's benefits outweigh its costs, which Alexander has struggled to do. Initially in June, he testified that the phone database, along with a less intrusive e-mail program targeting foreign suspects, had helped disrupt "potential terrorist events over 50 times since 9/11." By July, under skeptical questioning by Senate Judiciary Chairman Patrick Leahy, D-Vt., Alexander's deputy said the phone data "made a contribution" in just 12 cases. And at a symposium in Aspen, when asked how often phone data were the "tip-off" to a plot, Alexander replied: "I don't have the numbers off the top of my head to break it out like that." Now supporters of the program have fallen back on what-ifs about 9/11. If intelligence agencies had phone metadata before 9/11, they argue, it would have revealed one of the terrorists who was in the U.S. well before the attack. Talk about rewriting history. The tragic flaw before 9/11 was not lack of data but failure to share what agencies already knew.

AT Section 215 Will Stop Future Attacks

Since section 215 hasn't stopped past attacks, it is unlikely it will stop future attacks

Privacy and Civil Liberties Oversight Board, January 23, **2014**, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 1-13-14

Finally, in the absence of evidence that the NSA's Section 215 program has made any significant contribution to counterterrorism efforts to date, some officials have suggested to us that the program should be preserved because it might do so in the future. Like a burglar alarm or a fire insurance policy, under this reasoning, the program is valuable even if it has not yet been triggered by a break-in or a fire. Yet, it is worth noting that the program supplied no advance notice of attempted attacks on the New York City subway, the failed Christmas Day airliner bombing, or the failed Times Square car bombing. Given the limited value this program has demonstrated to date, as outlined above, we find little reason to expect that it is likely to provide significant value, much less essential value, in safeguarding the nation in the future.

No single successful program

Privacy and Civil Liberties Oversight Board, January 23, **2014**, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

Based on the information provided to the Board, we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program contributed directly to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. In that case, moreover, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program. Even in those instances where telephone records collected under Section 215 offered additional information about the contacts of a known terrorism suspect, in nearly all cases the benefits provided have been minimal — generally limited to corroborating information that was obtained independently by the FBI. And in those few cases where some information not already known to the government was generated through the use of Section 215 records, we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records. The classified briefings and materials the Board has received have not demonstrated that the increased speed, breadth, and historical depth of the Section 215 program have produced any concrete results that were otherwise unattainable. In other words, we see little evidence that the unique capabilities provided by the NSA's bulk collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program.

AT Section 215 Stopped the Zanzi/NY City Attack

Section 215 didn't prevent the Zazi/NY City terror attack

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf

While Section 215 was used during the Zazi investigation, it played no role in thwarting the subway bombing plot. The plot was discovered through email monitoring, and its details were fleshed out through additional electronic surveillance, physical surveillance, and other traditional investigative measures. The plot was disrupted when law enforcement inadvertently tipped off Zazi that he was being monitored, leading him and his associates to abandon their plans and prompting him to return to Colorado. Although the NSA provided the FBI with a report early in the investigation showing calls made from Zazi's telephone, and later provided additional leads based on the Section 215 data, these reports did not identify Zazi's associates in New York City or the apartments where materials intended to support the bombing were found. Rather, other investigative techniques led to those discoveries.

The only concrete result obtained in the Zazi case through the use of Section 215 was to identify an unknown telephone number of one of Zazi's New York coconspirators, Adis Medunjanin. The FBI, however, already was aware of Medunjanin and his connection to Zazi's plot, having obtained that information independently using other means. And while the NSA's information may have further heightened the FBI's interest in Medunjanin, there is no indication that use of the NSA's bulk collection program was necessary for the government to identify the unknown telephone number, or that this information was not obtainable through more traditional law enforcement techniques. Despite being under suspicion from the outset of the plot's discovery in September 2009, Medunjanin was not arrested until January 2010, several months after Zazi returned to Colorado and was taken into custody. As far as we can tell, the particular speed associated with Section 215 queries offered no apparent benefit in corroborating the FBI's interest in Medunjanin. Nor did the ability to search through five years of records or to have immediate access to several "hops" of telephone calls.

The Zazi case shows how Section 215 is used to complement other investigative tools, as intelligence community officials have emphasized. In our view, it also illustrates the minimal added benefit provided by the program in light of those other tools.

AT Now Terrorists Know We are Trying to Monitor Their Communication

Irrelevant – The information has already been made public

This just takes-out the disadvantage – it proves they will avoid these networks now

Terrorists would know the government was already trying to monitor their communications

They already knew

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Aside from my contempt for the process— the government should not be a collaborative editorial partner with newspapers in deciding what gets published— I knew there was no plausible national security argument against our specific Verizon report, which involved a simple court order showing the systematic collection of Americans' telephone records. The idea that “terrorists” would benefit from exposing the order was laughable: any terrorists capable of tying their own shoes would already know that the government was trying to monitor their telephone communications. The people who would learn something from our article weren’t the “terrorists” but the American people. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 1163-1167). Henry Holt and Co.. Kindle Edition.

AT Congressional Support Proves Democratic Support for Section 215

Section 215 not being used in the way Congress intended

Privacy and Civil Liberties Oversight Board, January 23, 2014, Report on the Telephone Records Program, https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf DOA: 9-1-14

In order for business records or other tangible things to be acquired through Section 215, the government must provide a statement of facts showing reasonable grounds to believe that they are “relevant to an authorized investigation (other than a threat assessment)” to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities. Before examining whether the massive quantity of telephone records acquired under Section 215 can plausibly be regarded as relevant to the government’s counterterrorism efforts, given that nearly all of them are not connected to terrorism in any way, the latter part of the statutory formulation “relevant to an authorized investigation” merits independent consideration. Regardless of how expansively the word “relevant” may be construed, the statute demands some nexus between the records sought and a specific investigation. Notably, **Section 215 requires that records sought be relevant to “an” authorized investigation.**

Elsewhere, the statute similarly describes the records that can be obtained under its auspices as those sought “for an investigation.” The use of the singular noun in these passages signals an expectation that the records are being sought for use in a specific, identified investigation. **This interpretation is reinforced by the requirement that the FISA court make specific findings about the investigation for which the records are sought** — that it is supported by a factual predicate, conducted according to guidelines approved by the Attorney General, and not based solely upon activities protected by the First Amendment when conducted of a U.S. person. **The government’s applications to the FISA court seeking renewal of the NSA’s program do not link the applications to a single counterterrorism investigation. Instead, the applications list multiple terrorist organizations, assert that the FBI is investigating all of them, and declare that the telephone records being sought are relevant to each of those investigations.** The FISA court orders granting the government’s applications all contain a finding that there are reasonable grounds to believe that the records sought are relevant to authorized “investigations.” **The orders further conclude that these investigations satisfy the three criteria listed above.** **The FISA court has stated that the purpose of the government’s applications “is to obtain foreign intelligence information in support of . . . individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations.** The government’s approach, in short, has been to declare that the calling records being sought are relevant to all of the investigations cited in its applications. **This approach, at minimum, is in deep tension with the statutory requirement that items obtained through a Section 215 order be sought for “an investigation,” not for the purpose of enhancing the government’s counterterrorism capabilities generally. Declaring that the calling records are relevant to every counterterrorism investigation cited by the government is little different, in practical terms, from simply declaring that they are relevant to counterterrorism in general.** That is particularly so when the number of calling records sought is not limited by reference to the facts of any specific investigation. **At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations.** The Board does not believe that this approach comports with a fair

reading of the statute. Moreover, this approach undermines the value of an important statutory limitation on the government's collection of records under Section 215. The statute provides that records cannot be obtained for a "threat assessment," meaning those FBI investigatory activities that "do not require a particular factual predicate." By excluding threat assessments from the types of investigations that can justify an order, Congress directed that Section 215 not be used to facilitate the broad and comparatively untethered investigatory probing that is characteristic of such assessments. But by collecting the nation's calling records en masse, under an expansive theory of their relevance to multiple investigations, the NSA's program undercuts one of the functions of the "threat assessment" exclusion: ensuring that records are not acquired by the government without some reason to suspect a connection between those records and a specific, predicated terrorism investigation. While the rules governing the program limit the use of telephone records to searches that are prompted by a specific investigation, the relevance requirement in Section 215 restricts the acquisition of records by the government.

Terrorists would know the government was already trying to monitor their communications

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Aside from my contempt for the process—the government should not be a collaborative editorial partner with newspapers in deciding what gets published—I knew there was no plausible national security argument against our specific Verizon report, which involved a simple court order showing the systematic collection of Americans' telephone records. The idea that "terrorists" would benefit from exposing the order was laughable: any terrorists capable of tying their own shoes would already know that the government was trying to monitor their telephone communications. The people who would learn something from our article weren't the "terrorists" but the American people. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 1163-1167). Henry Holt and Co.. Kindle Edition.

The only argument in favor of mass surveillance -- terrorism prevention – false

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Surveillance cheerleaders essentially offer only one argument in defense of mass surveillance: it is only carried out to stop terrorism and keep people safe. Indeed, invoking an external threat is a historical tactic of choice to keep the population submissive to government powers. The US government has heralded the danger of terrorism for more than a decade to justify a host of radical acts, from renditions and torture to assassinations and the invasion of Iraq. Ever since the

9/ 11 attack, US officials reflexively produce the word “terrorism.” It is far more of a slogan and tactic than an actual argument or persuasive justification for action. And in the case of surveillance, overwhelming evidence shows how dubious a justification it is. To begin with, much of the data collection conducted by the NSA has manifestly nothing to do with terrorism or national security. Intercepting the communications of the Brazilian oil giant Petrobras or spying on negotiation sessions at an economic summit or targeting the democratically elected leaders of allied states or collecting all Americans’ communications records has no relationship to terrorism. Given the actual surveillance the NSA does, stopping terror is clearly a pretext. Moreover, the argument that mass surveillance has prevented terror plots —a claim made by President Obama and a range of national security figures— has been proved false. As the Washington Post noted in December 2013, in an article headlined “Officials’ Defenses of NSA Phone Program May Be Unraveling ,” a federal judge declared the phone metadata collection program “almost certainly” unconstitutional, in the process saying that the Justice Department failed to “cite a single case in which analysis of the NSA’s bulk metadata collection actually stopped an imminent terrorist attack.” That same month, Obama’s hand-picked advisory panel (composed of, among others, a former CIA deputy director and a former White House aide, and convened to study the NSA program through access to classified information) concluded that the metadata program “was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional [court] orders.” Quoting the Post again: “In congressional testimony, [Keith] Alexander has credited the program with helping to detect dozens of plots both in the United States and overseas” but the advisory panel’s report “cut deeply into the credibility of those claims.” Additionally, as Democratic senators Ron Wyden, Mark Udall, and Martin Heinrich—all members of the Intelligence Committee— baldly stated in the New York Times, the mass collection of telephone records has not enhanced Americans’ protection from the threat of terrorism. The usefulness of the bulk collection program has been greatly exaggerated. We have yet to see any proof that it provides real, unique value in protecting national security. In spite of our repeated requests, the N.S.A. has not provided evidence of any instance when the agency used this program to review phone records that could not have been obtained using a regular court order or emergency authorization. A study by the centrist New America Foundation testing the veracity of official justifications for the bulk metadata collection concurred that the program “has had no discernible impact on preventing acts of terrorism.” Instead, as the Washington Post noted , in most cases where plots were disrupted the study found that “traditional law enforcement and investigative methods provided the tip or evidence to initiate the case.” The record is indeed quite poor. The collect-it-all system did nothing to detect, let alone disrupt, the 2012 Boston Marathon bombing. It did not detect the attempted Christmas-day bombing of a jetliner over Detroit, or the plan to blow up Times Square, or the plot to attack the New York City subway system— all of which were stopped by alert bystanders or traditional police powers. It certainly did nothing to stop the string of mass shootings from Aurora to Newtown. Major international attacks from London to Mumbai to Madrid proceeded without detection, despite involving at least dozens of operatives. And despite exploitative claims from the NSA, bulk surveillance would not have given the intelligence services better tools to prevent the attack on 9/ 11. Keith Alexander , speaking to a House intelligence committee, said, “I would much rather be here today debating” the program “than trying to explain how we failed to prevent another 9/ 11.” (The same argument, verbatim, appeared in talking points the NSA gave its employees to use to fend off questions.) The implication is rank fearmongering and deceitful in the extreme. As CNN security analyst Peter Bergen has shown, the CIA had multiple reports about an al-Qaeda plot and “quite a bit of information about two of the hijackers and their presence in the United States,” which “the

agency didn't share with other government agencies until it was too late to do anything about it." Lawrence Wright, the New Yorker's al-Qaeda expert, also debunked the NSA's proposition that metadata collection could have stopped 9/ 11, explaining that the CIA "withheld crucial intelligence from the FBI, which has the ultimate authority to investigate terrorism in the U.S. and attacks on Americans abroad ." The FBI could have stopped 9/ 11, he argued. It had a warrant to establish surveillance of everyone connected to Al Qaeda in America. It could follow them, tap their phones, clone their computers, read their e-mails, and subpoena their medical, bank, and credit-card records . It had the right to demand records from telephone companies of any calls they had made. There was no need for a metadata-collection program. What was needed was cooperation with other federal agencies, but for reasons both petty and obscure those agencies chose to hide vital clues from the investigators most likely to avert the attacks. The government was in possession of the necessary intelligence but had failed to understand or act on it. The solution that it then embarked on—to collect everything, en masse— has done nothing to fix that failure. Over and over, from multiple corners, the invocation of the terrorism threat to justify surveillance was exposed as a sham.

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2828-2832). Henry Holt and Co.. Kindle Edition.

Extension Mass Surveillance Undermines the War on Terror (Information Overload)

Mass surveillance creates noise that makes disrupting terrorism more difficult

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

In fact, mass surveillance has had quite the opposite effect : it makes detecting and stopping terror more difficult. Democratic Congressman Rush Holt, a physicist and one of the few scientists in Congress, has made the point that collecting everything about everyone's communications only obscures actual plots being discussed by actual terrorists. Directed rather than indiscriminate surveillance would yield more specific and useful information. The current approach swamps the intelligence agencies with so much data that they cannot possibly sort through it effectively. Beyond providing too much information, NSA surveillance schemes end up increasing the country's vulnerability: the agency's efforts to override the encryption methods protecting common Internet transactions—such as banking, medical records, and commerce—have left these systems open to infiltration by hackers and other hostile entities. Security expert Bruce Schneier, writing in the Atlantic in January 2014, pointed out: Not only is ubiquitous surveillance ineffective, it is extraordinarily costly.... It breaks our technical systems, as the very protocols of the Internet become untrusted... It's not just domestic abuse we have to worry about; it's the rest of the world, too. The more we choose to eavesdrop on the Internet and other communications technologies, the less we are secure from eavesdropping by others . Our choice isn't between a digital world where the NSA can eavesdrop and one where the NSA is prevented from eavesdropping; it's between a digital world that is vulnerable to all attackers, and one that is secure for all users. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2841-2845). Henry Holt and Co.. Kindle Edition.

NSA collects so much data it creates useless noise

Joshua Kapstein, May 16, 2014, “The NSA Can ‘Collect it All,’”, but what would it do with the data?, <http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html>

A point commonly made by NSA critics is that these dragnets collect not enough signal and too much noise. Several internal documents give that credence, including one that admits the NSA “collects far more content than is routinely useful to analysts.” A top-secret chart in Greenwald’s book displaying “Current Volumes and Limits” for data storage shows that the agency collected upwards of 20 billion “communications events” per day in 2012, the vast majority of which were stored in various databases. In December of the same year, a program called “Shelltrumpet” processed its 1 trillionth metadata record; almost half that amount was processed in 2012 alone. Such statistics seem to be cause for both celebration and headache within the NSA. Another classified slide, titled “The Challenge,” states that “Collection is outpacing our ability to ingest, process, and store the ‘norms’ to which we have been

accustomed.” This overcollection is such a widely acknowledged problem that the agency has a separate line in its budget devoted to “coping with information overload.”

AT Moalin/Saudi Capture

Moalin would have been caught anyhow

Matthatias Schwartz, January 26, 2015, The New Yorker, “The Whole Haystack,”
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

It's possible that Moalin would have been caught without Section 215. His phone number was "a common link among pending F.B.I. investigations," according to a report from the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency created in 2004 at the suggestion of the 9/11 Commission, which Obama had tasked with assessing Section 215. Later, in a congressional budget request, the Department of Justice said that the Moalin case was part of a broader investigation into Shabaab funding. Senator Ron Wyden, of Oregon, who, like Leahy, has pressured the N.S.A. to justify bulk surveillance, said, "To suggest that the government needed to spy on millions of law-abiding people in order to catch this individual is simply not true." He continued, "I still haven't seen any evidence that the dragnet surveillance of Americans' personal information has done a single thing to improve U.S. national security." Representative James Sensenbrenner, of Wisconsin, who introduced the Patriot Act in the House, agreed. "The intelligence community has never made a compelling case that bulk collection stops terrorism," he told me. Khalid al-Mihdhar's phone calls to Yemen months before he helped hijack American Airlines Flight 77, on 9/11, led Obama, Alexander, Feinstein, and others to suggest that Section 215 could have prevented the attacks. "We know that we didn't stop 9/11," Alexander told me last spring. "People were trying, but they didn't have the tools. This tool, we believed, would help them."

AT More Data Needed to Fight Terrorism

More data is not needed – all attacks accomplished by known terrorists

Matthias Schwartz, January 26, 2015, The New Yorker, “The Whole Haystack,”
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Almost every major terrorist attack on Western soil in the past fifteen years has been committed by people who were already known to law enforcement. One of the gunmen in the attack on Charlie Hebdo, in Paris, had been sent to prison for recruiting jihadist fighters. The other had reportedly studied in Yemen with Umar Farouk Abdulmutallab, the underwear bomber, who was arrested and interrogated by the F.B.I. in 2009. The leader of the 7/7 London suicide bombings, in 2005, had been observed by British intelligence meeting with a suspected terrorist, though MI5 later said that the bombers were “not on our radar.” The men who planned the Mumbai attacks, in 2008, were under electronic surveillance by the United States, the United Kingdom, and India, and one had been an informant for the Drug Enforcement Administration. One of the brothers accused of bombing the Boston Marathon was the subject of an F.B.I. threat assessment and a warning from Russian intelligence In each of these cases, the authorities were not wanting for data. What they failed to do was appreciate the significance of the data they already had. Nevertheless, since 9/11, the National Security Agency has sought to acquire every possible scrap of digital information—what General Keith Alexander, the agency’s former head, has called “the whole haystack.” The size of the haystack was revealed in June, 2013, by Edward Snowden. The N.S.A. vacuums up Internet searches, social-media content, and, most controversially, the records (known as metadata) of United States phone calls—who called whom, for how long, and from where. The agency stores the metadata for five years, possibly longer.

FBI had plenty of data prior to 9-11 and didn't act on it

Matthias Schwartz, January 26, 2015, The New Yorker, “The Whole Haystack,”
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

In retrospect, every terrorist attack leaves a data trail that appears to be dotted with missed opportunities. In the case of 9/11, there was Mihdhar’s landlord, the airport clerk who sold Mihdhar his one-way ticket for cash, and the state trooper who pulled over another hijacker on September 9th. In August, 2001, F.B.I. headquarters failed to issue a search warrant for one of the conspirators’ laptops, despite a warning from the Minneapolis field office that he was “engaged in preparing to seize a Boeing 747-400 in commission of a terrorist act.” There was plenty of material in the haystack. The government had adequate tools to collect even more. The problem was the tendency of intelligence agencies to hoard information, as well as the cognitive difficulty of anticipating a spectacular and unprecedented attack. The 9/11 Commission called this a “failure of the imagination.” Finding needles, the commission wrote in its report, is easy when you’re looking backward, deceptively so. They quoted the historian Roberta Wohlstetter writing about Pearl Harbor: It is much easier *after* the event to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear; we can now see what disaster it was signaling since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meanings.

AT Provides sense of security

Mass surveillance creates a false sense of security

Matthatias Schwartz, January 26, 2015, The New Yorker, “The Whole Haystack,”
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

Before the event, every bit of hay is potentially relevant. “The most dangerous adversaries will be the ones who most successfully disguise their individual transactions to appear normal, reasonable, and legitimate,” Ted Senator, a data scientist who worked on an early post-9/11 program called Total Information Awareness, said, in 2002. Since then, intelligence officials have often referred to “lone-wolf terrorists,” “cells,” and, as Alexander has put it, the “terrorist who walks among us,” as though Al Qaeda were a fifth column, capable of camouflaging itself within civil society. Patrick Skinner, a former C.I.A. case officer who works with the Soufan Group, a security company, told me that this image is wrong. “We knew about these networks,” he said, speaking of the *Charlie Hebdo* attacks. Mass surveillance, he continued, “gives a false sense of security. It sounds great when you say you’re monitoring every phone call in the United States. You can put that in a PowerPoint. But, actually, you have no idea what’s going on.”

AT Not enough information

Information overload makes it harder to identify terrorists

Matthatias Schwartz, January 26, 2015, The New Yorker, "The Whole Haystack,"
<http://www.newyorker.com/magazine/2015/01/26/whole-haystack>, DOA: 1-23-15

By flooding the system with false positives, big-data approaches to counterterrorism might actually make it harder to identify real terrorists before they act. Two years before the Boston Marathon bombing, Tamerlan Tsarnaev, the older of the two brothers alleged to have committed the attack, was assessed by the city's Joint Terrorism Task Force. They determined that he was not a threat. This was one of about a thousand assessments that the Boston J.T.T.F. conducted that year, a number that had nearly doubled in the previous two years, according to the Boston F.B.I. As of 2013, the Justice Department has trained nearly three hundred thousand law-enforcement officers in how to file "suspicious-activity reports." In 2010, a central database held about three thousand of these reports; by 2012 it had grown to almost twenty-eight thousand. "The bigger haystack makes it harder to find the needle," Sensenbrenner told me. Thomas Drake, a former N.S.A. executive and whistle-blower who has become one of the agency's most vocal critics, told me, "If you target everything, there's no target." Drake favors what he calls "a traditional law-enforcement" approach to terrorism, gathering more intelligence on a smaller set of targets. Decisions about which targets matter, he said, should be driven by human expertise, not by a database.

Paris proves information overload makes it more difficult to catch terrorists

Dustin Volz, January 21, 2015, National Journal, "Snowden: France's 'Intrusive' Surveillance Failed to Stop Paris Attacks," <http://www.nationaljournal.com/tech/snowden-france-s-intrusive-surveillance-laws-failed-to-stop-paris-attacks-20150121> DOA: 1-25-15

Edward Snowden is pointing to the recent terrorist attacks in France as evidence that government mass-surveillance programs don't work because they are "burying people under too much data." "When we look at the Paris attacks specifically, we see that **France passed one of the most intrusive, expansive surveillance laws in all of Europe last year, and it didn't stop the attack,**" the fugitive leaker said in an interview with NOS, a Dutch news organization, released Wednesday. "**And this is consistent with what we've seen in every country."**

Mass surveillance collects too much data, creating "noise" that makes it difficult to detect actual threats

RT.com, May 2, 2014, <http://rt.com/usa/156536-hayden-greenwald-state-surveillance-debate/>

Greenwald went on to spar with Hayden and Dershowitz over whether the current method of metadata collection would have prevented the terrorist attacks on September 11, 2001.

Hayden argued that intelligence analysts would have noticed the number of calls from San Diego to the Middle East and caught the terrorists who were living inside the US illegally.

The problem, he said, was that when the NSA prevented the attack, they would still have to defend the surveillance program because as far as the public would be concerned, nothing went wrong.

But Greenwald stated that a number of experts have come forward to say that such a claim is not only false, but also offensive to the public. Lawrence Wright, the winner of a 2003 Pulitzer Prize for his Al-Qaeda coverage, wrote in the New Yorker earlier this year that one of the primary reasons US authorities failed to stop 9/11 is because they were taking in too much information to accurately sort through. The sheer data volume that such a method of surveillance has created is now threatening to ruin the very internet that so many people now rely upon. “*The gift and the curse of all that data, aside from the civil liberty violations, is that yeah there may be some signal but there’s a lot of noise,*” Ohanian said. **“It’s a very hard software problem to solve...through the efforts of this mass surveillance we’ve also undermined so much of the technology that makes the internet work, that keeps us safe. It threatens the technology of how the internet works, and works well.”** "Be it resolved state surveillance is a legitimate defence of our freedoms."

AT tech solves Overload

Tech can't solve – it's not fast enough

Horvitz, 13

Leslie Alan Horvitz, American author, “Information Overload: Babel, Borges and the NSA,” 7/2/13, [//IS](http://lesliehorvitz.com/blog/2013/7/2/information-overload-babel-borges-and-the-nsa)

NSA and other security agents rely on computers using a variety of algorithms (some of them designed to search for key words like ‘terrorism’) to find the hoped-for needles in the ever expanding haystack. But I suspect that technology is incapable of keeping up. The data threatens to become indigestible. As soon as you bring humans into the equation – and eventually you need analysts to assess the credibility of the information and determine whether it is actionable or not – you run the risk of errors, bad judgment and bias. And it takes time – lots of time. So analysts couldn’t get to them all; instead they put aside what used to be called “bit buckets” in the industry —electronic bits that someday would have to be sorted out...by someone. According to James Lewis, a cyberexpert quoted in The New York Times, “They park stuff in storage in the hopes that they will eventually have time to get to it,” although he admitted that “most of it sits and is never looked at by anyone.” As another expert put it: “This means that if you can’t desalinate all the seawater at once, you get to hold on to the ocean until you figure it out.”

Technology doesn't check mass surveillance inefficiencies

Ferguson, 1/16 (DAVID FERGUSON, journalist Raw Story, “Mass surveillance is ineffective at fighting terrorism and makes us less safe, says tech expert” 16 JAN 2015 AT 12:53 ET <http://www.rawstory.com/2015/01/mass-surveillance-is-ineffective-at-fighting-terrorism-and-makes-us-less-safe-says-tech-expert/>) //GY

Mass surveillance has proven to be an ineffective tool against terrorists, and yet in the wake of the attacks on the offices of the French satirical magazine Charlie Hebdo, many politicians are calling for even tighter surveillance on private citizens.¹ In a Thursday column for New Scientist, Open University technology specialist Ray Corrigan explained that mass electronic surveillance will never be an effective means of ensuring public safety, no matter how sophisticated the technology becomes or how granular a level at which officials become capable of examining our lives.¹ “Prime Minister David Cameron wants to reintroduce the so-called snoopers’ charter — properly, the Communications Data Bill — which would compel telecoms companies to keep records of all internet, email and cellphone activity,” wrote Corrigan. The Prime Minister also wants to ban all forms of encrypted communication like Apple iMessage and the message service WhatsApp.¹ However, Corrigan pointed out, “Brothers Said and Cherif Kouachi and Amedy Coulibaly, who murdered 17 people, were known to the French security services and considered a serious threat. France has blanket electronic surveillance. It didn’t avert what happened.”¹ In France, authorities lost track of the extremists just long enough for them to carry out their attack. Surveillance systems are imperfect, Corrigan said, and blanket data gathering is a wildly inefficient way to weed out potential terror suspects. It generates too much useless information to sift through, he said, and often misses vital information that only becomes clear in hindsight.¹ “You cannot fix any of this by treating the entire population as suspects and then engaging in suspicionless, blanket collection and processing of personal data,” he said. It simply doesn’t

work.[¶] In fact, the practice may make populations less safe by generating so much data that it becomes statistically impossible for investigators to spot actual leads, generating false positives at an astonishing rate. “Even if your magic terrorist-catching machine has a false positive rate of 1 in 1000 — and no security technology comes anywhere near this — every time you asked it for suspects in the UK it would flag 60,000 innocent people,” said Corrigan.[¶] “Surveillance of the entire population, the vast majority of whom are innocent, leads to the diversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle in a haystack problem. You don’t make it easier by throwing more needless hay on the stack.” he wrote.[¶] In the U.S., a series of revelations from intelligence contractor turned whistleblower Edward Snowden revealed programs through which the National Security Agency is gathering information on average citizens, outraging privacy advocates and opening an international debate on the legality of mass surveillance. Now, in addition to being legally dubious, years into the surveillance programs, the practice of indiscriminate data-gathering has neither caught any terrorists nor prevented any attacks. On Friday, the American Civil Liberties Union reported on the newly-released results of a year-long investigation by the National Academies: Bulk Collection of Signals Intelligence: Technical Operations 2015.[¶] Neema Singh Guliani of the ACLU revealed that the report showed “the domestic nationwide call detail record program has never stopped an act of terrorism or led to the identification of a terrorist suspect.”[¶] Furthermore, “the report did not find that the resource costs, privacy impacts, and economic harms associated with bulk collection are balanced by any concrete benefits in intelligence capabilities,” Guliani wrote.[¶] “Finally,” she said, “the report acknowledges that there are additional steps that the intelligence community can take to increase transparency, improve oversight, and limit the use of information collected through surveillance.”[¶] In his column, Corrigan wrote that law enforcement agencies need to “use modern digital technologies intelligently and through targeted data preservation — not a mass surveillance regime — to engage in court-supervised technological surveillance of individuals whom they have reasonable cause to suspect.”[¶] “That is not, however,” he insisted, “the same as building an infrastructure of mass surveillance.”

Technology can't check overload

The SIGINT Philosopher, 11

The SIGINT Philosopher, a Russian language analyst employed by SID, “The SIGINT Philosopher: Cognitive Overload?” 4/15/11,
<https://s3.amazonaws.com/s3.documentcloud.org/documents/2088972/cognitive-overflow.pdf> // IS

(U) There's a computer sitting atop your shoulders. Granted, real computers can apparently best human brains on Jeopardy with ease, but all the same... Since Noam Chomsky and his cohorts at MIT opened the floodgates to the study of how we think, cognitive psychology has come a long way. Although the ensuing decades of research have highlighted the astounding capabilities of our gray matter, the field has also exposed the limitations our brains are subject to. It may be worth considering the implications these limitations have for our work in SID.

(U) “Channel capacity” is the term some cognitive psychologists have begun to apply to the brain’s limits on the amount of certain information it can retain. For instance, research shows that the average person can only differentiate between 5-9 different tones, shapes, or textures at a given time. Any more, and our capacity to categorize becomes overtaxed, and we begin to make

mistakes. In other words, the servers overload. It is yet another example of how unprepared humans are, in evolutionary terms, for the information age. Evolutionary biologist Sherwood Washburn once wrote:

(U) "Most of human evolution took place before the advent of agriculture, when we lived in small groups, face-to-face. Man evolved to feel strongly about few people, short distances, and relatively brief intervals."

(U) The question then becomes: If an individual brain has finite "channel capacity," does the vast collective of SID, comprised of thousands of brilliant, yet limited, brains also have a definite "channel capacity"? If so, what is it? How do we know when we've reached it? What if we've already exceeded it? In essence, could SID's reach exceed its grasp? Can the combined cognitive power of SID connect all the necessary dots to avoid, predict, or advise when the improbable, complex, or unthinkable happens?

(U) Take for example the number of tools, clearances, systems, compliances, and administrative requirements we encounter before we even begin to engage in the work of the mission itself. The mission then involves an ever-expanding set of complex issues, targets, accesses, and capabilities. The "cognitive burden," so to speak, must at times feel overwhelming to some of us. The SID is an organism with many moving parts. So how do we ensure our SIGINT potential is in line with, and doesn't overwhelm our collective cognitive capacity? Can we count on our overarching SID mechanism to self-regulate, to organically cull, sort, and retain? Or is there perhaps something extra we ought to be doing to ensure we operate at full exploitative and analytic force?

(U) Surely someone will point out that the burgeoning amalgam of technological advances will aid us in shouldering the burden. However, historically, this scenario doesn't seem to completely bear out. The onslaught of more computing power—often intended to automate some processes—has in many respects demanded an expansion of our combined "channel capacity," rather than curbing the flow of the information that's necessary to retain.

(U) It's an issue worth thinking about and discussing. In the meantime, I'll be working on my 14-character password...

(U) Editor's note: See a Tapioca Pebble on this topic.

AT more data solves

More data can't solve – current spending and Britain prove Maass, 15

Peter Maass, a Guggenheim Fellow on the advisory boards of the Solutions Journalism Network, and the Program for Narrative and Documentary Practice at Tufts University, “Inside NSA, Officials Privately Criticize ‘Collect it All’ Surveillance,” The Intercept, 5/28/15, <https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/> // IS

The agency appears to be spending significant sums of money to solve the haystack problem. The document headlined “Dealing With a ‘Tsunami’ of Intercept,” written in 2006 by three NSA officials and previously published by The Intercept, outlined a series of programs to prepare for a near future in which the speed and volume of signals intelligence would explode “almost beyond imagination.” The document referred to a mysterious NSA entity—the “Coping With Information Overload Office.” This appears to be related to an item in the Intelligence Community’s 2013 Budget Justification to Congress, known as the “black budget”—\$48.6 million for projects related to “Coping with Information Overload.” The data glut is felt in the NSA’s partner agency in Britain, too. A slideshow entitled “A Short Introduction to SIGINT,” from GCHQ, the British intelligence agency, posed the following question: “How are people supposed to keep on top of all their targets and the new ones when they have far more than [they] could do in a day? How are they supposed to find the needle in the haystack and prioritise what is most important to look at?” The slideshow continued, “Give an analyst three leads, one of which is interesting: they may have time to follow that up. Give them three hundred leads, ten of which are interesting: that’s probably not much use.”

More data fails – statistics – and their evidence is hype Bergen et al., 14

Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahill, *Peter Bergen is an American print and broadcast journalist, author, documentary producer, and CNN's national security analyst. **David Sterman is a program associate at New America and holds a master's degree from Georgetown's Center for Security Studies, ***senior program associate for the International Security Program at New America, “Do Nsa's Bulk Surveillance Programs Stop Terrorists?” New America Foundation, January 2014, https://www.newamerica.org/downloads/IS_NSA_surveillance.pdf // IS

D. The administration has repeatedly exaggerated the role of NSA bulk surveillance programs in preventing terrorism and is misleading the public when it says that 9/11 could have been prevented by such programs when, in fact, better information-sharing about already existing intelligence would have been far more effective in preventing 9/11.

Members of Congress, senior government officials, and NSA officials have justified the programs with statements about how many terrorist events the surveillance programs have foiled - citing a total of 54 “events” around the globe, of which 13 were in the United States - and have warned of the risk of a future 9/11-like attack if the programs were curtailed. As mentioned above, President Obama defended the NSA surveillance programs during a visit to Berlin in June, saying: “We know of at least 50 threats that have been averted because of this information not just in the

United States, but, in some cases, threats here in Germany. So lives have been saved.”³⁹ Gen. Alexander testified before Congress that: “the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world.”⁴⁰ Rep. Mike Rogers, chairman of the House Permanent Select Committee on Intelligence, said on the chamber floor in July that NSA programs “stopped and thwarted terrorist attacks both here and in Europe - saving real lives” a total of 54 times.⁴¹

The government’s defense has demonstrated a lack of precision regarding the exact nature of the threats in the terrorism cases the government has claimed were prevented by NSA surveillance. Were they real attacks that were thwarted? Serious plots that were still somewhere in the planning stages? Plots that were concerning, but never really operational? Or did they involve some sort of terrorism-support activity, such as fundraising? President Obama has called them “threats,” Gen. Alexander called them “events” and then later used the term “activities,” while Rep. Rogers and one of Gen. Alexander’s slides at the 2013 Black Hat conference referred to them as “attacks.”⁴²

Sen. Leahy brought attention to this disconnect at a Senate Judiciary Committee hearing in July 2013, saying he had been shown a classified list of “terrorist events” detected through surveillance which did not show that “dozens or even several terrorist plots” had been thwarted by the collection of American telephone metadata under Section 215.⁴³ Sen. Leahy asked Gen. Alexander: “Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S.?” and Gen. Alexander’s reply was a simple “Yes.”⁴⁴ On this key point, beyond his one-word answer, the NSA director did not elaborate while under oath.

Leading reporters have sometimes simply parroted the government claims that more than 50 attacks have been averted. Bob Schieffer of CBS News, for instance, said on “Face the Nation” on July 28: “Fifty-six terror plots here and abroad have been thwarted by the NASA [sic] program. So what’s wrong with it, then, if it’s managed to stop 56 terrorist attacks? That sounds like a pretty good record.”⁴⁵ This misrepresentation in the media most likely stems from confusion about what this oft-cited 54 number really refers to - terrorist activity such as fundraising, plots that were really only notional, or actual averted attacks.

Despite the government’s narrative that NSA surveillance of some kind prevented 13 domestic “events” or “attacks” in the United States, of the eight cases we have identified as possibly involving the NSA, including the three the government has not claimed, only one can be said to involve an operational al-Qaeda plot to conduct an attack within the United States, three were notional plots, and one involved an attack plan in Europe. And in three of the plots we identified as possibly having been prevented by the NSA - Moalin, Muhtorov and Jumaev, and Warsame - the defendants were committing or allegedly committing crimes of support for a terrorist group, rather than plotting terrorist attacks.

More data fails – empirics

Bergen et al., 14

Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahill, *Peter Bergen is an American print and broadcast journalist, author, documentary producer, and CNN's national security analyst. **David Sterman is a program associate at New America and holds a master's degree

from Georgetown's Center for Security Studies, ***senior program associate for the International Security Program at New America, "Do Nsa's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014,
https://www.newamerica.org/downloads/IS_NSA_surveillance.pdf // IS

These multiple missed opportunities challenge the administration's claims that the NSA's bulk surveillance program could have prevented the 9/11 attacks. The key problem was one of information-sharing, not lack of information. If information-sharing had been functioning, Mihdhar would likely have been caught regardless of the collection of telephone metadata, and if information- sharing was not functioning, it is unclear why collecting more information would have changed the result. Even if Mihdhar's phone calls from San Diego to Yemen is considered a moment for preventing the 9/11 attacks, it is likely that more targeted surveillance of that phone number rather than bulk collection of metadata would have been sufficient. Communications to and from the house in Yemen were already being intercepted by the NSA as a result of investigations into the 1998 U.S. embassy bombings in Africa and the USS Cole bombing in 2000.⁶² According to U.S. officials quoted by Josh Meyer, a leading national security reporter at the Los Angeles Times, the information from the calls could have been shared through a FISA warrant under the authorities the NSA had even before 9/11.⁶³ The United States government could and should have been alerted to Mihdhar's phone calls even without the expanded authority to collect the telephone metadata of all Americans under Section 215. Indeed, Richard Clarke, the national coordinator for security, infrastructure protection, and counterterrorism from 1998 to 2001, has explained that the Justice Department "could have asked the FISA Court for a warrant to all phone companies to show all calls from the U.S. which went to the Yemen number. As far as I know, they did not do so. They could have."⁶⁴ Clarke played down the need for bulk collection in such a scenario, continuing, "My understanding is that they did not need the current All Calls Data Base FISA warrant to get the information they needed. Since they had one end of the calls (the Yemen number), all they had to do was ask for any call connecting to it."⁶⁵ (Clarke was one of the five members of the White House review group that President Obama established in August 2013 to review the U.S. government's surveillance activities and which issued its report on December 18, 2013). The overall problem for U.S. counterterrorism officials is not that they need the information from the bulk collection of phone data, but that they don't sufficiently understand or widely share the information they already possess that is derived from conventional law enforcement and intelligence techniques. This was true of the two 9/11 hijackers living in San Diego and it is also the unfortunate pattern we have seen in several other significant terrorism cases: • Chicago resident David Coleman Headley was central to the planning of the 2008 terrorist attacks in **Mumbai** that killed 166 people. Yet, following the 9/11 attacks, U.S. authorities received plausible tips regarding Headley's associations with militant groups at least five times from his family members, friends, and acquaintances.⁶⁶ These multiple tips were never followed up in an effective fashion. • Maj. Nidal Hasan, a U.S. Army psychiatrist, killed 13 people at **Fort Hood**, Texas, in 2009. Before the attack, U.S. intelligence agencies had intercepted multiple emails between Maj. Hasan and Anwar al-Awlaki, a U.S.- born cleric living in Yemen who was notorious for his ties to militants. The emails included a discussion of the permissibility in Islam of killing U.S. soldiers. Counterterrorism investigators didn't follow up on these emails, believing that they were somehow consistent with Maj. Hasan's job as a military psychiatrist.⁶⁷ • Carlos Bledsoe, a convert to Islam, fatally shot a soldier at a **Little Rock**, Ark., military recruiting office in 2009, several months after returning from a stay in Yemen. As a result of that trip, Bledsoe was under investigation by the FBI. Yet, he was still able to buy the

weapons for his deadly attack when he was back in the United States.⁶⁸ • Nigerian Umar Farouq Abdulmutallab attempted to blow up Northwest Flight 253 over Detroit on Christmas Day 2009 with an “underwear bomb.” Fortunately, the bomb failed to explode. Yet, a few weeks before the botched attack, Abdulmutallab’s father contacted the U.S. Embassy in Nigeria with concerns that his son had become radicalized and might be planning something.⁶⁹ This information wasn’t further investigated. Abdulmutallab had been recruited by al-Qaeda’s branch in Yemen for the mission. The White House review of the bomb plot concluded that there was sufficient information known to the U.S. government to determine that Abdulmutallab was likely working for al-Qaeda in Yemen and that the group was looking to expand its attacks beyond Yemen.⁷⁰ Yet, Abdulmutallab was allowed to board a plane bound for the United States without any question. All of the missed opportunities in these serious terrorism cases argue not for the gathering of ever-more vast troves of information, but simply for a better understanding of the information the government has already collected that was derived from conventional law enforcement and intelligence methods.

Network and pattern identification fails Keefe, 6

(Patrick Radden, Century Foundation fellow, author of 'Chatter: Dispatches from the Secret World of Global Eavesdropping', 3-12-2006, New York Times, "Can Network Theory Thwart Terrorists?", lexis, amp)

Network academics caution that the field is still in its infancy and should not be regarded as a panacea. Duncan Watts of Columbia University points out that it's much easier to trace a network when you can already identify some of its members. But much social-network research involves simply trawling large databases for telltale behaviors or activities that might be typical of a terrorist. In this case the links among people are not based on actual relationships at all, but on an "affiliation network," in which individuals are connected by virtue of taking part in a similar activity. This sort of approach has been effective for corporations in detecting fraud. A credit-card company knows that when someone uses a card to purchase \$2 of gas at a gas station, and then 20 minutes later makes an expensive purchase at an electronics store, there's a high probability that the card has been stolen. Marc Sageman, a former C.I.A. case officer who wrote a book on terror networks, notes that correlating certain signature behaviors could be one way of tracking terrorists: jihadist groups in Virginia and Australia exercised at paint-ball courses, so analysts could look for Muslim militants who play paint ball, he suggests. But whereas there is a long history of signature behaviors that indicate fraud, jihadis terror networks are a relatively new phenomena and offer fewer reliable patterns.

There is also some doubt that identifying hubs will do much good. Networks are by their very nature robust and resistant to attack. After all, while numerous high ranking Qaeda leaders have been captured or killed in the years since Sept. 11, the network still appears to be functioning. "If you shoot the C.E.O., they'll hire another one," Duncan Watts says. "The job will still get done."

AT Congress Checks Overload

Congress can't check overload Shoemaker, 15

Tim Shoemaker, the Director of Legislation at Campaign for Liberty. He graduated Magna Cum Laude with a Bachelor of Arts from Indiana University of Pennsylvania. "Can Congress Effectively Oversee the Vast Surveillance State," Campaign for Liberty, 4/8/15, <http://www.campaignforliberty.org/can-congress-effectively-oversee-vast-surveillance-state> // IS

According to a new report from the Associated Press, the Senate Intelligence Committee is creating a sort of "secret encyclopedia" of America's surveillance programs.

Surprisingly, this hasn't picked up as much media attention as it should.

What the report actually tells us, without directly saying so, is Congress isn't capable of conducting informed, effective oversight of the surveillance state.

Despite calling Snowden's actions "treason" at the time, it's clear that Feinstein and other members of Congress were completely unaware of the foreign surveillance being conducted under Executive Order 12333 -- and would never have learned of the programs being carried out by a small number of Executive Branch employees without his whistleblowing activities.

Of course, what ought to upset us all is how the Intel Committee members HAD been briefed on some of the most controversial intelligence programs such as the surveillance of American's phone records and the PRISM program and other than Ron Wyden and Mark Udall, none of them seemed to be overly concerned about how Americans' civil liberties were being routinely violated.

AT CIA

CIA mass surveillance fails

Fingas, 4/25 (Jon Fingas, Associate Editor Engadget “The CIA couldn't properly use a mass surveillance program for years” April 25th 2015 <http://www.engadget.com/2015/04/25/cia-mass-surveillance-problems/>) //GY

Whatever you think about the morality of using mass surveillance to catch evildoers, the technology only works if people can use it -- just ask the CIA. The New York Times has obtained a declassified report revealing that that the agency was largely kept in the dark about the President's Surveillance Program (aka Stellarwind), which allows for bulk data collection, until at least 2009. Only the highest-ranking officials could use PSP as a general rule, and those few agents that did have access often didn't know enough to use it properly, faced "competing priorities" or had other tools at their disposal. To boot, there wasn't documentation showing how effective the program was in fighting terrorism. It's not certain if the CIA has shaped up in the years since that report, although its shift toward online operations is going to make these kinds of digital initiatives more important. Regardless of any improvements, it's clearer than ever that the US government has sometimes had private doubts about the effectiveness of its large-scale surveillance efforts.

Mass surveillance can't find terrorists – mathematically impossible

Rudmin, '06 (FLOYD RUDMIN Professor of Social & Community Psychology at the University of Tromsø in Norway “Why Does the NSA Engage in Mass Surveillance of Americans When It's Statistically Impossible for Such Spying to Detect Terrorists?” MAY 24, 2006 <http://www.counterpunch.org/2006/05/24/why-does-the-nsa-engage-in-mass-surveillance-of-americans-when-it-s-statistically-impossible-for-such-spying-to-detect-terrorists/>) //GY

The Bush administration and the National Security Agency (NSA) have been secretly monitoring the email messages and phone calls of all Americans. They are doing this, they say, for our own good. To find terrorists. Many people have criticized NSA's domestic spying as unlawful invasion of privacy, as search without search warrant, as abuse of power, as misuse of the NSA's resources, as unconstitutional, as something the communists would do, something very unAmerican. In addition, however, mass surveillance of an entire population cannot find terrorists. It is a probabilistic impossibility. It cannot work. What is the probability that people are terrorists given that NSA's mass surveillance identifies them as terrorists? If the probability is zero ($p=0.00$), then they certainly are not terrorists, and NSA was wasting resources and damaging the lives of innocent citizens. If the probability is one ($p=1.00$), then they definitely are terrorists, and NSA has saved the day. If the probability is fifty-fifty ($p=0.50$), that is the same as guessing the flip of a coin. The conditional probability that people are terrorists given that the NSA surveillance system says they are, that had better be very near to one ($p \approx 1.00$) and very far from zero ($p=0.00$). The mathematics of conditional probability were figured out by the Scottish logician Thomas Bayes. If you Google "Bayes' Theorem", you will get more than a million hits. Bayes' Theorem is taught in all elementary statistics classes. Everyone at NSA certainly knows Bayes' Theorem. To know if mass surveillance will work, Bayes' theorem requires three estimations:¹ 1) The base-rate for terrorists, i.e. what proportion of the population are terrorists.² 2) The accuracy rate, i.e., the probability that real terrorists will be identified by NSA;³ 3) The misidentification rate, i.e., the probability that innocent citizens will be misidentified by NSA as terrorists.⁴ No matter how sophisticated and super-duper are NSA's methods for identifying

terrorists, no matter how big and fast are NSA's computers, NSA's accuracy rate will never be 100% and their misidentification rate will never be 0%. That fact, plus the extremely low base-rate for terrorists, means it is logically impossible for mass surveillance to be an effective way to find terrorists.¹ I will not put Bayes' computational formula here. It is available in all elementary statistics books and is on the web should any readers be interested. But I will compute some conditional probabilities that people are terrorists given that NSA's system of mass surveillance identifies them to be terrorists.² The US Census shows that there are about 300 million people living in the USA.³ Suppose that there are 1,000 terrorists there as well, which is probably a high estimate. The base-rate would be 1 terrorist per 300,000 people. In percentages, that is .00033% which is way less than 1%. Suppose that NSA surveillance has an accuracy rate of .40, which means that 40% of real terrorists in the USA will be identified by NSA's monitoring of everyone's email and phone calls. This is probably a high estimate, considering that terrorists are doing their best to avoid detection. There is no evidence thus far that NSA has been so successful at finding terrorists. And suppose NSA's misidentification rate is .0001, which means that .01% of innocent people will be misidentified as terrorists, at least until they are investigated, detained and interrogated. Note that .01% of the US population is 30,000 people. With these suppositions, then the probability that people are terrorists given that NSA's system of surveillance identifies them as terrorists is only $p=0.0132$, which is near zero, very far from one. Ergo, NSA's surveillance system is useless for finding terrorists.⁴ Suppose that NSA's system is more accurate than .40, let's say, .70, which means that 70% of terrorists in the USA will be found by mass monitoring of phone calls and email messages. Then, by Bayes' Theorem, the probability that a person is a terrorist if targeted by NSA is still only $p=0.0228$, which is near zero, far from one, and useless.⁵ Suppose that NSA's system is really, really, really good, really, really good, with an accuracy rate of .90, and a misidentification rate of .00001, which means that only 3,000 innocent people are misidentified as terrorists. With these suppositions, then the probability that people are terrorists given that NSA's system of surveillance identifies them as terrorists is only $p=0.2308$, which is far from one and well below flipping a coin. NSA's domestic monitoring of everyone's email and phone calls is useless for finding terrorists.⁶ NSA knows this. Bayes' Theorem is elementary common knowledge. So, why does NSA spy on Americans knowing it's not possible to find terrorists that way? Mass surveillance of the entire population is logically sensible only if there is a higher base-rate. Higher base-rates arise from two lines of thought, neither of them very nice:⁷ 1) McCarthy-type national paranoia; 2) political espionage.⁸ The whole NSA domestic spying program will seem to work well, will seem logical and possible, if you are paranoid. Instead of presuming there are 1,000 terrorists in the USA, presume there are 1 million terrorists. Americans have gone paranoid before, for example, during the McCarthyism era of the 1950s. Imagining a million terrorists in America puts the base-rate at .00333, and now the probability that a person is a terrorist given that NSA's system identifies them is $p=.99$, which is near certainty. But only if you are paranoid. If NSA's surveillance requires a presumption of a million terrorists, and if in fact there are only 100 or only 10, then a lot of innocent people are going to be misidentified and confidently mislabeled as terrorists.⁹ The ratio of real terrorists to innocent people in the prison camps of Guantanamo, Abu Ghraib, and Kandahar shows that the US is paranoid and is not bothered by mistaken identifications of innocent people. The ratio of real terrorists to innocent people on Bush's no-fly lists shows that the Bush administration is not bothered by mistaken identifications of innocent Americans.¹⁰ Also, mass surveillance of the entire population is logically plausible if NSA's domestic spying is not looking for terrorists, but looking for something else, something that is not so rare as terrorists.¹¹ For example, the May 19 Fox News opinion poll of 900 registered voters found that 30% dislike the Bush administration so

much they want him impeached. If NSA were monitoring email and phone calls to identify pro-impeachment people, and if the accuracy rate were .90 and the error rate were .01, then the probability that people are pro-impeachment given that NSA surveillance system identified them as such, would be $p=0.98$, which is coming close to certainty ($p \approx 1.00$). Mass surveillance by NSA of all Americans' phone calls and emails would be very effective for domestic political intelligence.But finding a few terrorists by mass surveillance of the phone calls and email messages of 300 million Americans is mathematically impossible, and NSA certainly knows that.

Effectiveness of mass surveillance is massively overblown – hasn't aided a single case

Bergen et al, PhD, '14 (Bailey Cahall David Sterman Emily Schneider Peter Bergen, member of the Homeland Security Project, a successor to the 9/11 Commission a Professor of Practice at Arizona State University and a fellow at Fordham University's Center on National Security "DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS?" JANUARY 13, 2014 <https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/>) //GY

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it's unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government's investigations of these cases: <http://natsec.newamerica.net/nsa/analysis>).Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided \$8,500 to al-Shabaab, al-Qaeda's affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to "connect the dots" faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after

using the NSA's phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it's unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin's calls, despite official statements that the bureau had Moalin's phone number and had identified him. This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues. Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange. In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used. We have also identified three additional plots that the government has not publicly claimed as NSA successes, but in which court records and public reporting suggest the NSA had a role. However, it is not clear whether any of those three cases involved bulk surveillance programs. Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

Surveillance can't solve – their authors inflate data

Nicks, '14 (Denver Nicks, TIME, "Report: Usefulness of NSA Mass Surveillance 'Overblown'" Jan. 13, 2014 <http://swampland.time.com/2014/01/13/report-usefulness-of-nsa-mass-surveillance-overblown/>) //GY

Ever since Edward Snowden's leaks began revealing the extent of the National Security Agency's mass surveillance—or "bulk collection"—programs last June, officials have defended the programs with one number: 50. "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved," President Obama said on a visit to Berlin. NSA Director Gen. Keith Alexander made the same claim testifying before Congress. But a new study out Monday from The New America Foundation says that claim is simply false, calling it "overblown, and even misleading." "Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group," says the nonpartisan think tank's report, titled "Do NSA's Bulk Surveillance Programs Stop Terrorists?" In an analysis of 225 al-Qaeda-linked

individuals charged with terrorism in the U.S. since 9/11, the report found NSA mass surveillance of Americans telephone records—authorized under Section 215 of the USA PATRIOT Act—“played an identifiable role in initiating, at most, 1.8 percent” of investigations. The report acknowledges that in 28 percent of cases it reviewed, researchers couldn’t determine what methods initiated the investigation. But in many of those cases an informant played a role in the investigation, says the report.⁴ ACLU Legislative Counsel Michelle Richardson told TIME the report “confirms that the numbers and examples the government has floated in support of its domestic spying programs are grossly inflated. More broadly though, it underlines how far the government has actually gotten away from the original lessons of 9/11. Instead of working on connecting the dots collected from traditional investigations, it has become obsessed with collecting ever more data whether it is useful or not.”

Surveillance can't solve – their authors are lying

Terbush, '13 (Jon Terbush, correspondent The Week, “Is the NSA's data snooping actually effective?” December 19, 2013 <http://theweek.com/articles/453981/nsas-data-snooping-actually-effective>) //GY

The White House on Wednesday released a much-anticipated independent review of the National Security Agency's spy programs, which offered 46 recommendations for reforming the agency's spy ops.⁵ The report concluded that the programs, though they had gone too far, should stay in place. But it nevertheless may have undermined the NSA's claim that the collection of all phone metadata is a necessary tool to combat terrorism.⁶ "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders," the report said.⁷ That finding came just days after a federal judge ruled that the phone data collection program was "likely unconstitutional." Moreover, he wrote in his decision that, for all the government's bluster, there was no indication the program had actually produced tangible results.⁸ "The government does not cite a single case in which analysis of the NSA's bulk metadata collection actually stopped an imminent terrorist attack," Judge Richard Leon wrote.⁹ Given the limited record before me at this point in the litigation — most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics — I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism. [PDF]¹⁰ Granted, the collection of phone data is just one of the NSA's many once-secret tools. And unsurprisingly, the White House, hawkish lawmakers, and those who oversee the spy programs have repeatedly claimed that the NSA's programs in their entirety have proven crucial to snuffing out terror plots.¹¹ Shortly after whistleblower Edward Snowden's leaks turned up in the press, NSA Director Gen. Keith Alexander defended his agency's surveillance practices before the Senate. The surveillance programs, he said, had stopped dozens of attacks at home and abroad, including a 2009 plot to bomb the New York City subway system.¹² Obama, too, said back in June that the programs had thwarted "at least 50" possible attacks. (He and others often cite 54 as an exact number.) He also defended the tradeoff of civil liberties for security as a necessary one — "we have to make choices as a society" — adding that the programs were merely "modest encroachments on privacy."¹³ However, two prominent critics of the NSA, Democratic Sens. Ron Wyden (Ore.) and Mark Udall (Colo.), challenged that assessment in a joint statement following Alexander's testimony.¹⁴ "We have not yet seen any evidence showing that the NSA's dragnet collection of Americans' phone records has produced any uniquely valuable intelligence." they wrote.¹⁵

Alexander had only specified a couple of the supposed "dozens" of instances in which NSA spying thwarted terror plots. The two senators added in a subsequent statement that it appeared the government had actually uncovered those plots via other investigative tools, and that the NSA's data snooping had "played little or no role in most of these disruptions." A ProPublica investigation earlier this year likewise determined that there was "no evidence that the oft-cited figure [of 54 disrupted plots] is accurate," and that the NSA was often "inconsistent on how many plots it has helped prevent and what role the surveillance programs played." It's pretty much impossible to say who's right with any certainty. A full explanation of the supposedly disrupted plots remains classified, so only some lawmakers and those involved in the programs know exactly how effective they've been. Still, it's likely that the NSA has at least overstated the effectiveness of its tools, particularly in comparison to the sheer scale of the spying. Sen. Patrick Leahy (D-Vt.), after reviewing the full classified list of thwarted plots, concluded the programs had "value," but that the 54 figure was a gross exaggeration. "That's plainly wrong," he said at a July hearing. "These weren't all plots and they weren't all thwarted."

Surveillance doesn't work – can't combat terror

Tufnell, Wired, '14 (NICHOLAS TUFNELL, Wired, "NSA bulk surveillance has 'no discernible impact' on the prevention of terrorism" 14 JANUARY 14

<http://www.wired.co.uk/news/archive/2014-01/14/naf-report-on-nsa> //GY

The New America Foundation (NAF) has released a damning report claiming the NSA's mass surveillance programme has "no discernible impact" on the prevention of terrorism. The report, "Do NSA's Bulk Surveillance Programs Stop Terrorists?", also claims that the NSA is guilty of repeatedly exaggerating the efficacy of its bulk surveillance techniques in addition to misleading the public over aspects of 9/11, and of failing to prevent crime efficiently due to an insufficient understanding of its own intelligence already sourced by traditional means. The NAF describes itself as a non-profit, nonpartisan public policy institute and think tank focussing on a wide range of issues, including national security studies. Investigating claims made by the US government concerning the competence and effectiveness of the NSA's bulk surveillance since 9/11, the NAF report compiled a database of 225 people from the US, including US nationals abroad, who have been indicted, convicted, or killed since the 9/11 terror attacks. Key methods used to initiate investigations on these individuals were identified by the report and divided into eight separate categories: "Those cases in which the initiating or key role was played by the bulk collection of American telephone metadata under Section 215; NSA surveillance of non-US persons overseas under Section 702; NSA surveillance under an unknown authority; tips from the extremist's family or local community members; tips regarding suspicious activity from individuals who were not part of an extremist's family or local community; the use of an undercover informant; the routine conduct of law enforcement or intelligence operations in which the NSA did not play a key role; and self-disclosure of extremist activity on the part of the extremist in question." The report also acknowledges that the public records from which it drew the information may be incomplete and that there is reason to believe the government has actively concealed the role of NSA programmes in some investigations: "Drug Enforcement Administration (DEA) agents have been trained in some instances, for example, to conceal the role of a DEA unit that analysed metadata to initiate cases." The bulk collection of US citizens' telephone metadata -- which includes phone numbers, both incoming and outgoing, as well as the exact time, date and duration of the calls (but not the content) under Section 215 of the US Patriot Act -- accounts for having aided only 1.8 percent of the NSA's terrorist cases. An equally unimpressive 4.4 percent of terrorism cases were aided by the NSA's surveillance of non-US persons outside of the United

States under Section 702 of the FISA Amendments Act.⁴ Commenting on these figures the report states, "Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist related activity, such as fundraising for a terrorist group."⁵ Of the terrorist plot regularly cited by the US government as evidence of the necessity and success of its surveillance techniques -- namely, Basaaly Moalin, a San Diego taxi driver who provided \$8,500 (£5,171) to an al-Qaeda affiliate in Somalia -- the NAF report states that the NSA's actions contradict its claims that the expediency afforded by Section 215 was largely responsible for the success of Moalin's capture.⁶ According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to 'connect the dots' faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA's phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone.⁷ The reasons behind the two-month delay -- during which time the FBI was not monitoring Moalin's calls, despite being aware of his number and identity -- are still unclear. What is clear, however, is that the bulk surveillance programme did not expedite the investigative process, despite the US government's claims to the contrary.⁸ The report also reviewed three key terrorism cases frequently cited by the US government in defence of the NSA's bulk surveillance. It concluded that government officials exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi. The significance of the threat of Zazi, who planned to bomb the New York Stock Exchange, was also exaggerated, claims the report.⁹ More emphasis, the report suggests, should be placed on conventional forms of law enforcement, which are demonstrably more efficient. "The overall problem for US counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques."

Can't solve – studies and Snowden

Osterndorf, 3/17 (Chris Osterndorf, writer Daily Dot, "Edward Snowden is right—NSA surveillance won't stop terrorism" Mar 17, 2015 <http://www.dailycdot.com/opinion/edward-snowden-mass-surveillance-nsa-america/>) //GY

It appears that Snowden season is approaching once again.¹⁰ The controversial whistleblower made a surprise appearance via Google Hangout at SXSW this week, where his remarks proved captivating as always. Essentially a less flashy sequel to his ACLU speech from 2014, Snowden only spoke to a few people this time around, engaging in a conversation with a select group of leaders from America's tech sector. In particular, he urged tech companies to become "champions of privacy," suggesting that they use their power to help shield Americans from an increasingly watchful government.¹¹ In addition to speaking at SXSW in Austin, Snowden also said a few words at FutureFest in London, where he warned that massive surveillance won't stop terrorism.¹² In this instance, Snowden is absolutely correct, and it's time we start heeding his advice.¹³ At this point, the only people clinging to this idea is an effective is the NSA themselves. In 2013, NSA Director Gen. Keith Alexander went before the House Intelligence Committee to testify to claim that increased surveillance had helped to stop terrorist threats over 50 times since 9/11, including attacks on U.S. soil such as a plot to blow up the New York Stock Exchange and a defunct scheme to fund an overseas terrorist group.¹⁴ Other witnesses in the same hearing also suggested that the Snowden leaks had harmed America greatly. "We are now faced with a situation that because this information has been made public, we run the risk of losing these collection

capabilities,” stated Robert S. Litt, general counsel of the Office of the Director of National Intelligence. “We’re not going to know for many months whether these leaks in fact have caused us to lose these capabilities, but if they do have that effect, there is no doubt that they will cause our national security to be affected.” However, the details the NSA provided in this hearing were somewhat hazy, and a closer look at the numbers indicates the benefits of increased surveillance may not be so clear-cut after all. Research from International Security found that out of the 269 terrorist suspects apprehended since 9/11, 158 were brought in through the use of traditional investigative measures. That’s almost 60 percent of all who were arrested. Meanwhile, 78 suspects were apprehended through measures which were “unclear” and 15 were implicated in plots but were not apprehended, while the remaining 18 were apprehended by some form of NSA surveillance. Eighteen is no small number when you’re discussing matters of national security; however, the above statistics do not necessarily indicate that mass surveillance was responsible for the apprehension of these 18 terrorists or whether these suspects were detained under more traditional surveillance measures. Moreover, the evidence suggests that traditional means of combatting terrorism are more effective than surveillance when it comes to overall arrests.

Additional analysis from the New America Foundation further supports these findings.

Examining 225 post-9/11 terrorism cases in the U.S., their 2014 report found that the NSA’s bulk surveillance program “has had no discernible impact on preventing acts of terrorism,” citing traditional methods of law enforcement and investigation as being far more effective in the majority of cases. In as many as 48 of these cases, traditional surveillance warrants were used to collect evidence, while more than half of the cases were the product of other traditional investigative actions, such as informants and reports of suspicious activity. In fact, New America determined that the NSA has only been responsible for 7.5 percent of all counterterrorism investigations and that only one of those investigations led to suspects being convicted based on metadata collection. And that case, which took months to solve, as the NSA went back and forth with the FBI, involved money being sent to a terrorist group in Somalia, rather than an active plan to perpetrate an attack on U.S. soil. According to the report’s principal author Peter Bergen, who is the director of the foundation’s National Security Program and their resident terrorism expert, the issue has less to do with the collection of data and more to do with the comprehension of it. Bergen said, “The overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don’t sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques.” Of course, even when all of the data has been collected, it still isn’t enough to stop a terrorist attack. “It’s worth remembering that the mass surveillance programs initiated by the U.S. government after the 9/11 attacks—the legal ones and the constitutionally dubious ones—were premised on the belief that bin Laden’s hijacker-terrorists were able to pull off the attacks because of a failure to collect enough data,” asserts Reason’s Patrick Eddington. “Yet in their subsequent reports on the attacks, the Congressional Joint Inquiry (2002) and the 9/11 Commission found exactly the opposite. The data to detect (and thus foil) the plots was in the U.S. government’s hands prior to the attacks; the failures were ones of sharing, analysis, and dissemination.” So once again, we see that the key is not collection, but comprehension. If all of this still doesn’t seem like enough evidence that mass surveillance is ineffective, consider that a White House review group has also admitted the NSA’s counterterrorism program “was not essential to preventing attacks” and that a large portion of the evidence that was collected “could readily have been obtained in a timely manner using conventional [court] orders.” But mass surveillance isn’t just the United States’ problem. Research has shown that Canada’s Levitation project, which also involves collecting large

amounts of data in the service of fighting terrorism, may be just as questionable as the NSA's own data collection practices. Meanwhile, in response to the Charlie Hebdo attacks in Paris, British Prime Minister David Cameron has reintroduced the Communications Data Bill, which would force telecom companies to keep track of all Internet, email, and cellphone activity and ban encrypted communication services. ¶ But support for this type of legislation in Europe doesn't appear to be any stronger than in North America. Slate's Ray Corrigan argued, "Even if your magic terrorist-catching machine has a false positive rate of 1 in 1,000—and no security technology comes anywhere near this—every time you asked it for suspects in the U.K., it would flag 60,000 innocent people." ¶ Fortunately, the cultural shift against increased data collection has become so evident in the U.S. that even President Obama is trying to get out of the business of mass surveillance; the president announced plans last March to reform the National Security Agency's practice of collecting call records, which have yet to come to fruition. ¶ Benjamin Franklin famously said that "those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety." While this quote has been notoriously butchered and misinterpreted over the years, it has now become evident that we shouldn't have to give up either of these things in pursuit of the other. The U.S. is still grappling with how to fight terrorism in this technologically advanced age, but just because we have additional technology at our disposal, doesn't mean that technology is always going to be used for the common good. You may believe Edward Snowden to be a traitor or a hero, but on this matter, there is virtually no question: Mass surveillance is not only unconstitutional, it is also the wrong way to fight terrorism.

AT Privacy

AT Privacy General

Weigh consequences — especially when responding to terrorism.

Isaac 2

Jeffrey C. Isaac, James H. Rudy Professor of Political Science and Director of the Center for the Study of Democracy and Public Life at Indiana University-Bloomington, 2002 ("Ends, Means, and Politics," *Dissent*, Volume 49, Issue 2, Spring, p. 35-37)

As writers such as Niccolo Machiavelli, Max Weber, Reinhold Niebuhr, and Hannah Arendt have taught, an unyielding concern with moral goodness undercuts political responsibility. The concern may be morally laudable, reflecting a kind of personal integrity, but it suffers from three fatal flaws: (1) It fails to see that the purity of one's intention does not ensure the achievement of what one intends. Abjuring violence or refusing to make common cause with morally compromised parties may seem like the right thing; but if such tactics entail impotence, then it is hard to view them as serving any moral good beyond the clean conscience of their supporters; (2) it fails to see that in a world of real violence and injustice, moral purity is not simply a form of powerlessness; it is often a form of complicity in injustice. [end page 35] This is why, from the standpoint of politics—as opposed to religion—pacifism is always a potentially immoral stand. In categorically repudiating violence, it refuses in principle to oppose certain violent injustices with any effect; and (3) it fails to see that politics is as much about unintended consequences as it is about intentions; it is the effects of action, rather than the motives of action, that is most significant. Just as the alignment with "good" may engender impotence, it is often the pursuit of "good" that generates evil. This is the lesson of communism in the twentieth century: it is not enough that one's goals be sincere or idealistic; it is equally important, always, to ask about the effects of pursuing these goals and to judge these effects in pragmatic and historically contextualized ways. Moral absolutism inhibits this judgment. It alienates those who are not true believers. It promotes arrogance. And it undermines political effectiveness.

Privacy violations inevitable – tech and corporations

Goldsmith, 2015

Jack the Henry L. Shattuck Professor at Harvard Law School, The Ends of Privacy, The New Rambler, Apr. 06, 2015 (reviewing Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (2015)). Published Version

http://newramblerreview.com/images/files/Jack-Goldsmith_Review-of-Bruce-Schneier.pdf

The truth is that consumers love the benefits of digital goods and are willing to give up traditionally private information in exchange for the manifold miracles that the Internet and big data bring. Apple and Android each offer more than a million apps, most of which are built upon this model, as are countless other Internet services. More generally, big data promises huge improvements in economic efficiency and productivity, and in health care and safety. Absent abuses on a scale we have not yet seen, the public's attitude toward giving away personal information in exchange for these benefits will likely persist, even if the government requires firms to make more transparent how they collect and use our data. One piece of evidence for this is that privacy-respecting search engines and email services do not capture large market shares. In general these services are not as easy to use, not as robust, and not as efficacious as their personal-data-heavy competitors. Schneier understands and discusses all this. In the end his position seems to be that we should deny ourselves some (and perhaps a lot) of the benefits big data because the costs to privacy and related values are just too high. We "have to stop the slide" away from privacy, he says, not because privacy is "profitable or efficient, but because it is moral." But as Schneier also recognizes, privacy is not a static moral concept. "Our personal definitions of privacy are both cultural and situational," he acknowledges. Consumers are voting

with their computer mice and smartphones for more digital goods in exchange for more personal data. The culture increasingly accepts the giveaway of personal information for the benefits of modern computerized life. This trend is not new. “The idea that privacy can’t be invaded at all is utopian,” says Professor Charles Fried of Harvard Law School. “There are amounts and kinds of information which previously were not given out and suddenly they have to be given out. People adjust their behavior and conceptions accordingly.” That is Fried in the 1970 Newsweek story, responding to an earlier generation’s panic about big data and data mining. The same point applies today, and will apply as well when the Internet of things makes today’s data mining seem as quaint as 1970s-era computation.

No Moral Objections to Surveillance – even new concerns don’t assume the strength of activist potential

Sagar 15—Rahul Sagar, Assistant Professor of Politics at Princeton University, 2015 (“Against Moral Absolutism: Surveillance and Disclosure After Snowden,” *Cambridge Journals Online*, June 12th, Available online at <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9749725&fileId=S0892679415000040>, Accessed on 7/15/15)

I have challenged the conspiratorial view that state surveillance serves to reinforce the hegemony of a shadowy elite. A basic premise of the discussion that follows is that in contemporary liberal democracies, communications surveillance is a legitimate activity. What, then, ought to be the bounds of such surveillance and how far can we be confident that these bounds are being observed? In order to ascertain the rightful bounds on communications surveillance we need to weigh the interests it furthers against those it threatens. The interest it furthers is national security. Greenwald questions this link on a number of grounds. He argues that surveillance is a disproportionate response to the threat of terrorism, which has been “plainly exaggerated” because the “risk of any American dying in a terrorist attack is . . . considerably less than the chance of being struck by lightning.” □ Furthermore, even if the threat of terrorism is real, surveillance is unjustified because to “venerate physical safety above all other values” means accepting “a life of paralysis and fear.” □ He also questions surveillance’s relevance to national security on the grounds that it is often employed to further other national or commercial interests. He asks how, for instance, does “spying on negotiation sessions at an economic summit or targeting the democratically elected leaders of allied states” serve national security? □ Arguably these criticisms miss the mark. That terrorist plots thus far have been amateurish does not mean that terrorists will not learn and eventually succeed in causing greater harm. Nor is being concerned about terrorism tantamount to “pursuing absolute physical safety.” □ The terror in terrorism comes from the unpredictability and the brutality of the violence inflicted on civilians. There is a difference between voluntarily undertaking a somewhat risky bicycle ride in rush hour traffic and being unexpectedly blown to bits while commuting to work. Finally, it is widely accepted that countries have a right to pursue their national interests, subject of course to relevant countervailing ethical considerations. It is not hard to imagine how intercepting Chancellor Angela Merkel’s conversation could serve the United States’ national security interests (for example, it could provide intelligence on Europe’s dealings with Russia). What are the countervailing values that have been overlooked in this case? The President’s Review Group on Intelligence and Communications Technologies, set up in the wake of Snowden’s disclosures, warns that surveillance of foreign leaders must be “respectful.” But the justification offered is strategic rather than moral: the group urges caution out of recognition for “the importance of cooperative relationships with other nations.” □ A moral justification would have weak legs since American allies, including Germany, reportedly engage in similar practices. □ As Greenwald himself acknowledges, the NSA’s surveillance of foreign leaders is “unremarkable” because “countries have spied on heads of state for centuries, including allies.” □ □ Greenwald also raises objections from a national security perspective. He warns that mass surveillance undermines national security because “it swamps the intelligence agencies with so much data that they cannot possibly sort through it effectively.” □ □ He also questions the efficacy of communications surveillance, arguing that it has little to show in terms of success in combating terrorism. But these criticisms are equally unpersuasive. It is certainly possible that a surveillance program could generate so much raw data that an important piece of information is overlooked. But in such a case the appropriate response would not be to shut down the program but rather to bulk up the processing power and manpower devoted to it. Finally, both the President’s Review Group and the Privacy and Civil Liberties Oversight Board have examined the efficacy of the NSA’s programs. Both report that the NSA’s foreign surveillance programs have contributed to more than fifty counterterrorism investigations, leading them to conclude that the NSA “does in fact play an important role in the nation’s effort to prevent terrorist attacks across the globe.” □ □ So far I have argued that communications surveillance can further national security. However, national

security is not the only value liberal democracies and their citizens deem important. Hence we need to consider how far communications surveillance impinges on other important interests and values. Greenwald identifies two major harms. The first is political in nature. Mass surveillance is said to stifle dissent because “a citizenry that is aware of always being watched quickly becomes a compliant and fearful one.” Compliance occurs because, anticipating being shamed or condemned for nonconformist behavior, individuals who know they are being watched “think only in line with what is expected and demanded.” ☐☐ Even targeted forms of surveillance are not to be trusted, Greenwald argues, because the “indifference or support of those who think themselves exempt invariably allows for the misuse of power to spread far beyond its original application.” ☐☐ These claims strike me as overblown. The more extreme claim, that surveillance furthers thought control, is neither logical nor supported by the facts. It is logically flawed because accusing someone of trying to control your mind proves that they have not succeeded in doing so. On a more practical level, the fate met by states that have tried to perfect mass control—the Soviet Union and the German Democratic Republic, for example—suggests that surveillance cannot eliminate dissent. It is also not clear that surveillance can undermine dissident movements as easily as Greenwald posits. The United States’ record, he writes, “is suffused with examples of groups and individuals being placed under government surveillance by virtue of their dissenting views and activism—Martin Luther King, Jr., the civil rights movement, antiwar activists, environmentalists.” ☐☐ These cases are certainly troubling, but it hardly needs pointing out that surveillance did not prevent the end of segregation, retreat from Vietnam, and the rise of environmental consciousness. This record suggests that dissident movements that have public opinion on their side are not easily intimidated by state surveillance (a point reinforced by the Arab Spring). Surveillance may make it harder for individuals to associate with movements on the far ends of the political spectrum. But why must a liberal democracy refrain from monitoring extremist groups such as neo-Nazis and anarchists? There is the danger that officials could label as “extreme” legitimate movements seeking to challenge the prevailing order. Yet the possibility that surveillance programs could expand beyond their original ambit does not constitute a good reason to end surveillance altogether. A more proportionate response is to see that surveillance powers are subject to oversight. The second harm Greenwald sees surveillance posing is personal in nature. Surveillance is said to undermine the very essence of human freedom because the “range of choices people consider when they believe that others are watching is . . . far more limited than what they might do when acting in a private realm.” ☐☐ Internet-based surveillance is viewed as especially damaging in this respect because this is “where virtually everything is done” in our day, making it the place “where we develop and express our very personality and sense of self.” Hence, “to permit surveillance to take root on the Internet would mean subjecting virtually all forms of human interaction, planning, and even thought itself to comprehensive state examination.” ☐☐ This claim too seems overstated in two respects. First, it exaggerates the extent to which our self-development hinges upon electronic communication channels and other related activities that leave electronic traces. The arrival of the Internet certainly opens new vistas, but it does not entirely close earlier ones. A person who fears what her browsing habits might communicate to the authorities can obtain texts offline. Similarly, an individual who fears transmitting materials electronically can do so in person, as Snowden did when communicating with Greenwald. There are costs to communicating in such “old-fashioned” ways, but these costs are neither new nor prohibitive. Second, a substantial part of our self-development takes place in public. We become who we are through personal, social, and intellectual engagements, but these engagements do not always have to be premised on anonymity. Not everyone wants to hide all the time, which is why public engagement—through social media or blogs, for instance—is such a central aspect of the contemporary Internet.

The right to security trumps the right to privacy – Individual ethics prove Himma 2007 (KENNETH EINAR , “Privacy Versus Security: Why Privacy is Not an Absolute Value or Right” *San Diego Law Review*, [**DebateUS!**
Formerly Millennial
Speech and Debate](http://poseidon01.ssrn.com/delivery.php?ID=946099113093066103077074112016017090015022028045089092075001073099001099109106114127011017012000106100015114101076020123093078010050012092072093113078096021081008038034055090107126078091116028103066027088072124015085097094100087114086001099009078&EXT=pdf&TYPE=2)</p></div><div data-bbox=)

From an intuitive standpoint, the idea that the right to privacy is an absolute right seems utterly implausible. Intuitively, it seems clear that there are other rights that are so much more important that they easily trump privacy rights in the event of a conflict. For example, if a psychologist knows that a patient is highly likely to commit a murder, then it is, at the very least, morally permissible to disclose that information about the patient in order to prevent the crime—regardless of whether such information would otherwise be protected by privacy rights. Intuitively, it seems clear that life is more important from the standpoint of morality than any of the interests protected by a moral right to privacy. Still one often hears—primarily from academics in information schools and library schools, especially in connection with the controversy regarding the USA PATRIOT Act—the claim that privacy should never be sacrificed for security, implicitly denying what I take to be the underlying rationale for the PATRIOT Act. This also seems counterintuitive because it does not seem unreasonable to believe we have a moral right to security that includes the right to life. Although this right to security is broader than the right to life, the fact that security interests include our interests in our lives implies that the right to privacy trumps even the right to life—something that seems quite implausible from an intuitive point of view. If I have to give up the most private piece of information about myself to save my life or protect myself from either grievous bodily injury or financial ruin, I would gladly do so without hesitation. There are many things I do not want you to know about me, but should you make a credible threat to my life, bodily integrity, financial security, or health, and then hook me up to a lie detector machine, I will truthfully answer any question you ask about me. I value my privacy a lot, but I value my life, bodily integrity, and financial security much more than any of the interests protected by the right to privacy.

Surveillance reinforces the equal protection of the law – key to equitable morals

Taylor 05

[In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance; James Stacey Taylor; Public Affairs Quarterly Vol. 19, No. 3 (Jul., 2005), pp. 227-246 Published by: University of Illinois Press on behalf of North American Philosophical Publications Stable URL: <http://www.jstor.org/stable/40441413>] //duff

A system of constant State surveillance would have other advantages, too. Under the current criminal justice system a wealthy defendant who is innocent of the charges that she is faced with can use her wealth to hire private investigators to demonstrate her innocence, either by finding persons who witnessed the crime of which she is accused, or by finding persons who can provide her with a legitimate alibi. This option is not open to poorer defendants who are similarly innocent, but who cannot afford to hire private investigators. Since this is so, innocent, poor defendants are more likely than innocent, wealthy defendants to accept plea bargains, or to be convicted of crimes that they did not commit. If, however, a poor person were to be accused of a crime in a State that subjected its citizens to constant surveillance, the judge in her case would be morally justified (indeed, would be morally required) in enabling the defense to secure information that would prove her innocence, and that would have been gathered by the State's surveillance devices. A State's use of constant surveillance could thus reduce the number of persons who are wrongfully convicted. This would not only be good in itself, but it would also lead to a more equitable justice system, for the disparity in wrongful conviction rates between the wealthy (who could use their wealth to prove their innocence) and the poor could be eliminated.

Transparency is inevitable and aids psychological and ethical self-development – welcome to Post-Privacy

Seemann, 2015,

Michael Seemann studied Applied Cultural Studies in Lüneburg. Now he blogs at mspr0.de and writes for various media like Rolling Stone, TIME online, SPEX, Spiegel Online, c't and the DU magazine "Digital Tailspin Ten Rules for the Internet After Snowden" The Network Notebooks series March 2015 http://networkcultures.org/wp-content/uploads/2015/03/NN09_Digital_Tailspin_SP.pdf

POST-PRIVACY: TRANSPARENCY AS A STOIC EXERCISE In his book Post-Privacy: Prima leben ohne Privatsphäre (Post-Privacy: Living just Fine Without Privacy),¹⁸ Christian Heller embraces an even more radical strategy. He argues that it is time to say goodbye to privacy altogether and to embrace the inevitable: transparency. He highlights, amongst other points, the fact that privacy as we know it today is a relatively new form of coexistence, and one that has not only been advantageous. The private sphere has, for the longest time, been the place of the oppression of women, for example. Contrast this with the gay rights movements, which were among the first to show how social progress can be achieved by making ultimately personal information public. Since we are unable to halt technological progress, we'd better get used to the idea of total transparency, says Heller. Heller himself acts out this idea in practice. He documents all of his daily routines, his finances, and large amounts of highly personal information in a publicly accessible wiki.¹⁹ It is easy to dismiss this as a self-indulgent discovery trip, but Heller is undeniably radicalizing an issue that has become the norm, in social networks anyway, namely the fact that formerly private matters are explicitly being made public. Unlike many Facebook users, however, Heller doesn't deceive himself. He is highly aware of the fact that his data can be used and abused, by anyone, at any time, for any purpose. In this sense, post-privacy as a strategy complies well with Nassim Nicholas Taleb's dictum of antifragility. Post-privacy is a practical exercise in stoicism: basing your assumptions on the worst case scenario – in this case, that all information is public by default – will not give you a false sense of security, but rather will allow you to make plans in such a way that, should this worst case actually occur, you will not be confronted with unsolvable problems. If you keep in mind that all data is accessible, in one way or another, this can actually reduce anxiety – one of the more negative effects of surveillance.

Their understanding of privacy rights as personal will fail because its impossible in modern society.

Stalder, 2009,

Felix. Department of Sociology, Queens University "Privacy is not the Antidote to Surveillance." Surveillance & Society 1.1 (2009): 120-124.

So rather than fight those connections – some of which are clearly beneficial, some of which are somewhat ambiguous, and some are clearly disconcerting – we have to reconceptualize what these connections do. Rather than seeing them as acts of individual transgression (X has invaded Y's privacy) we have to see them part of a new landscape of social power. Rather than continuing on the defensive, by trying to maintain an ever-weakening illusion of privacy, we have to shift to the offensive and start demanding accountability of those whose power is enhanced by the new connections. In a democracy, political power is, at least ideally, tamed by making the government accountable to those who are governed, not by carving out areas in which the law doesn't apply. It is, in this perspective, perhaps no coincidence that many of the strongest privacy advocates (at least in the US) lean politically towards libertarianism, a movement which includes on its fringe white militias which try to set up zones liberated from the US government. In our democracies, extensive institutional mechanisms have been put into place to create and maintain accountability, and to punish those who abuse their power. We need to develop and instate similar mechanisms for the handling of personal information – a technique as crucial to power as the ability to exercise physical violence – in order to limit the

concentration of power inherent in situations that involve unchecked surveillance. The current notion of privacy, which frames the issue as a personal one, won't help us accomplish that.⁹ However, notions of institutionalized accountability will, because they acknowledge surveillance as a structural problem of political power. It's time to update our strategies for resistance and develop approaches adequate to the actual situation rather than sticking to appealing but inadequate ideas that will keep locking us into unsustainable positions.

Private Seector Makes Violations Non-Unique

Private sector collects a lot of data already

Los Angeles Times, May 5, 2014, <http://www.latimes.com/business/la-fi-lazarus-20140506-column.html>

I wrote recently about Verizon Wireless quietly downloading code into people's home computers that would transmit your online browsing to marketers, who could then target you with related ads on your smartphone or tablet. Such corporate spying is apparently legal and, experts say, will become increasingly common as businesses try to track consumers from device to device. And the more they share people's information among themselves — a shadowy industry of data brokers already exists — the more they'll amass digital dossiers containing intimate details about your life, including where you shop, how you pass your weekends and what medicines you take.

NSA surveillance no different than what private companies do and with only a couple hundred people

Allan Swarn, May 5, 2014, arnnet,
http://www.arnnet.com.au/article/544320/cebit_2014_privacy_about_more_than_compliance_it_vital_economy_ccu/

He said the post-Snowden revelations about NSA spying have been overblown. Much of that has been machine parsing of data, and that the NSA has at most a couple of hundred people attempting to read a given language, globally. It has larger numbers of people attempting to read all languages. But even the total number of NSA linguists is tiny compared to the total volume of global communications. The NSA's spying is mostly done by machines and algorithms - there simply aren't enough staff to 'human spy' on everyone. Borg compares the NSA surveillance to the same tracking Amazon, Facebook and Google do daily in our lives.

Corporate surveillance is inevitable and they'll willingly provide data to the government

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

Corporate surveillance and government surveillance aren't separate. They're intertwined; the two support each other. It's a public-private surveillance partnership that spans the world. This isn't a formal agreement; it's more an alliance of interests. Although it isn't absolute, it's become a de facto reality, with many powerful stakeholders supporting its perpetuation. And though Snowden's revelations about NSA surveillance have caused rifts in the partnership—we'll talk about those in Chapter 14—it's still strong. The Snowden documents made it clear how much the NSA relies on US corporations to eavesdrop on the Internet. The NSA didn't build a massive Internet eavesdropping system from scratch. It noticed that the corporate world was already

building one, and tapped into it. Through programs like PRISM, the NSA legally compels Internet companies like Microsoft, Google, Apple, and Yahoo to provide data on several thousand individuals of interest. Through other programs, the NSA gets direct access to the Internet backbone to conduct mass surveillance on everyone. Sometimes those corporations work with the NSA willingly. Sometimes they're forced by the courts to hand over data, largely in secret. At other times, the NSA has hacked into those corporations' infrastructure without their permission.

This is happening all over the world. Many countries use corporate surveillance capabilities to monitor their own citizens. Through programs such as TEMPORA, the UK's GCHQ pays telcos like BT and Vodafone to give it access to bulk communications all over the world. Vodafone gives Albania, Egypt, Hungary, Ireland, and Qatar—possibly 29 countries in total—direct access to Internet traffic flowing inside their countries. We don't know to what extent these countries are paying for access, as the UK does, or just demanding it. The French government eavesdrops on France Télécom and Orange. We've already talked about China and Russia in Chapter 5. About a dozen countries have data retention laws—declared unconstitutional in the EU in 2014—requiring ISPs to keep surveillance data on their customers for some months in case the government wants access to it. Internet cafes in Iran, Vietnam, India, and elsewhere must collect and retain identity information of their customers.

Similar things are happening off the Internet. Immediately after 9/11, the US government bought data from data brokers, including air passenger data from Torch Concepts and a database of Mexican voters from ChoicePoint. US law requires financial institutions to report cash transactions of \$10,000 or larger to the government; for currency exchangers, the threshold is \$1,000. Many governments require hotels to report which foreigners are sleeping there that night, and many more make copies of guests' ID cards and passports. CCTV cameras, license plate capture systems, and cell phone location data are being used by numerous governments.

By the same token, corporations obtain government data for their own purposes. States like Illinois, Ohio, Texas, and Florida sell driver's license data, including photos, to private buyers. Some states sell voter registration data. The UK government proposed the sale of taxpayer data in 2014, but public outcry has halted that, at least temporarily. The UK National Health Service also plans to sell patient health data to drug and insurance firms. There's a feedback loop: corporations argue for more government data collection, then argue that the data should be released under open government laws, and then repackage the data and sell it back to the government.

The net result is that a lot of surveillance data moves back and forth between government and corporations. One consequence of this is that it's hard to get effective laws passed to curb corporate surveillance—governments don't really want to limit their own access to data by crippling the corporate hand that feeds them.

The government can just ask for or buy the data – surveillance unnecessary

Turner, 15 - Brad Turner is a graduate of Duke Law School and a practicing attorney in Ohio. ("When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data" 16 N.C. J.L. & Tech. 377, January, lexis)

The government can obtain second-hand data from private parties in a variety of ways. First, the government can simply ask for it. According to Google, nearly 1% of requests for its user data from law enforcement are emergency requests. n185 A bill that has been proposed in Congress, called the Cyber Intelligence Sharing and Protection Act ("CISPA"), might dramatically increase this percentage. CISPA would make it legal for the government to ask companies for data about their customers and then protect those companies from lawsuits related to the handing over of that data, "notwithstanding any other provision of law." n186

Second, the government can demand the data with a subpoena. A subpoena need not be reviewed or pre-approved by a court to be valid and enforceable. n187 Google says that 68% of its data requests from the government are in the form of a subpoena. n188 Subpoenas can request any information or documents that are at all relevant to an investigation. Relevance is defined very broadly and includes any information or documents that "might have the potential to lead to relevant information." n189 So long as a subpoena meets this very lenient standard, a court will deem the subpoena valid to the extent that the subpoena's demands are not overbroad or unduly burdensome. n190

Third, the government can demand the information with a court order, which, by definition, does require prior approval by a [*411] court. n191 Google says that 22% of its requests for data by the government are from warrants, and another 6% are from court orders. n192 The NSA collects much of its data by using secret FISA court orders, collecting huge sums of data from U.S. telephone companies, including AT&T, Verizon, and Sprint, and Internet service-providers like Facebook, Apple, Google, Microsoft, Yahoo, and AOL. n193 Statutes regulate these data-collection efforts. n194

Fourth, the government can purchase the information. Big Data is valuable and companies are willing to sell. n195 For the right price, [*412] government can access the same rich data-troves held by private organizations. For example, the federal government recently started buying access to a private database maintained by the credit bureau Equifax, called "The Work Numbers." n196 The database contains 54 million active salary and employment records and more than 175 million historical records from approximately 2,500 U.S. employers. n197 Equifax also sells this same data to credit card issuers, property managers, and auto lenders. n198

Can't solve privacy – private sector and foreign government collection

Lewis 5/28 – Director and Senior Fellow, Strategic Technologies Program (James Lewis, "What Happens on June 1?", CSIS Strategic Technologies Program, [//MBB](http://www.csistech.org/blog/2015/5/28/what-happens-on-june-1, 5/28/2015)

Privacy itself will not increase. The privacy battle was lost years ago when extracting your personal data became the business model of the internet. Americans have far less privacy than they did in 1995 and NSA has nothing to do with this. There are several ironies in this situation, not the least being that NSA collection operated under far more rules than private sector or foreign government collection, and many of the immense private sector databases are likely accessible to foreign governments (if they decide they can use them).

Economic incentives for corporate surveillance overwhelm the plan on a massive scale

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

Historically, surveillance was difficult and expensive. We did it only when it was important: when the police needed to tail a suspect, or a business required a detailed purchasing history for billing purposes. There were exceptions, and they were extreme and expensive. The exceptionally paranoid East German government had 102,000 Stasi surveilling a population of 17 million: that's one spy for every 166 citizens, or one for every 66 if you include civilian informants.

Corporate surveillance has grown from collecting as little data as necessary to collecting as much as possible. Corporations always collected information on their customers, but in the past they didn't collect very much of it and held it only as long as necessary. Credit card companies collected only the information about their customers' transactions that they needed for billing. Stores hardly ever collected information about their customers, and mail-order companies only collected names and addresses, and maybe some purchasing history so they knew when to remove someone from their mailing list. Even Google, back in the beginning, collected far less information about its users than it does today. When surveillance information was expensive to collect and store, corporations made do with as little as possible.

The cost of computing technology has declined rapidly in recent decades. This has been a profoundly good thing. It has become cheaper and easier for people to communicate, to publish their thoughts, to access information, and so on. But that same decline in price has also brought down the price of surveillance. As computer technologies improved, corporations were able to collect more information on everyone they did business with. As the cost of data storage became cheaper, they were able to save more data and for a longer time. As big data analysis tools became more powerful, it became profitable to save more information. This led to the surveillance-based business models I'll talk about in Chapter 4.

Government surveillance has gone from collecting data on as few people as necessary to collecting it on as many as possible. When surveillance was manual and expensive, it could only be justified in extreme cases. The warrant process limited police surveillance, and resource constraints and the risk of discovery limited national intelligence surveillance. Specific individuals were targeted for surveillance, and maximal information was collected on them alone. There were also strict minimization rules about not collecting information on other people. If the FBI was listening in on a mobster's phone, for example, the listener was supposed to hang up and stop recording if the mobster's wife or children got on the line.

As technology improved and prices dropped, governments broadened their surveillance. The NSA could surveil large groups—the Soviet government, the Chinese diplomatic corps, leftist political organizations and activists—not just individuals. Roving wiretaps meant that the FBI could eavesdrop on people regardless of the device they used to communicate with. Eventually, US agencies could spy on entire populations and save the data for years. This dovetailed with a

changing threat, and they continued espionage against specific governments, while expanding mass surveillance of broad populations to look for potentially dangerous individuals. I'll talk about this in Chapter 5.

The result is that corporate and government surveillance interests have converged. Both now want to know everything about everyone. The motivations are different, but the methodologies are the same. That is the primary reason for the strong public-private security partnership that I'll talk about in Chapter 6.

All personal information is freely available – the aff is a meaningless gesture

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

The result of this declining cost of surveillance technology is not just a difference in price; it's a difference in kind. Organizations end up doing more surveillance—a lot more. For example, in 2012, after a Supreme Court ruling, the FBI was required to either obtain warrants for or turn off 3,000 GPS surveillance devices installed in cars. It would simply be impossible for the FBI to follow 3,000 cars without automation; the agency just doesn't have the manpower. And now the prevalence of cell phones means that everyone can be followed, all of the time.

Another example is license plate scanners, which are becoming more common. Several companies maintain databases of vehicle license plates whose owners have defaulted on their auto loans. Spotter cars and tow trucks mount cameras on their roofs that continually scan license plates and send the data back to the companies, looking for a hit. There's big money to be made in the repossession business, so lots of individuals participate—all of them feeding data into the companies' centralized databases. One scanning company, Vigilant Solutions of Livermore, California, claims to have 2.5 billion records and collects 70 million scans in the US per month, along with date, time, and GPS location information.

In addition to repossession businesses, scanning companies also sell their data to divorce lawyers, private investigators, and others. They sometimes relay it, in real time, to police departments, which combine it with scans they get from interstate highway onramps, toll plazas, border crossings, and airport parking lots. They're looking for stolen vehicles and drivers with outstanding warrants and unpaid tickets. Already, the states' driver's license databases are being used by the FBI to identify people, and the US Department of Homeland Security wants all this data in a single national database. In the UK, a similar government-run system based on fixed cameras is deployed throughout the country. It enforces London's automobile congestion charge system, and searches for vehicles that are behind on their mandatory inspections.

Expect the same thing to happen with automatic face recognition. Initially, the data from private cameras will most likely be used by bounty hunters tracking down bail jumpers. Eventually, though, it will be sold for other uses and given to the government. Already the FBI has a database of 52 million faces, and facial recognition software that's pretty good. The Dubai police are

integrating custom facial recognition software with Google Glass to automatically identify suspects. With enough cameras in a city, police officers will be able to follow cars and people around without ever leaving their desks. This is mass surveillance, impossible without computers, networks, and automation. It's not “follow that car”; it's “follow every car.” Police could always tail a suspect, but with an urban mesh of cameras, license plate scanners, and facial recognition software, they can tail everyone—suspect or not.

Similarly, putting a device called a pen register on a suspect's land line to record the phone numbers he calls used to be both time-consuming and expensive. But now that the FBI can demand that data from the phone companies' databases, it can acquire that information about everybody in the US. And it has.

In 2008, the company Waze (acquired by Google in 2013) introduced a new navigation system for smartphones. The idea was that by tracking the movements of cars that used Waze, the company could infer real-time traffic data and route people to the fastest roads. We'd all like to avoid traffic jams. In fact, all of society, not just Waze's customers, benefits when people are steered away from traffic jams so they don't add to them. But are we aware of how much data we're giving away?

For the first time in history, governments and corporations have the ability to conduct mass surveillance on entire populations. They can do it with our Internet use, our communications, our financial transactions, our movements ... everything. Even the East Germans couldn't follow everybody all of the time.

Corporate privacy invasions

Danny Schechter edits Mediachannel.org and blogs at Newdissector.net. He is producing a TV documentary series on America's surveillance state, May 16, 2014, "Can we stop America's Surveillance State?" http://www.huffingtonpost.com/danny-schechter/can-we-stop-americas-surv_b_5334572.html?utm_hp_ref=politics&ir=Politics

American corporations are not just cooperating with the NSA but competing with it. And, not just with Google cars photographing every street in the world. Just ask Donald Sterling, the LA Clippers owner and jerk as he may be, about what non-government spying did to him. Who has been prosecuted in that eavesdropping incident? I spoke to Sam Antar who was wiretapped by the government as part of an investigation into illegal practices by the Crazy Eddy electronics chain years ago and who became a convicted felon. He says that spying has become a profitable business, that is bigger and even more insidious than the NSA.

Private sector collects a lot of data already

Los Angeles Times, May 5, 2014, <http://www.latimes.com/business/la-fi-lazarus-20140506-column.html>

I wrote recently about Verizon Wireless quietly downloading code into people's home computers that would transmit your online browsing to marketers, who could then target you with related ads on your smartphone or tablet. Such corporate spying is apparently legal and, experts say, will become increasingly common as businesses try to track consumers from device to device. And the more they share people's information among themselves — a shadowy industry of data brokers already exists — the more they'll amass digital dossiers containing intimate details about your life, including where you shop, how you pass your weekends and what medicines you take.

NSA surveillance no different than what private companies do

Allan Swann, May 5, 2014, arnnet,

http://www.arnnet.com.au/article/544320/cebit_2014_privacy_about_more_than_compliance_it_vital_economy_ccu/

He said the post-Snowden revelations about NSA spying have been overblown. Much of that has been machine parsing of data, and that the NSA has at most a couple of hundred people attempting to read a given language, globally. It has larger numbers of people attempting to read all languages. But even the total number of NSA linguists is tiny compared to the total volume of global communications.

The NSA's spying is mostly done by machines and algorithms - there simply aren't enough staff to 'human spy' on everyone. Borg compares the NSA surveillance to the same tracking Amazon, Facebook and Google do daily in our lives.

Private abuse of digital information is worse and only surveillance can stop that.

Simon, Arthur Levitt Professor of Law at Columbia University, 2014,

William H. Simon, 10-20-2014, "Rethinking Privacy," Boston Review,

<http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance>

The critics' preoccupation with the dangers of state oppression often leads them to overlook the dangers of private abuse of surveillance. They have a surprisingly difficult time coming up with actual examples of serious harm from government surveillance abuse. Instead, they tend to talk about the "chilling effect" from awareness of surveillance. By contrast, there have been many examples of serious harm from private abuse of personal information gained from digital sources. At least one person has committed suicide as a consequence of the Internet publication of video showing him engaged in sexual activity. Many people have been humiliated by the public release of a private recording of intimate conduct, and blackmail based on threats of such disclosure has emerged as a common practice. Some of this private abuse is and should be illegal. But the legal prohibitions can only be enforced if the government has some of the surveillance capacities that critics decry. Illicit recording and distribution can only be restrained if the wrongdoers can be identified and their actions effectively restrained. Less compromising critics would deny government these capacities.

Corporation commit much worse privacy violations.

Lowry 15,

Rich, Editor, the National Review, 5-27-2015, "Lowry: NSA data program faces death by bumper

sticker," Salt Lake Tribune,
<http://www.sltrib.com/csp/mediapool/sites/sltrib/pages/printfriendly.csp?id=2557534>

In the context of all that is known about us by private companies, the NSA is a piker. Take the retailer Target, for example. According to The New York Times, it collects your “demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you’ve moved recently, what credit cards you carry in your wallet and what Web sites you visit.” Of course, the Fourth Amendment applies to the government, not private entities like Target. The amendment protects against unreasonable searches and seizures of our “persons, houses, papers, and effects.” If the NSA were breaking into homes and seizing metadata that people had carefully hidden away from prying eyes, it would be in flagrant violation of the Fourth Amendment. But no one is in possession of his or her own metadata. Even if the NSA didn’t exist, metadata would be controlled by someone else, the phone companies. The Supreme Court has held that you don’t have an expectation of privacy for such information in the possession of a third party. One frightening way to look at mail delivery is that agents of the state examine and handle the correspondence of countless of millions of Americans. They aren’t violating anyone’s Fourth Amendment rights, though, because no one expects the outside of their envelopes to be private.

Alt causes to privacy violations – corporations, the use of nonsensitive information

Etzioni 15 Amitai, “The New Normal – Finding a Balance between Individual Rights and the Common Good, Transaction Publishers – New Brunswick, NJ, Senior Advisor to the Carter White House; taught at Columbia, Harvard Business, Copyright 2015, ISBN 978-1-4128-5477-1)

Another key principle is a ban on using nonsensitive information to divine the sensitive (e.g., using information about routine consumer purchases to divine one's medical condition) because it is just as intrusive as collecting and employing sensitive information.⁶⁵ This is essential because currently such behavior is rather common.⁶⁶ Thus, under the suggested law, Target would be prevented from sending coupons for baby items to a teenage girl after the chain store's analysis of her recent purchases suggested she might be pregnant.⁶⁷ To further advance the cyber age privacy doctrine, much more attention needs to be paid to private actors. Privacy rights, like others, are basically held against the government, to protect people from undue intrusion by public authori- ties. However, cybernation is increasingly carried out by the private sector. There are corporations that make shadowing Internet users-and keeping very detailed dossiers on them-their main line of business. According to Slobogin, Companies like Acxiom, Docussearch, ChoicePoint, and Oracle can provide the inquirer with a wide array of data about any of us, including: Basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity.⁶⁸ These data are routinely made available to government agencies, including the FBI. Unless this private cybernation is covered, the cyber age privacy doctrine will be woefully incomplete.⁶⁹ Given that private actors are very actively engaged in cybernation and often tailor their work so that it might be used by the government (even if no contract is in place and they are, hence, not subject to the limits imposed on the government), extending the privacy doctrine beyond the public/private divide is of pivotal importance for the future of privacy in the cyber age. Admittedly, applying to the private sector restrictions and regulations similar to those that control the government may well be politically unfeasible in the current environment. However, as one who analyzes the conditions of society from a normative viewpoint, I am duty-bound to point out that it makes ever less sense to maintain this distinction.⁷⁰ Privacy will be

increasingly lost in the cyber age, with little or no gain to the common good, unless private actors- and not just the government-are more reined in. To what extent this may be achieved by self-regulation, changes in norms, increased transparency, or government regulation is a question not addressed here.

Plan can't solve for private alternate causes to massive invasions of privacy

Neil M. Richards 13, Professor of Law at George Washington University, 2012-2013, 126 Harv. L. Rev. 1934, "The Dangers of Surveillance,"
http://heinonline.org/HOL/Page?handle=hein.journals/hlr126&div=89&g_start=1&collection=journals&men_tab=citnav&men_hide=false

Surveillance is not just for governments either. Private companies big and small generate vast fortunes from the collection, use, and sale of personal data. At the broadest level, we are building an Internet that is on its face free to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits." Such "behavioral advertising" is a multibillion-dollar business, and is the foundation on which the successes of companies like Google and Facebook have been built." One recent study concludes that this form of surveillance is so ingrained into the fabric of the Internet "that a small number of companies have a window into most of our movements online."¹⁰ Other technologies engage in similar forms of private surveillance. "Social reading" applications embedded into Facebook and other platforms enable the disclosure of one's reading habits, while electronic readers like the Kindle and the Nook track reader behavior down to the specific page of the specific book on which a user's attention is currently lingering."

In recent years, industry, media, and scholars have increasingly focused their attention on the concept of "Big Data," an unwieldy term often used to describe the creation and analysis of massive data sets. Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and analyzed to produce new inferences and endings. As social scientists danah boyd and Kate Crawford put it, "Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself?" Big Data holds much potential for good in areas as diverse as medical research, the "smart" electrical grid, and traffic management."

But Big Data also raises many potential problems in areas such as privacy and consumer power. For example, the retail superstore Target uses Big Data analytics to infer which of its customers are pregnant based upon their purchases of other products and upon personally identifying data from other sources. As the New York Times Magazine reports, new parents are highly desirable customers not just because they buy many new products, but because their normally stable purchasing habits are "up for grabs" in the chaotic exhaustion that accompanies the birth of a child." Target uses Big Data to snare new parents because, as one of its data analysts concedes, "[w]e knew that if we could identify them in their second trimester, there's a good chance we could capture them for years As soon as we get them buying diapers from us, they're going to start buying everything else too." Big Data analytics enabled Target to discover that expectant parents display a change in buying habits (for example, buying unscented lotion and magnesium supplements) that mark them as expectant, allowing this kind of (appropriately enough) "targeted" marketing. Big Data surveillance and analysis thus affect the commercial power of consumers, identifying their times of relative weakness and allowing more effective marketing to nudge them in the directions that watchful companies desire.

The incentives for the collection and distribution of private data are on the rise. The past fifteen years have seen the rise of an Internet in which personal computers and smartphones have been the dominant personal technologies. But the next fifteen will likely herald the "Internet of Things," in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control." Many of us already carry GPS tracking devices in our pockets, not by government command, but in the form of powerful multifunction smartphones. Sociologists Zygmunt Bauman and David Lyon have identified the spread of surveillance beyond nonconsensual state watching to a sometimes-private surveillance in

which the subjects increasingly consent and participate - a phenomenon that they call “liquid surveillance.”¹⁴ Professor Scott Peppet foresees the “unraveling” of privacy, as economic incentives lead consumers to agree to surveillance devices like Progressive Insurance’s “MyRate” program, which offers reduced insurance rates in exchange for the installation of a device that monitors driving speed, time, and habits.¹⁵ Peppet argues that this unraveling of privacy creates a novel challenge to privacy law, which has long focused on unconsented surveillance rather than on surveillance as part of an economic transaction.”

It might seem curious to think of information gathering by private entities as “surveillance”
Notions of surveillance have traditionally been concerned with the watchful gaze of government actors like police and prison officials rather than companies and individuals. But in a postmodern age of “liquid surveillance,” the two phenomena are deeply intertwined. Government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle. At the outset, the technologies of surveillance - software, RFID chips, GPS trackers, cameras, and other cheap sensors are being used almost interchangeably by government and nongovernment watchers.” Private industry is also marketing new surveillance technologies to the state. Though it sounds perhaps like a plot from a paranoid science fiction novel, the Guardian reports that the Disney Corporation has been developing facial recognition technologies for its theme parks and selling the technology to the U.S. military.” Nor do the fruits of surveillance respect the public private divide. Since the September 11 attacks, governments have been eager to acquire the massive consumer and Internet-activity databases that private businesses have compiled for security and other purposes, either by subpoena, or outright purchase,” information can also flow in the other direction: the U.S. government recently admitted that it was giving information to insurance companies that it had collected from automated license-plate readers at border crossings.”

Overwhelming corporate and government tracking is inevitable – the aff is a meaningless half-measure

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

There’s a whole industry devoted to tracking you in real time. Companies use your phone to track you in stores to learn how you shop, track you on the road to determine how close you might be to a particular store, and deliver advertising to your phone based on where you are right now.

Your location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone willing to pay for it. Companies like Sense Networks specialize in using this data to build personal profiles of each of us.

Phone companies are not the only source of cell phone data. The US company Verint sells cell phone tracking systems to both corporations and governments worldwide. The company’s website says that it’s “a global leader in Actionable Intelligence solutions for customer engagement optimization, security intelligence, and fraud, risk and compliance,” with clients in “more than 10,000 organizations in over 180 countries.” The UK company Cobham sells a system that allows someone to send a “blind” call to a phone—one that doesn’t ring, and isn’t detectable. The blind call forces the phone to transmit on a certain frequency, allowing the sender to track that phone to within one meter. The company boasts government customers in Algeria, Brunei, Ghana, Pakistan, Saudi Arabia, Singapore, and the United States. Defentek, a company mysteriously registered in Panama, sells a system that can “locate and track any phone number in the world … undetected and unknown by the network, carrier, or the target.” It’s not an idle

boast; telecommunications researcher Tobias Engel demonstrated the same thing at a hacker conference in 2008. Criminals do the same today.

All this location tracking is based on the cellular system. There's another entirely different and more accurate location system built into your smartphone: GPS. This is what provides location data to the various apps running on your phone. Some apps use location data to deliver service: Google Maps, Uber, Yelp. Others, like Angry Birds, just want to be able to collect and sell it.

You can do this, too. HelloSpy is an app that you can surreptitiously install on someone else's smartphone to track her. Perfect for an anxious mom wanting to spy on her teenager—or an abusive man wanting to spy on his wife or girlfriend. Employers have used apps like this to spy on their employees.

The US National Security Agency (NSA) and its UK counterpart, Government Communications Headquarters (GCHQ), use location data to track people. The NSA collects cell phone location data from a variety of sources: the cell towers that phones connect to, the location of Wi-Fi networks that phones log on to, and GPS location data from Internet apps. Two of the NSA's internal databases, code-named HAPPYFOOT and FASCIA, contain comprehensive location information of devices worldwide. The NSA uses the databases to track people's movements, identify people who associate with people of interest, and target drone strikes.

The NSA can allegedly track cell phones even when they are turned off. I've just been talking about location information from one source—your cell phone—but the issue is far larger than this. The computers you interact with are constantly producing intimate personal data about you. It includes what you read, watch, and listen to. It includes whom you talk to and what you say. Ultimately, it covers what you're thinking about, at least to the extent that your thoughts lead you to the Internet and search engines. We are living in the golden age of surveillance.

Sun Microsystems' CEO Scott McNealy said it plainly way back in 1999: "You have zero privacy anyway. Get over it." He's wrong about how we should react to surveillance, of course, but he's right that it's becoming harder and harder to avoid surveillance and maintain privacy.

Surveillance is a politically and emotionally loaded term, but I use it deliberately. The US military defines surveillance as "systematic observation." As I'll explain, modern-day electronic surveillance is exactly that. We're all open books to both governments and corporations; their ability to peer into our collective personal lives is greater than it has ever been before.

The bargain you make, again and again, with various companies is surveillance in exchange for free service. Google's chairman Eric Schmidt and its director of ideas Jared Cohen laid it out in their 2013 book, *The New Digital Age*. Here I'm paraphrasing their message: if you let us have all your data, we will show you advertisements you want to see and we'll throw in free web search, e-mail, and all sorts of other services. It's convenience, basically. We are social animals, and there's nothing more powerful or rewarding than communicating with other people. Digital means have become the easiest and quickest way to communicate. And why do we allow governments access? Because we fear the terrorists, fear the strangers abducting our children, fear the drug dealers, fear whatever bad guy is in vogue at the moment. That's the NSA's justification for its mass surveillance programs; if you let us have all of your data, we'll relieve your fear.

AT Deontological Right to Privacy

Too vague to be legit

Chris DL Hunt 11, PhD Candidate in law and WM Tapp Scholar, Gonville & Caius College, University of Cambridge, “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort”, <http://queensu.ca/lawjournal/issues/pastissues/Volume37a/5-Hunt.pdf>)

The “right to be let alone” occupies a hallowed place in privacy discourse. Although the phrase was coined by Judge Cooley⁴²—who used it not to justify a right to privacy, but rather to explain why tort law regards trespass to the person as wrongful—it is now generally attributed to Warren and Brandeis, who invoked it throughout their seminal 1890 article.⁴³ The latter authors analyzed numerous cases of trespass, defamation, confidence, and especially common law copyright, and identified a latent principle of privacy—operating unarticulated—which they argued should thenceforth be protected independently, as a distinct tort.⁴⁴ This principle of privacy, expressed as a “right to be let alone”, is anchored in the more fundamental interest of an “inviolate personality”.⁴⁵ The Warren and Brandeis formulation has come under much academic criticism. The first problem is its vagueness.⁴⁶ Because neither the “right to be let alone” nor the concept of “inviolate personality” is adequately defined,⁴⁷ the article gives no practical or conceptual guidance on the scope of the right.⁴⁸ A related criticism is that the phrase “right to be let alone” itself appears to be less a definition of privacy than simply a description of one example of it.⁴⁹

Privacy is too sweeping/broad

Chris DL Hunt 11, PhD Candidate in law and WM Tapp Scholar, Gonville & Caius College, University of Cambridge, “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort”, <http://queensu.ca/lawjournal/issues/pastissues/Volume37a/5-Hunt.pdf>, AB)

The second criticism, stemming from the above mentioned vagueness, is that this conception of privacy is overly broad. As Gavison explains: [It] cover[s] almost any conceivable complaint anyone could ever make. A great many instances of “not letting people alone” cannot readily be described as invasions of privacy. Requiring that people pay their taxes or go into the army, or punishing them for murder, are just a few . . . examples.⁵⁰ This conceptual over breadth is evident in how the “right to be let alone” has been used in American constitutional jurisprudence, where it is often equated with privacy⁵¹ and is taken to encompass the right to “live one’s life as one chooses”.⁵² This includes the “privilege of an individual to plan his own affairs . . . [and] do what he pleases”.⁵³ This “substantive”⁵⁴ conception of privacy confers a zone of decisional autonomy, and currently forms the basis for the right to abortion in American constitutional law.⁵⁵ It has been much criticized as being really an “assertion of liberty per se [rather] than one of privacy”.⁵⁶ A narrower and clearer definition of privacy is needed.

People have plenty of privacy

Carolyn Doyle & Mirko Bagaric 5, “The right to privacy: appealing, but flawed”, The International Journal of Human Rights, Volume 9, Issue 1, 2005, p. 3-36, Taylor & Francis Online, AB)

The existence of a right to privacy is dubious. Even if such a right does exist it is not a very important right, ranking well down in the list of interests that are conducive to human flourishing. Privacy proponents have been incapable of explaining the foundation for such a right and why it should enjoy a high

level of legal protection. The present level of protection of privacy in specific contexts both through legislation and at common law is adequate, particularly in view of the recourse now available under the doctrine of confidence in relation to public disclosures of intimate information. The right to privacy can be seen as a late-twentieth/early twenty-first century First World invention, indicative of a highly individualistic society fearful of the capabilities of the technology it has developed. However the alarmist rhetoric of privacy advocates who proclaim the imminent demise of privacy does not match reality: in fact, it is arguable that citizens in Western societies enjoy a level of de facto privacy unprecedented in history.¹⁵⁸ As to the threats posed by the monitoring capabilities of the new information technologies, it is now becoming apparent that technology itself can provide the means to counter them.¹⁵⁹ The current legal focus and level of discussion concerning the right of privacy is a clear illustration of the human propensity for losing perspective. It follows that very few interests should be subjugated to the right of privacy.

Privacy can't be restored – technological and corporate invasions happen all the time.

Lewis 2014

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies. Previously, US Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service.
“Underestimating Risk in the Surveillance Debate” - Center For Strategic & International Studies - Strategic Technologies Program – December - <http://csis.org/publication/underestimating-risk-surveillance-debate>

On average, there are 16 tracking programs on every website.⁴ This means that when you visit a website, it collects and reports back to 16 companies on what you've looked at and what you have done. These programs are invisible to the user. They collect IP address, operating system and browser data, the name of the visiting computer, what you looked at, and how long you stayed. This data can be made even more valuable when it is matched with other data collections. Everything a consumer does online is tracked and collected. There is a thriving and largely invisible market in aggregating data on individuals and then selling it for commercial purposes. Data brokers collect utility bills, addresses, education, arrest records (arrests, not just convictions). All of this data is recorded, stored, and made available for sale. Social networking sites sell user data in some anonymized form so that every tweet or social media entry can be used to calculate market trends and refine advertising strategies. What can be predicted from this social media data is amazing—unemployment trends, disease outbreaks, consumption patterns for different groups, consumer preferences, and political trends. It is often more accurate than polling because it reflects peoples' actual behavior rather than the answer they think an interviewer wants to hear. Ironically, while the ability of U.S. agencies to use this commercial data is greatly restricted by law and policy, the same restrictions do not apply to foreign governments. The development of the Internet would have been very different and less dynamic if these business models had not been developed. They provide incentives and financial returns to develop or improve Internet services. There is an implicit bargain where you give up privacy in exchange for services, but in bargains between service providers and consumers, one side holds most of the cards and there is little transparency. But the data-driven models of the Internet mean that it is an illusion to think that there is privacy online or that NSA is the only entity harvesting personal data.

Privacy is an unobtainable right – it always trades off with itself leading to circumvention of the plan's efforts

David Pozen 15, Associate Professor of Law at Columbia University, 6/28/15,

83 U. CHI. L. REV. __ (2015), “Privacy-Privacy Tradeoff,”

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2624281

Privacy clashes with important social values. We are told as much all the time.¹ Commentators struggle to reconcile privacy and security,² privacy and efficiency,³ privacy and technological innovation,⁴ and privacy and free speech, among other (real or imagined) antinomies. Privacy is constantly being juxtaposed with competing goods and interests, balanced against alternative needs and demands. Legal and policy debates about privacy revolve around these tradeoffs.

But privacy also clashes with itself. That is to say, in myriad social and regulatory contexts, enhancing or preserving privacy along a certain dimension may entail compromising privacy along another dimension. If they wish to be more analytically rigorous, theorists and decisionmakers must take such privacy-privacy tradeoffs into account. If they wish to advance the cause of privacy, civil libertarians must do the same.

Privacy-privacy tradeoffs come in a variety of flavors. Sometimes they are unexpected and unwanted. When EU citizens began exercising their right to be forgotten last year and flooded Google with “delete me” requests, the deleted links quickly reappeared—in more concentrated form—on a website devoted to documenting Internet censorship.⁷ Other times, privacy-privacy tradeoffs are consciously cultivated and promoted. The Transportation Security Administration’s PreCheck program invites travelers to “volunteer personal information in advance” if they wish “to leave on their shoes, belts and light outerwear and keep their laptops in their bags.”⁸ Enhanced governmental access to your data can be traded for reduced access to your body and belongings.

In many cases, privacy-privacy tradeoffs simply follow from scarce resources and opportunity costs. A tenant on a fixed budget who spends money soundproofing her walls will have less to spend on mending her window curtains or protecting her online identity. Alternatively, these tradeoffs may be caused by behavioral responses and dynamic feedback effects. Increasing airline-passenger privacy levels from X at Time 1 to a multiple of X at Time 2 may increase the odds of a terrorist attack, with the consequence that passengers’ privacy levels will be reduced to a fraction of X at Time 3. In still other cases, risk is redistributed across different aspects or bearers of privacy. By establishing a forensic DNA database, law enforcement officials may impair the privacy of everyone whose DNA is included but protect the privacy of a smaller group who will not be needlessly investigated for the crimes of others. By stripping its analysts of “any privacy or anonymity when they look at [collected] data,”⁹ an intelligence agency may deter them from exceeding their investigative mandates and thereby secure a measure of privacy for the rest of society—or at least for the analysts’ love interests.¹⁰

Deontological theories of privacy rights are baseless and guaranteed to fail

Carolyn Doyle & Mirko Bagaric 5, “The right to privacy: appealing, but flawed”, The International Journal of Human Rights, Volume 9, Issue 1, 2005, p. 3-36, Taylor & Francis Online, AB)

Non-consequentialist (rights) theories. The leading contemporary non-consequentialist theories are those which are framed in the language of rights. Following the Second World War, there has been an immense increase in ‘rights talk’,⁸¹ both in the number of supposed rights and in total volume. Rights doctrine has progressed a long way since its original aim of providing ‘a legitimisation of ... claims against tyrannical or exploiting regimes’.⁸² As Tom Campbell points out: The human rights movement is based on the need for a counter-ideology to combat the abuses and misuses of political authority by those who invoke, as a justification for their activities, the need to subordinate the particular interests of individuals to the general good.⁸³ There is now, more than ever, a strong tendency to advance moral claims and arguments in terms of rights.⁸⁴ Assertion of rights has become the customary means to express our moral sentiments. As Sumner notes: ‘There is virtually no area of public controversy in which rights are not to be found on at least one side of

the question – and generally on both.⁸⁵ The domination of rights talk is such that it is accurate to state that human rights have at least temporarily replaced maximising utility as the leading philosophical inspiration for political and social reform.⁸⁶ Despite the dazzling veneer of deontological rights-based theories, when examined closely they are unable to provide convincing answers to central issues such as: what is the justification for rights? How can we distinguish real from fanciful rights? Which right takes priority in the event of conflicting rights? Such intractable difficulties stem from the fact that contemporary rights theories lack a coherent foundation. It has been argued that attempts to ground rights in virtues such as dignity, concern or respect are unsound and that they fail to provide a mechanism for moving from abstract ideals to concrete rights.⁸⁷ A non-consequentialist ethic provides no method for distinguishing between genuine and fanciful rights claims and is incapable of providing guidance regarding the ranking of rights in the event of a clash. In light of this, it is not surprising that the number of alleged rights has blossomed exponentially since the fundamental protective rights of life, liberty and property were advocated in the seventeenth and eighteenth centuries. Today, all sorts of dubious claims have been advanced on the basis of rights: for example, ‘the right to a tobacco-free job’, the ‘right to sunshine’, the ‘right of a father to be present in the delivery room’, the ‘right to a sex break’,⁸⁸ and even ‘the right to drink myself to death without interference’.⁸⁹ Novel rights are continually evolving and being asserted. A good example is the recent claim by the Australian Prime Minister (in the context of the debate concerning the availability of IVF treatment to same-sex couples or individuals) that each child has the right to a mother and father. In a similar vein, in light of the increasing world oil prices, it has been declared that this violates the right of Americans to cheap gasoline. In England, the Premier League has been accused of violating the right of football club supporters to an F.A. Cup ticket. Due to the great expansion in rights talk, rights are now in danger of being labelled as mere rhetoric and are losing their cogent moral force. Or, as Sumner points out, rights become an ‘argumentative device capable of justifying anything [which means they are] capable of justifying nothing’.⁹⁰ Therefore, in attempting to uncover the scope and content of ‘emerging’ rights such as the right to privacy it is normally unhelpful to consider the issue from the perspective of a deontological rights-based normative theory. Against the background of such a theory, proponents of the right can simply assert the existence of a right to privacy and equally validly, opponents can assert a ‘right to know’. An impasse is then reached because there is no underlying ideal that can be invoked to provide guidance on the issue. As with many rights, the victor may unfortunately be the side which simply yells the loudest.⁹¹ This may seem to be unduly dismissive of rights-based theories and pay inadequate regard to the considerable moral reforms that have occurred against the backdrop of rights talk over the past half-century. There is no doubt that rights claims have proved to be an effective lever in bringing about social change. As Campbell correctly notes, rights have provided ‘a constant source of inspiration for the protection of individual liberty’.⁹² For example, recognition of the (universal) right to liberty resulted in the abolition of slavery; more recently the right of equality has been used as an effective weapon by women and other disenfranchised groups. For this reason, it is accepted that there is an ongoing need for moral discourse in the form of rights. This is so even if deontological rights-based moral theories (with their absolutist overtones) are incapable of providing answers to questions such as the existence and content of proposed rights, and even if rights are difficult to defend intellectually or are seen to be culturally biased. There is a need for rights-talk, at least at the ‘edges of civilisation and in the tangle of international politics’.⁹³ Still, the significant changes to the moral landscape for which non-consequentialist rights have provided the catalyst must be accounted for. There are several responses to this. First, the fact that a belief or judgment is capable of moving and guiding human conduct says little about its truth – the widespread practice of burning ‘witches’ in medieval times being a case in point. Secondly, at the descriptive level, the intuitive appeal of rights claims, and the absolutist and forceful manner in which they are expressed, has heretofore been sufficient to mask fundamental logical deficiencies associated with the concept of rights. Finally, and perhaps most importantly, we do not believe that there is no role in moral discourse for rights claims, simply that the only manner in which rights can be substantiated is in the context of a consequentialist ethic.⁹⁴

Privacy is not an absolute right- government must violate it to function

Robert Gerstein, Professor of Political Science, UCLA, PHILOSOPHICAL DIMENSIONS OF PRIVACY, Ferdinand Schoeman, ed., 1984, p.247-8.

If privacy is a constitutional right it is immediately apparent that it cannot be an absolute right. Governments have always compelled people to disclose some sorts of information about themselves, and it is hard to see how they could get along effectively without the ability to do so. If the argument for privacy is made so broadly as to sweep away tax returns, accident reports, and the capacity to compel testimony on personal matters in civil cases, for example, it must surely be rejected. The right of privacy cannot be understood as embodying the rule that "privacy may never be violated."

Philosophers disagree over the value of privacy

Silas Wasterstrom, law professor, GEORGETOWN LAW JOURNAL, October 1998, pp. 59-60

But there are serious obstacles to using moral philosophy to justify fourth amendment law. First, a growing number of philosophers have come to doubt that the techniques of moral philosophy can ever succeed in providing neutral ground that will allow us to escape our own beliefs and desires or, indeed, that this is even a coherent goal. Second, even if philosophers themselves were more self-confident, judges still would have to decide which philosophers to listen to. Unfortunately, moral philosophers who have thought about privacy do not speak with one voice. On the contrary, they are hopelessly divided about what privacy is; about whether it is a value in itself, or whether it is only valuable because of its consequences; about whether respect for privacy is a facet of respect for personhood; about what claims the word privacy encompasses; and even about whether it describes a coherent concept at all. A judge who is determined to make use of what moral philosophy has to offer would have to evaluate and choose between these conflicting positions. Moral philosophy may offer ways to think about the choice more clearly. But it does not offer a technique for making the choice "objectively" or in a fashion uncontaminated by the viewpoint of the person doing the choosing.

Legal interests different from philosophical privacy interests; security must be balanced.

Silas Wasterstrom, law professor, GEORGETOWN LAW JOURNAL, October 1998, p. 60-1

Moreover, even if we overlook the disagreements that divide moral philosophers and assume that judges could separate good moral philosophy from bad without reference to their own preferences, it still is doubtful that the writings of moral philosophers provide much that is useful to settle contemporary disputes about the meaning of the fourth amendment. Most of these writings are on an extremely high level of generality. Philosophers have argued at length about what "privacy" means, and about the justifications for treating it as a value or a right. In contemporary legal discourse, however, it is uncontroversial that some value should be

attached to privacy. The important issue in most fourth amendment cases is the balance that should be struck between that value and competing concerns, such as interests in effective law enforcement and in decisionmaking based upon full information. Beyond the injunction to take privacy seriously, moral philosophers have little to say about this crucial question.

AT Mass Surveillance

No NSA abuses – checks the internal link

Lowry 2015,

Rich, Editor, the National Review, 5-27-2015, "Lowry: NSA data program faces death by bumper sticker," Salt Lake Tribune,

<http://www.sltrib.com/csp/mediapool/sites/sltrib/pages/printfriendly.csp?id=2557534>

You can listen to orations on the NSA program for hours and be outraged by its violation of our liberties, inspired by the glories of the Fourth Amendment and prepared to mount the barricades to stop the NSA in its tracks — and still have no idea what the program actually does. That's what the opponents leave out or distort, since their case against the program becomes so much less compelling upon fleeting contact with reality. The program involves so-called metadata, information about phone calls, but not the content of the calls — things like the numbers called, the time of the call, the duration of the call. The phone companies have all this information, which the NSA acquires from them. What happens next probably won't shock you, and it shouldn't. As Rachel Brand of the Privacy and Civil Liberties Oversight Board writes, "It is stored in a database that may be searched only by a handful of trained employees, and even they may search it only after a judge has determined that there is evidence connecting a specific phone number to terrorism." The charge of domestic spying is redolent of the days when J. Edgar Hoover targeted and harassed Martin Luther King Jr. Not only is there zero evidence of any such abuse, it isn't even possible based on the NSA database alone. There are no names with the numbers. As former prosecutor Andrew C. McCarthy points out, whitepages.com has more personal identifying information. The NSA is hardly a rogue agency. Its program is overseen by a special panel of judges, and it has briefed Congress about its program for years.

Focus on surveillance as information gathering ignores content of the surveillance – causes restriction which turns the case

Chris DL Hunt 11, PhD Candidate in law and WM Tapp Scholar, Gonville & Caius College, University of Cambridge, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort", <http://queensu.ca/lawjournal/issues/pastissues/Volume37a/5-Hunt.pdf>, AB)

Conceiving of privacy as a claim to control personal information gets us very close to understanding its essence.⁶³ Simply put, we intuit privacy as a claim to control, and this intuition is reflected in the social norms that surround us.⁶⁴ We feel that this conception of privacy is the reason someone has a moral claim to keep the contents of his diary secret; and reasonable people reflect that understanding by respecting this right, or at least by intuiting that reading a person's diary violates something we all sense to be private. Furthermore, as I explain in section two, the claim to control personal information is closely associated with the values underpinning privacy (especially the values of dignity and autonomy). However, there are three significant problems with control-based definitions. The first problem is that insofar as they concentrate on information,⁶⁵ they are too restricted.⁶⁶ We all recognize, intuitively, that privacy can be invaded even where information is not communicated, such as where a peeping tom trains his telescope on a woman's bedroom to watch her undress. A definition of privacy that fails to capture such physical intrusions simply lacks intuitive coherence. It might be suggested that informational control can capture this example, the argument being that the tom has in fact received information about his victim (in the sense that he has learned what she looks like without clothes). This argument is problematic however, owing to its artificiality. Parker responds to it by asking us to imagine that the tom and the woman are lovers.⁶⁷ Is it still sensible to regard the tom, when he sneaks a peak at his lover through the window after leaving her side, as obtaining information about what she looks like naked—information he already has?⁶⁸

If the answer is no, then such peeping falls outside this definition of privacy, resulting in an intuitive under-inclusiveness. Even if we strain and answer yes because the man has learned that his lover remains undressed or is in a different pose, this information-based approach clearly fails to capture the true essence of the invasion.⁶⁹ It is not that information has been acquired but rather that she is being “looked at . . . against her wishes”.⁷⁰ Wacks explains: What is essentially in issue in cases of intrusion is the frustration of the legitimate expectations of the individual that he should not be seen or heard in circumstances where has not consented to or is unaware of such surveillance. The quality of the information thereby obtained, though it will often be of an intimate nature, is not the major objection.⁷¹ These observations lead to a related point. As Moreham has convincingly argued, by failing to appreciate the true essence of the complaint, this information-based approach necessarily fails to appreciate the gravity of the privacy violation itself, and therefore must logically undervalue it.⁷² This is because, to be internally coherent, the information-based approach must regard the information learned as the only relevant factor when assessing the gravity of an invasion; but if we consider Parker’s peeping lover example, we see that very little new information has in fact been communicated. Consequently, as the information learned was negligible, so too must be the violation of privacy. Such an approach is clearly inadequate if we regard this example as a serious violation of privacy.⁷³ So, the first major problem with the “control over information” approaches is their narrowness, in that they fail to adequately capture what we intuit—that physical intrusions violate privacy for reasons unrelated to, and irrespective of, any information that may also be gleaned (or subsequently published) as a consequence of an intrusion. It is the looking (or listening or touching) itself, not the acquisition of information, that is offensive to our intuitive sense of privacy. Furthermore, as I explain in section two, the values underpinning privacy, and the reasons why it is important, strongly support including a physical intrusion dimension in our definition. Before moving to the remaining criticisms, it is worth noting that there is widespread academic⁷⁴ and law commission⁷⁵ recognition, and some judicial recognition, that physical intrusions lie at the conceptual core of privacy.

Google and Yahoo developing encryption-based email that they can't even access

Korea Times, August 10, 2014, Google, Yahoo collaborating on spy-free email,
http://www.koreatimes.co.kr/www/news/nation/2015/02/100_162637.html DOA: 3-21-15

Google and Yahoo are working together to give emails a post-Snowden update. The Internet giants confirmed they were collaborating to develop a secure new email system by next year that could make it nearly impossible for government officials and hackers to read users' messages. Google and Yahoo claim that even they won't be able to decrypt the messages under the new system. Shocking revelations by ex-National Security Agency contractor Edward Snowden last year have elevated Internet users' awareness on government surveillance and data breaches. **Yahoo has altered its email process to require users to type encryption messages in a separate window, which prevents anyone, including Yahoo, from reading the messages as they are typed, the Wall Street Journal reports. Google also has taken a similar measure by encouraging website developers to make their sites secure for visitors by using site encryption.**

AT NSA Spying Violates Privacy

Surveillance programs do not violate rights, security key to liberty

Gen. Keith B. Alexander is the former director of the National Security Agency. John "Chris" Inglis is the former deputy director, June 5, USA Today, <http://www.usatoday.com/story/opinion/2014/06/05/nsa-spying-foreign-governments-security-column/9969625/>

NSA's authorities and processes are complex. But the issues are not complicated:

- **NSA adheres to the requirements set out in the Fourth Amendment and respects the privacy of U.S. persons.**
- **NSA does not hide information from its overseers. The agency welcomes external oversight and accountability as the necessary price of the authorities delegated to NSA.**
- **NSA employs a broad range of directed and self-imposed controls to limit its activities to those explicitly authorized. And it regularly reports to its oversight bodies, which operate across all three branches of government.**
- **NSA does not set its own agenda. Everything that it does is in response to specific, vetted foreign intelligence requirements. Moreover, NSA does not collect everything. There must be a valid foreign intelligence purpose. Period.**

NSA has played strictly by the rules, supporting both the spirit and the letter of the law. As President Obama said in his January 17 speech to the nation: "The men and women of the Intelligence Community, including NSA, consistently follow protocols designed to protect the privacy of ordinary people. They are not abusing authorities in order to listen to your private phone calls or read your e-mails." Last year, an Independent Review Group appointed by the president also determined that NSA followed the rules that were established by all three branches of government. This is not to say the programs are perfect.

Modifications have been made over the years and will continue to be made in the future as a result of this public debate. For example, the full-time Civil Liberties and Privacy Officer at NSA, put in place by President Obama, will help produce greater trust between the American people and NSA. **Liberty and security are not competing interests. We have always believed the two are co-dependent. We can't have liberty without security. Security without liberty is of little value. We need to constantly ensure that our government is vigilant about protecting each of them.**

AT NSA Surveillance Violates Privacy

NSA sees way less than 1% of web traffic

MailOnline, August 12, 2013

NSA claims it only reviews 0.0004 percent of Internet traffic on a daily basis,
<http://www.dailymail.co.uk/news/article-2390604/NSA-claims-reviews-00004-percent-Internet-traffic-daily-basis.html>

The National Security Agency made the claims in a rare, publicly-released document defending its surveillance programs. The seven-page document was released late Friday. NSA denies claims that it has used foreign partners to circumvent U.S. laws. **The NSA has claimed in a publicly-released document that it only reviews 0.0004% of Internet traffic on a daily basis.** The seven-page document, titled 'The National Security Agency: Missions, Authorities, Oversight and Partnerships,' was released late Friday. **It compares the amount of Internet data that the NSA collects to the size of a dime on a basketball court.** According to figures published by a major tech provider, **the Internet carries 1,826 Petabytes of information per day.** In its foreign intelligence mission, **NSA touches about 1.6% of that,' the agency states. 'However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission - that's less than one part in a million.** 'Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.' The NSA denies claims that it has used foreign partners to get around U.S. laws.

NSA privacy violations minuscule

The New York Times, August 17, 2013

N.S.A. Calls Violations Of Privacy 'Minuscule', http://www.nytimes.com/2013/08/17/us/nsa-calls-violations-of-privacy-minuscule.html?_r=0, p. 12

WASHINGTON -- The top National Security Agency official charged with making sure analysts comply with rules protecting the privacy of Americans pushed back on Friday against reports that the N.S.A. had frequently violated privacy rules, after the publication of a leaked internal audit showing that there had been 2,776 such "incidents" in a one-year period. The official, **John DeLong, the N.S.A. director of compliance, said that the number of mistakes by the agency was extremely low compared with its overall activities. The report showed about 100 errors by analysts in making queries of databases of already-collected communications data; by comparison, he said, the agency performs about 20 million such queries each month.** Mr. DeLong, speaking to reporters on a conference call, also argued that **the overwhelming majority**

of the violations were unintentional human or technical errors and that the existence of the report showed that the agency's efforts to detect and correct violations of the rules were robust. He said the number of willful errors was "minuscule," involving a "couple over the past decade."

Government can't indiscriminately sift through data

The Christian Science Monitor, July 22, 2013, How will Obama defend secret NSA program in court? Letter offers clue.; The ACLU is challenging the NSA's secret data-collection program in court. The Obama administration responded with a letter making its case for why the program is constitutional and necessary, <http://www.csmonitor.com/USA/Justice/2013/0722/How-will-Obama-defend-secret-NSA-program-in-court-Letter-offers-clue>

The Justice Department disagrees with those assessments. The letter, by David Jones, an assistant US attorney, argues that the program's checks and balances are adequate. For example, **the government may not eavesdrop on anyone's phone calls or record anything participants say. All it can do is collect phone numbers making and receiving certain calls, as well as the date, time, and duration of each call - the so called "metadata." Even then, the letter continues, "the Government is prohibited ... from indiscriminately sifting through the data. The data-base may only be queried for intelligence purposes by NSA analysts where there is a reasonable, articulable suspicion ("RAS"), based on specific facts. If the government wants to take a closer look, any data gleaned must be associated with people or phone numbers already identified and approved by the secret Foreign Intelligence Surveillance Court.** In 2012, the letter revealed, **the court approved fewer than 300 "query terms" that would allow intelligence analysts to pursue a phone call further. These protocols are overseen by the Justice Department and intelligence officials, and congressional intelligence committees are briefed regularly. "Thus, the program has been approved and is rigorously overseen by all three branches of the Government." For these reasons, the program " is fully consistent with the Fourth Amendment," states the letter. "Most fundamentally, the program does not involve 'searches' of plaintiffs' persons or effects, because the collection of ... metadata from the business records of a third-party telephone service provider, without collecting the contents of plaintiffs' communications, implicates no 'legitimate expectation of privacy' that is protected by the Constitution."**

Extensive oversight of surveillance programs

Deputy Attorney General James **Cole July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs" https://www.hsl.org/?view&did=741931**

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

JAMES COLE: Thank you, Mr. Chairman, Mr. Ranking Member, members of the committee, for inviting us here today to speak about the 215 business records program and section 702 of FISA.

With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance. First of all, both programs are conducted under public statutes passed and later reauthorized by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of government play a significant role in the oversight of these programs. The judiciary, through the Foreign Intelligence Surveillance Court plays a role in authorizing the programs and overseeing compliance. The executive branch conducts extensive internal reviews to ensure compliance. And Congress passes the laws, oversees our implementation of those laws and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. The 215 program involves the collection of metadata from telephone calls. These are telephone records maintained by the phone companies. They include the number the call was dialed from, the number the call was dialed to, the date and time of the call and the length of the call. The records do not include the names or other personal identifying information. They do not include cell site or other location information. And they do not include the content of any phone calls. These are the kinds of records that under long-standing Supreme Court precedent are not protected by the Fourth Amendment. The short court order that you have seen published in the newspapers only allows the government to acquire the phone records. It does not allow the government to access or use them. The terms under which the government may access or use the records is covered by another, more detailed court order that the DNI declassified and released today. That other court order, called the primary order, provides that the government can only search the data if it has reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations. The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented. The document of the analyst's justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance. In the criminal context, the government could obtain the same types of records with a grand jury subpoena without going to the court. But here we go to the court every 90 days to see the court's authorization to collect the records. In fact, since 2006 the court has authorized the program on 34 separate occasions involving 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems. And if there have been, the court will take a very hard look and make sure that we have corrected those problems. As we have explained before, the 11 judges on the FISA court are far from a rubber stamp. Instead, they review all of our pleadings thoroughly, they question us. And they don't approve an order until they are satisfied that we have met all statutory and constitutional requirements. In addition to the judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with

the 215 programs, we would report those to the two committees right away. Any significant interpretations by the FISA court would likewise be reported to the committees under our statutory obligations, including opinions of any significant interpretation, along with any of the court orders that go with that. **In addition, Congress plays a role in reauthorizing the provision** under the -- under which the government carries out this program, and has done so since 2006. Section 215 of the Patriot Act has been renewed several times since the program was initiated, including most recently for an additional four years in 2011. In connection with those recent renewals, the government provided a classified briefing paper to the House and Senate Intelligence Committees, to be made available to all members of Congress. The briefing paper, and a second updated version of it, set out the operation of the programs in detail, explained that the government and the FISA court had interpreted the Section 215 authorization to authorize bulk collection of telephone metadata and stated that the government was in fact collecting such information. The DNI also declassified and released those two paper today. We also made offers to brief any member of the 215 program. And the availability of the paper and the opportunity for oral briefings were communicated through dear colleagues letters issued by the chairs of the intelligence committees to all members of Congress. Thus, **although we could not talk publicly about the program at the time, since it was properly classified, the executive branch took all reasonable, available steps to ensure that members of Congress were appropriately informed about the programs when they renewed it.** I

AT Nazi's Violated Privacy

US isn't try to establish a Nazi state

Alan Dershowitz, Harvard Law School, May 5, 2014, The Atlantic, "No one opposes all surveillance;; false equivalence on the NSA,
<http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-dershowitz/361694/>

What are those motives? Why would the Obama Administration continue this policy of surveillance after being briefed? Was it because President Obama has some sinister motive that he won't tell anybody about for gathering this information and is only using terrorism as a pretext the way the Nazis in Germany used the Reichstag fire as a way of suppressing civil liberties? I don't believe that.

AT Constitutional Violation

NSA programs don't violate the Fourth Amendment because the information has been given to a third-party.

Herman & Yoo, 2014

Yoo, John, law professor at the University of California, Berkeley, and a visiting scholar at the American Enterprise Institute and Arthur Herman, senior fellow at Hudson Institute. "A Defense of Bulk Surveillance." National Review 65 (2014): 31-33.

Considering the millions of phone numbers making billions of phone calls that year and every year, these levels of surveillance can hardly be considered a major intrusive system. But what about the program's constitutionality and alleged violation of the Fourth Amendment? The Fourth Amendment does not protect some vague and undefined right to privacy. Instead, it declares: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause." The Constitution protects only the privacy of the "person," the home, and "papers and effects," which are usually located in the home. It does not reach information or things that we voluntarily give up to the government or to third parties outside of the home or our persons. The Fourth Amendment also does not make such information absolutely immune—it is still subject to search if the government is acting reasonably or has a warrant. These basic principles allow the government to search through massive databases of call and e-mail records when doing so is a reasonable measure to protect the nation's security, which is its highest duty.

AT Warrant Requirements Meant to Protect Privacy

Searches mean to defend against military-style terror attacks do not require warrants

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 920-1

Even if constitutional privacy interests were thought to extend to telephone metadata or to foreign e-mails, the Fourth Amendment's warrant requirement still would not apply because the NSA searches seek to prevent military attacks, not garden-variety criminal activity. As observed earlier, every lower court to examine the question has found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement. Though, admittedly, the Supreme Court has never ruled on the question, it has suggested in dicta that roadblocks and dragnets to stop a terrorist bombing in an American city would not need to meet the warrant requirement's demand for individualized suspicion.

This approach is fully consistent with the Supreme Court's recent Fourth Amendment cases. Not all searches require a warrant. Rather, as the Court found in a 1995 case upholding random drug testing of high school athletes, "as the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" When a passenger enters an airport, government employees search his belongings and subject him to an x-ray-- undoubtedly a search--without a warrant. When travelers enter the country, customs and immigration officials can search their baggage and sometimes their persons without a warrant. Of course, when law enforcement undertakes a search to discover evidence of criminal wrongdoing, reasonableness generally requires a judicial warrant. But when the government's conduct is not focused on law enforcement, a warrant is unnecessary. A warrantless search can be constitutional, the Court has said, "'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"

A search must be "reasonable" under the circumstances. What does "reasonable" mean? The Court has upheld warrantless searches to reduce deaths on the nation's highways, to maintain safety among railway workers, and to ensure that government officials were not using drugs. In these cases, the "'importance of the governmental interests'" outweighed the "'nature and quality of the intrusion on the individual's Fourth Amendment interests.'" It is hard to imagine that any of these situations are more important than protecting the nation from a direct foreign attack in wartime. "It is obvious and unarguable," the Supreme Court has observed several times, "that no governmental interest is more compelling than the security of the Nation." It is the duty of the President to respond to attacks on the territory and people of the United States, and Congress confirmed the President's authority to use force after September 11. The extraordinary circumstances of war require that the government seek specific information relevant to possible attacks on Americans, sometimes in situations where obtaining a warrant is not practical.

Before the September 11 attacks, the Supreme Court observed that the Fourth Amendment's warrant requirement would probably not apply to the special circumstances created by a potential terrorist attack. "[T]he Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route." To be sure, this case, *City of Indianapolis v. Edmond*, challenged the constitutionality of a highway checkpoint program that searched cars for illegal drugs rather than for terrorists. And in *Edmond*, the Court found that the checkpoints violated the Fourth Amendment protection against search and seizure because the police were searching for drugs for the purpose of "crime control" and "the ordinary enterprise of investigating crimes." But the Court still observed that some warrantless searches were acceptable in the emergency situation of a possible terrorist attack, in which the "need for such measures to ensure public safety can be particularly acute." If the Supreme Court has found that searches for border and airport control present special needs that do not call for a warrant, a court would be hard pressed to deny that searches to find foreign terrorists bent on attacking the United States fall within the same category.

If national security searches do not require a warrant, it might be asked why FISA is even necessary. FISA offers the executive branch a deal. If a President complies with the process of obtaining a FISA warrant, courts will likely agree that the search was reasonable and will admit its fruits as evidence in a criminal case. FISA does not create the power to authorize national security searches. Rather, it describes a safe harbor that deems searches obtained with a warrant reasonable under the Fourth Amendment. If a President proceeds with a search under his own authority rather than under FISA or under ordinary criminal procedure, he takes his chances. A court might refuse to admit evidence in any future proceeding that had been obtained without a warrant, or even allow the target to sue the government for damages. n96 Then again, it might not.

FISA ultimately cannot limit the President's powers to protect national security through surveillance if those powers stem from his unique Article II responsibilities. Intercepting enemy communications has long been part of waging war; indeed, it is critical to the successful use of force. The U.S. military cannot attack or defend to good effect unless it knows where to aim. America has a long history of conducting intelligence operations to obtain information on the enemy. General Washington used spies extensively during the Revolutionary War and as President established a secret fund for spying that existed until the creation of the CIA. President Lincoln personally hired spies during the Civil War, a practice the Supreme Court upheld. In both World Wars I and II, Presidents ordered the interception of electronic communications leaving the United States. Some of America's greatest wartime intelligence successes have involved signals intelligence (SIGINT), most notably the breaking of Japanese diplomatic and naval codes during World War II, which allowed the U.S. Navy to anticipate the attack on Midway Island. SIGINT is even more important in this war than in those of the last century. Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them. The primary way to stop those attacks is to find and stop al Qaeda operatives who have infiltrated the United States. The best way to find them is to intercept their electronic communications entering or leaving the country.

AT Rights General

Anti-terror measures won't lead to authoritarianism and security is a precondition for freedom

Paul Rosenzweig, Heritage Senior Legal Research Fellow, 2004

["Preventive Detention and Actionable Intelligence," 9/16, w/ James Jay Carafano, <http://www.heritage.org/Research/HomelandDefense/lm13.cfm>]

The response to this criticism is threefold: First, the criticism blinks reality. We already have incomplete and irregular forms of preventive detention because it is a necessity. We advance liberty when we regularize the practice, cabin it to narrow circumstances, and use it sparingly. Second, as detailed above, other countries (such as the United Kingdom) have managed to adopt very limited forms of preventive detention without becoming noticeably “unfree” or “authoritarian.” Adoption of similar legal forms in the United States will not render us an authoritarian regime either. Finally, and most important, to reject preventive detention in those rare circumstances in which it is necessary is to exalt liberty at the expense of security. The founding of the American Republic was for the purpose of constructing a political system of ordered liberty. It simply cannot be right to unilaterally prefer liberty. Liberty is not an absolute value; it depends upon security (both personal and national) for its exercise. As Thomas Powers has written: “In a liberal republic, liberty presupposes security; the point of security is liberty.” The growth in danger from the consequences of the failure to stop terrorism necessitates altering our tolerance for governmental order. More fundamentally, our goal should be to maximize both order and liberty.

The foundation of rights is the promotion of the public good

John Hasnas, professor of Business Ethics, Georgetown, NORTHWESTERN UNIVERSITY LAW REVIEW, 1995, p. 916

Rights are conferred (and their correlating duties imposed) with the direct or immediate purpose of promoting the general good; (as, for example, tie rights of judges and other political subordinates): and rights are conferred indirectly to the same extensive purpose, although their proximate end be the advantage of the parties entitled, or of other determinate parties for whom they are conferred in trust.

Constitutional Rights are not trump cards; policy goals can outweigh the interests of rights & no rights are absolute under the Constitution

Harvey, J.D., Yale Law School, '02 (Philip Harvey, "Human Rights and Economic Policy Discourse: Taking Economic And Social Rights Seriously", Spring, 2002, 33 Colum. Human Rights L. Rev. pp. 370-1)

A view frequently expressed by human rights advocates is that valid rights should "trump" other policy goals, but I argue that this prescription, if taken at face value, is inadequate. A genuine trump outweighs even the highest valued card in another suit, but rights-based claims are rarely treated that way. They are given added weight, but not a genuinely trumping value. For example, in American constitutional jurisprudence, even fundamental rights may be infringed; however, a "compelling state interest" is required to justify such actions. What I argue is needed, therefore, is not a social choice methodology that treats rights as absolute trumps, but one that treats them with appropriate deference. The level of deference owed a particular right may vary with the importance of the ultimate interests it protects and with the nature of the countervailing interests that oppose it. Whether the balance between human rights protection and other policy goals is struck appropriately in particular instances may not be easy to determine. It certainly will not be demonstrable with the mathematical precision to which welfare economics aspires. The most we can expect is persuasive argument.

Turn -- Absolutism hurts rights – we get lost in moral constraints rather than being moved by real concern

Waldron, Jeremy, 1993 (Liberal Rights, Collected Papers: Cambridge Univ. Press)

I have some sympathy with this, but, as I also argue in Chapter 9, the insistence on absolutism does not make the conflicts go away; it doesn't make the situations that appear to call for trade-offs disappear. Those situations are not something that consequentialists and their fellow travelers have perversely *invented* in order to embarrass moral absolutists. It is not the theorist's fault that there are sometimes several drowning people and only one lifeguard. As I said earlier, the world turns out not to be the sort of place to which absolute moral requirements are an apt response. If we insist on the absoluteness of rights, there is a danger that we may end up with no rights at all, or, at least, no rights embodying the idea of real concern for the individuals whose rights they are. At best, we will end up with a set of moral constraints whose absoluteness is secured only by the contortions of agent-relativity, that is, by their being understood not as concerns focused on those who may be affected by our actions but as concerns focused on ourselves and integrity.

Turn -- One must divert to utilitarianism when the alternative is to let everyone die

Kateb, Professor of Politics, 1992 (George, Prof of Politics, Princeton Univ., The Inner Ocean: Individualism and Democratic Culture; Cornell University Press, p. 12)

The main point, however, is that utilitarianism has a necessary place in any democratic country's normal political deliberations. But its advocates must know its place, which ordinarily is only to

help to decide what the theory of rights leaves alone. *When may rights be overridden by government?* I have two sorts of cases in mind: overriding a particular right of some persons for the sake of preserving the same right of others, and overriding the same right of everyone for the sake of what I will clumsily call "civilization values." An advocate of rights could countenance, perhaps must countenance, the state's overriding of rights for these two reasons. The subject is painful and liable to dispute every step of the way. For the state to override is, sacrifice—a right of some so that others may keep it. the situation must be desperate. I have in mind, say, circumstances in which the choice is between sacrificing a right of some and letting a right of all be lost. The state (or some other agent) may kill some (or allow them to be killed), if the only alternative is letting every-one die. It is the right to life which most prominently figures in thinking about desperate situations. I cannot see any resolution but to heed the precept that "numbers count." Just as one may prefer saving one's own life to saving that of another when both cannot be saved, so a third party—let us say, the state—can (perhaps must) choose to save the greater number of lives and at the cost of the lesser number, when there is otherwise no hope for either group. That choice does not mean that those to be sacrificed are immoral if they resist being sacrificed. It follows, of course, that if a third party is right to risk or sacrifice the lives of the lesser for the lives of the greater number when the lesser would otherwise live, the lesser are also not wrong if they resist being sacrificed.

You are responsible for outcomes that are caused by others when you cause the others to do the outcome

Uniacke (University of Wollongong, NSW, Australia) '99

(Suzanne, Jun99, International Journal of Philosophical Studies, "Absolutely Clean Hands? Responsibility for What's Allowed in Refraining from What's Not Allowed," Vol. 7 Issue 2, p189, 21p)

We bear responsibility for the outcome of another's actions, for instance, when we provoke these actions (Iago); or when we supply the means (Kevorkian), identification (Judas), or incentive (Eve); or where we encourage another to act as he [or she] does (Lady Macbeth). Despite his disclaimer, Pilate cannot acquit himself entirely of the outcome of what others decide simply by ceding the judgment to them. In these examples agents are indirectly, partly responsible for the outcomes of what others do in virtue of something they themselves have done. But indirect, partial responsibility for what another person does can also arise through an agent's non-intervention and be grounded in intention or fault; for example, when Arthur does not prevent Brian killing Catherine, because Arthur wants Catherine dead, or because Arthur simply cannot be bothered to warn her or call the police. Of course attributions of indirect, partial responsibility can be difficult. And as far as absolutism is concerned, the relevant sense of 'brings about', outlined earlier, will sometimes be quite stretched where an agent is attributed with responsibility for what someone else does. All the same, by our non-intervention we can help bring about some things that are directly and voluntarily caused by others.

Turn -- Consequentialism affirms the unconditional value of rational beings as equals – its is the best framework; Kantian ethics faces the same dilemma of kill to save

Cummiskey, Associate Professor of Philosophy, Bates College, '96 (David, Kantian Consequentialism, New York: Oxford University Press, p. 150-1)

On the other hand, in practice, consequentialists do not defend the sacrifice of the innocent as a principle of public policy. In practice, of course, a Kantian consequentialist can and should appeal to good consequentialist reasons for limiting the use of coercion and maintaining a sphere of personal liberty. There are good consequentialist reasons for secondary principles that constrain a direct appeal to the more basic consequentialist principle. Just as honesty is typically the best policy, protecting individual rights really does advance the common good. In addition, the demands of duty are such that, as Kant would say, finite rational beings cannot be expected to fully satisfy them. We must distinguish what one should do if one can from what we should expect or demand of ourselves and others. Although consequentialists reject moral complacency and self-satisfaction, they also provide a justification for a distinction between extraordinary and ordinary compliance with duty. Thus, the Kantian consequentialist should follow the tradition, going back at least to Aquinas, "that recognizes that "human law" should externally legislate only the more harmful vices and should set its demands at a level a normally virtuous person can satisfy. Full virtue is indeed best left to the internal legislation of finite rational beings. Consequentialism thus provides an indirect justification for our intuitive conviction that we should not demand that the innocent sacrifice themselves, and also that we should not sacrifice the innocent. Kant's moral theory, however, simply does not provide a more direct and indefeasible justification for deontological constraints. In principle, a conscientious Kantian moral agent may be required to kill one in order to save two. Nonetheless, if someone is unable to do so, this may well not be grounds for reproach. Similarly, if I cannot amputate a leg to save a life-either my own or that of another-I may not be blameworthy for my failure, although it is true that I should have done the nasty deed. Still, in such a situation I must try to force my attention on the good I am doing and thereby enable myself to act. Similarly, in the highly unusual case where it would truly be best to kill some to save others, a good person should also try to focus on the lives to be saved rather than becoming fixated exclusively on those who will be killed. Nonetheless, even though sacrificing some to save others is sometimes the right thing to do, one should still feel regret and mourn the people who are lost. After all, the goal is to save each and every person; thus, one should indeed feel the loss of even one. According to Kant, the objective end of moral action is the existence of rational beings. Respect for rational beings requires that in deciding what to do, one must give appropriate practical consideration to the unconditional value of rational beings and to the conditional value of happiness. Since agent-centered constraints require a non-value-based rationale, the most natural interpretation of the demand that one give equal respect to all rational beings leads to a consequentialist normative theory. We have seen that there is no sound Kantian reason for abandoning this natural consequentialist interpretation. In particular, a consequentialist interpretation does not require sacrifices that a Kantian ought to consider unreasonable, and it does not involve doing evil so that good may come of it. It simply requires an uncompromising commitment to the equal value and equal claims of all rational beings and a recognition that in the moral consideration of conduct, one's own subjective concerns do not have overriding importance.

Security is a fundamental economic and social right

HARVARD CIVIL RIGHTS CIVIL LIBERTIES LAW REVIEW, Summer 1995, p. 589-90

The *Pratt* decision and continuing litigation typifies the way in which strict adherence to classical liberalism's understanding of freedom creates an incomplete balance between fundamental rights and the basic needs imperative to realize those rights. The court's formalistic adherence to a classical liberal view of civil and political rights obscured the public housing residents' underlying social and economic rights. By privileging the civil and political rights of residents, *Pratt* ignores their basic need for security. The legal parameters in which the *Pratt* case was decided forced public housing residents to pay for one of their most fundamental constitutional rights, the right to be free from governmental intrusion, with their basic need for security.

The risk of extinction via nuclear war outweighs all - ethics demands you evaluate consequences

Robert A. Seeley, Central Committee for Conscientious Objectors, **1986**, The Handbook of Non-Violence, p. 269-70

In moral reasoning prediction of consequences is nearly always impossible. One balances the risks of an action against its benefits; one also considers what known damage the action would do. Thus a surgeon in deciding whether to perform an operation weighs the known effects (the loss of some nerve function, for example) and risks (death) against the benefits, and weighs also the risks and benefits of not performing surgery. Morally, however, human extinction is unlike any other risk. No conceivable human good could be worth the extinction of the race, for in order to be a human good it must be experienced by human beings. Thus extinction is one result we dare not-may not-risk. Though not conclusively established, the risk of extinction is real enough to make nuclear war utterly impermissible under any sane moral code.

AT “Petro – Freedom is Absolute”

freedoms can't be absolute because freedoms contradict

Roberto Unger, CRITICAL LEGAL STUDIES, Ed. Hutchinson, 1984, p. 26

The theory of formal freedom suffers from the same dilemma as the morality of reason, of which it is the political equivalent. Take Kant's universal principle of right, “Every action is right that in itself or in its maxim is such that the freedom of the will of each can coexist together with the freedom of the will of everyone according to a universal law.” When this proposition is left in its abstract form, it seems impossible to derive from it definitive conclusions about what precisely the laws should command, prohibit, or permit...But, as soon as we try to reach the level of concrete regulation of conduct, we are forced to prefer some values to others. This, however, is just what the formal theory of freedom was meant to avoid. Like the morality of reason, the formal doctrine of freedom has to choose between being unworkable and being incoherent.

Freedom can't be absolute because it is grounded in the social

Roberto Unger, THE CRITICAL LEGAL STUDIES MOVEMENT, 1986, p. 104

The other available answer to the question- what lies on the other side of arbitrary constraint – might be called existentialist. This is the answer that modernists themselves often give and that, lacking any other alternative to the Aristotelian view, they must give. It sees nothing on the other side but the pure and purely negative experience of freedom itself. The aim becomes to assert the self as freedom and to live freedom as rebellion against whatever is partial and facilitious in the established social or mental structures. The existentialist position seems unsatisfactory for reasons of its own It fails to acknowledge that enduring social and mental orders may differ from one another in the extent to which they display the truth about human freedom. Consequently, it is also powerless to deal adequately with a basic objection: freedom, to be real, must exist in lasting social practices and institutions; it cannot effectively exhaust itself in temporary acts of context smashing.

Aff Misc

Serial Policy Failure

Banking on tech advances to solve overload causes serial policy failure Woods, et al, 2

(D.D. Woods, Emily Patterson, Emilie Roth, Professors, Cognitive Systems Engineering Laboratory, Institute for Ergonomics, Cognition, Technology and Work, April 2002, Volume 4, Issue 1, pp 22-36, “Can We Ever Escape From Data Overload? A Cognitive Systems Diagnosis”, <http://link.springer.com/article/10.1007/s101110200002, amp>)

Each round of technical advances, whether in artificial intelligence, computer graphics or electronic connectivity, promises to help people better understand and manage a whole host of activities, from financial analysis to monitoring data from space missions to controlling the national air space. Certainly, this ubiquitous computerisation of the modern world has tremendously advanced our ability to collect, transmit and transform data, producing unprecedented levels of access to data.

However, our ability to interpret this avalanche of data, i.e., to extract meaning from artificial fields of data, has expanded much more slowly, if at all. In studies across multiple settings, we find that practitioners are bombarded with computer-processed data, especially when anomalies occur. We find users lost in massive networks of computerbased displays, options and modes. For example, one can find a version of the following statement in most accident investigation reports: although all of the necessary data was physically available, it was not operationally effective. No one could assemble the separate bits of data to see what was going on. (Joyce and Lapinski 1983) The challenge has become finding what is informative given our interests and needs in a very large field of available data.

The paper is organised as follows. To set the stage, we characterise how technology change has created a paradoxical situation and, we introduce people as a model of competence through a historical example. From this base we summarise the three different major characterisations of the data overload problem. We then provide a ‘diagnosis’ of what makes data overload a difficult problem based on a synthesis of results from past studies that examine how new computerised devices can help overcome or can exacerbate data overload-related problems in control centres such as mission control for space shuttle operations, highly automated aviation flight decks, computerised emergency operations control centres in nuclear power plants and surgical anaesthetic management systems in operating rooms. Given this background, we can see how the typical solutions to the data overload problem avoid confronting the heart of the matter directly, remaining content to nibble away at the edges through indirect means. Finally, we outline a direction for progress towards more effective solutions to data overload relying on people as a competence model.

1.1. The Data Availability Paradox

Our situation seems paradoxical: more and more data is available in principle, but our ability to interpret what is available has not increased. On one hand, all participants in a field of activity recognise that having greater access to data is a benefit in principle. On the other hand, these same participants recognise how the flood of available data challenges their ability to find what is informative or meaningful for their goals and tasks (Miller 1960). We will refer to this as the data availability paradox. Data availability is paradoxical because of the simultaneous juxtaposition of our success and our vulnerability. Technological change grows our ability to make data readily and more directly accessible – the success, and, at the same time and for the same reasons, the change increasingly and dramatically challenges our ability to make sense of the data available – the vulnerability.

1.2. ‘A Little More Technology Will Be Enough’

Criando dificuldades para vender facilidades [creating difficulties to sell solutions]. (Common Brazilian saying)

As the powers of technology explode around us, developers imagine potential benefits and charge ahead in pursuit of the next technological advance. The claim is that data overload and other problems will be

solved by significant advances in machine ‘information’ processing, i.e., the technology for creating sophisticated graphics, for connecting distant people together and for creating intelligent software agents.

However, after each round of development, field researchers continue to observe beleaguered practitioners actively trying to cope with data overload in one form or another. This is a fundamental finding, repeatedly noted in many fields of practice and with many kinds of technology (e.g., Woods 1995a; Woods and Patterson 2000). When viewed in context, systems, developed putatively to aid users, often turn out to create new workload burdens when practitioners are busiest, new attentional demands when practitioners are plagued by multiple channels/voices competing for their attention, and new sources of data when practitioners are overwhelmed by too many channels spewing out too much ‘raw’ data (Woods et al 1994, Ch. 5).

In practice, new rounds of technology development become yet another voice in the data cacophony around us. Ironically, the major impact has been to expand the problem beyond specialised technical fields of activity (an aircraft cockpit or power plant control room) to broader areas of activity (web-based activities we engage in everyday).

Academic studies prove excessive information hurts decisionmaking Metzger, 5

(Michael, Chair in Business Ethics, Kelley School of Business, Indiana University, December 2005, University of Florida Journal of Law & Public Policy, 16 U. Fla. J.L. & Pub. Pol'y 435, “ARTICLE: BRIDGING THE GAPS: COGNITIVE CONSTRAINTS ON CORPORATE CONTROL & ETHICS EDUCATION”, lexis, amp)

From a thinking quality perspective, error can be introduced in every phase of the human thought process. Much of the critical action in decisionmaking of all sorts occurs in the problem identification and classification stages. n89 Do we even admit that we have a problem, n90 and if [*456] we do, how do we classify it and the people involved? n91 Individual desires n92 and bias n93 can play a pivotal role in both problem identification and problem framing. n94 Even things such as the language we use to describe the problem can have a powerful impact on our final decision. n95 [*457] If our attention is selective, n96 then we may not register all of the relevant data available in our external environment. n97 If our memories are also selective and frequently inaccurate, n98 this can be expected to have a consequent negative effect on our ability to bring our past experience to bear in solving current problems. n99 Further, our desire to maintain our self- esteem n100 may lead us to accept dubious arguments and data, n101 to reject compelling arguments and data, n102 and to persist in behaviors and strategies long after an objective observer would have concluded that they were ineffective. n103

Even in circumstances where our memories are accurate, our initial perceptions are complete, and our egos are in check, other threats to gooddecisionmaking exist. In the heuristic phase of our reasoning process, [*458] preconscious mental programs called heuristics n104 retrieve relevant information from memory and identify which bits of externally available information are relevant, and therefore subject to further processing. n105 Heuristics are necessary parts of human cognition for at least two reasons. First, they are essential elements in maintaining some semblance of cognitive economy. We each have limited processing power, and thinking shortcuts n106 that require no conscious thought can be a very efficient way to process information. n107 Second, without some device to screen information, we would quickly suffer cognitive overload from the millions of bits of information embedded in our consciousness and in our environment. n108

[*459]

But while heuristics are essential and may work well most of the time, they can sometimes result in bias n109 in our reasoning. n110 So, the information that seems "relevant" to us psychologically may not necessarily be what is relevant logically. n111 If this happens, no amount of good reasoning in the conscious, analytical phase of our decisionmaking is likely to lead to a correct solution. Why? Good reasoning based on bad information is unlikely to lead to good conclusions. n112 Information can be "bad" if it is [*460]

inaccurate or incomplete, but it can also be "bad" if it is complete and completely accurate, but not really germane to the thinking task at hand.

Even if our information is accurate and complete, and our selection of it is free of bias, we may nonetheless make thinking mistakes during the conscious, analytical phase of the thought process if our grasp of logic, basic probability principles, or statistics is poor, or if certain aspects of the problem prevent us from bringing our full reasoning powers to bear on it. n113 Because it is conscious, and because everyone can learn to improve her logical reasoning ability and improve her understanding of basic statistical principles, n114 the analytical phase of the reasoning process should be the phase that is most amenable to improvement.

The heuristic phase is, by definition, more problematic because it is unconscious. n115 As a leading authority on bias puts it, "the representational [*461] heuristics responsible for many biases constitute preconscious processes. Subjects are aware of that to which they are attending but not of the selective process directing their attention." n116

Infoglut

We are in an era of information overload – a period characterized by an intractable paradox – while we have access to seemingly infinite amounts of information, we are simultaneously unable to process it – the attempt to become omniscient is counterproductive in that it makes it harder to understand and trust information sources

Andrejevic 13 – Honorary Research Associate Professor, Centre for Critical and Cultural Studies; media scholar who writes about surveillance, new media, and popular culture (Mark, “InfoGlut,” Data Overload) //RGP

After a two-year investigation into the post-9/11 intelligence industry, the Washington Post revealed that a sprawling array of public and private agencies was collecting more information than anyone could possibly comprehend. As the newspaper’s report put it, “Every day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications. The NSA sorts a fraction of those into 70 separate databases.”¹ The NSA is merely one amongst hundreds of agencies and contractors vacuuming up data to be sifted, sorted, and stored. The resulting flood of information is, in part, a function of the technological developments that have made it possible to automatically collect, store, and share fantastic amounts of data. However, making sense of this information trove at the all-too-human receiving end can pose a problem: “Analysts who make sense of documents and conversations obtained by foreign and domestic spying share their judgment by publishing 50,000 intelligence reports each year – a volume so large that many are routinely ignored.”² The so-called “Super Users” who are supposed to have access to the whole range of information generated by the intelligence apparatus reportedly told the Post that “there is simply no way they can keep up with the nation’s most sensitive work.”³ As one of them put it, “I’m not going to live long enough to be briefed on everything.”⁴ The lament is a familiar one in an era of information overload – and not just for intelligence agencies, marketers, and other collectors of databases. The same challenge is faced by any citizen attempting to read all of the news stories (or Tweets, or status updates, or blogs posts) that are published on a given day, or a financial analyst researching all of the available information pertaining to the performance of a particular company. When I was a journalist in the early 1990s, just as computers entered the newsroom, we had available to us several electronic newswires that updated themselves automatically with stories on topics ranging from international news to US politics to sports and entertainment. I remember thinking at the time that it was impossible to keep up with the news as it unfolded on my screen. By the time I had read one wire story, dozens of new ones had been filed from around the world. That was just a tiny taste of the coming information cornucopia. Now an unimaginably unmanageable flow of mediated information is available to anyone with Internet access. The paradox of an era of information glut emerges against the background of this new information landscape: at the very moment when we have the technology available to inform ourselves as never before, we are simultaneously and compellingly confronted with the impossibility of ever being fully informed. Even more disturbingly, we are confronted with this impossibility at the very moment when we are told that being informed is more important than ever before to our livelihood, our security, and our social lives. This is not to suggest that it might, once upon a time, have been possible to be “fully informed” – in the sense of knowing all the details of the daily events, their various causes, explanations, and interpretations relating to our social, cultural, political, and economic lives. As Jorge Luis Borges’s (insomnia-inspired) allegory of the mnemonic phenomenon Funes suggests, every day we are bombarded with more information than we can possibly absorb or recall. The ability to capture and recount all of this information in detail is precisely what made Funes a freak – or a god. “We, at one glance, can perceive three glasses on a table; Funes, all the leaves and tendrils and fruit that make up a grape vine. He knew by heart the forms of the southern clouds at dawn on the 30th of April, 1882, and could compare them in his memory with the mottled streaks on a book in Spanish binding he had only seen once and with the outlines of the form raised by an oar in the Rio Negro the night before the Quebracho uprising.”⁵ There are, of course, some drawbacks to total information awareness, Funes-style: it took him a full day to remember a day (and presumably even longer to recall the day spent remembering it). Moreover, Funes was only recording his direct experiences – as yet un-augmented by the Internet and its bottomless reserves of mediated information. If it has always been impossible to fully absorb the information by which we are surrounded – still more so to be “fully informed” – he palpable

information overload associated with the digital, multi-channel era has made us aware as never before of this impossibility. In his book Data Smog, David Shenk observed that “It is estimated that one weekday edition of today’s New York Times contains more information than the average person in seventeenth-century England was likely to come across in a lifetime.”⁶ He does not say who did the estimating – and it is a formulation whose credibility, such as it is, depends on a particular definition of information: “in mass mediated form.” Surely during the 17th century people were absorbing all kinds of information directly from the world around them, as we do today through the course of our daily lives. There is little indication that our sensory apparatus has become more finely tuned or capacious. However, the amount of mediated information – that which we self-consciously reflect upon as information presented to us in constructed and contrived formats (TV shows, movies, newspapers, Tweets, status updates, blogs, text messages, and so on) via various devices including televisions, radios, computers, and so on – has surely increased dramatically, thanks in no small part to the proliferation of portable, networked, interactive devices. Even before the advent of these devices, all we had to do was go to the library to feel overwhelmed by more than we could possibly absorb. Now this excess confronts us at every turn: in the devices we use to work, to communicate with one another, to entertain ourselves. Gult is no longer a “pull” phenomenon but a “push” one. We don’t go to it, it comes to us. It is the mediated atmosphere in which we are immersed. When all we had to do to keep up with the news, for example, was to read a daily newspaper and watch the network evening news, it was easier to imagine the possibility that someone like Walter Cronkite could tell us “the way it is” during the half-hour interlude of an evening newscast. By the first decade of the 21st century, the era of the most-trusted man in America was long gone, as evidenced, for example, by a poll revealing that despite (or perhaps because of) the proliferation of hours devoted to television news, not one major news outlet was trusted by the majority of the American people. Poll upon poll have revealed declining levels of public trust in news outlets and a heightened sense of perceived bias on the part of journalists. The researcher responsible for a 2008 poll noted that “an astonishing percentage of Americans see biases and partisanship in their mainstream news sources” presumably because, “The availability of alternative viewpoints and news sources through the Internet ... contributes to the increased skepticism about the objectivity of profit-driven news outlets owned by large conglomerates.”⁷ It is not just that there is more information available, but that this very surfeit has highlighted the incompleteness of any individual account. An era of information overload coincides, in other words, with the reflexive recognition of the constructed and partial nature of representation.

Surveillance is no exception – the normalization of intrusive surveillance programs is justified under the pre-emptive logic of deterrence – we are convinced that once we know everything, we can prevent all crime

Andrejevic 13 – Honorary Research Associate Professor, Centre for Critical and Cultural Studies; media scholar who writes about surveillance, new media, and popular culture (Mark, “InfoGlut,” “Foreknowledge is Supremacy”) //RGP

These formulations bring us a bit closer to the notion of deterrence: a kind of pre-emption of the core experience of desire itself – what gets averted is the moment of lack with which this experience coincides. Taken to its limit, the goal is to relegate desire to the pre-empted status of crime in “The Minority Report”: “pure metaphysics.” If you’re jailed before you committed the crime, are you really guilty? If the database knows what you want before you do, did you really want it? The lack is filled before it is subjectively perceived. Would the crime really have happened? Was the desire really there? Is that purchase/search term really what the subject wanted prior to the precipitation of the moment of consumption or search? The mutants and the statisticians say yes, and who is to prove them wrong? In his description of what he describes as the simulation of surveillance, Bogard argues that predictive analytics is not simply about predicting outcomes, but about devising ways of altering them. In policing terms, the goal of predicting the likelihood of criminal behavior is to deter it. In marketing or campaigning terms it is to anticipate desire before it happens – to precipitate an accelerating range of latent desires that were allegedly “already there.” Transposed into business jargon, as one digital marketing executive put it, “In the early days of digital marketing, analytics emerged to tell us what happened and, as analytics got

better, why it happened. Then solutions emerged to make it easier to act on data and optimize results.”³³ The more data that can be processed faster, the better for turning “big data into a big opportunity.”³⁴ The promise of predictive analytics is to incorporate the future as a set of anticipated data points into the decision-making process: “Historically all Web analytics have reflected data from the past which has been to a certain extent like driving a car using only the rear view mirror … for the first time we can be marketers using data in a manner that allows us to drive while facing the road ahead.”³⁵ It is a vision of a future in which the structure outlined by predictions is subject to modification along certain pivot points. If, for example, a credit card company can predict a scenario that might lead to losses, it can intervene in advance to attempt to minimize these, as in one example described by the New York Times: “credit-card companies keep an eye on whether you are making purchases of that kind [indicating marital problems], because divorce is expensive and they are paranoid that you might stop paying your credit-card bill. For example, if you use your card to pay for a marriage counselor, they might decrease your credit line.”³⁶ Similarly, in the book Super Crunchers, Ian Ayres describes how the credit card company CapOne uses data mining to predict the smallest possible reduction in interest rates that can be used to retain customers. When someone calls in with a complaint about a card’s high interest rates, a computer uses detailed information about the consumer combined with information about how similar customers have behaved in the past to rapidly generate a range of rates likely to pre-empt the consumer’s cancellation request: “Because of Super Crunching, CapOne knows that a lot of people will be satisfied with this reduction (even when they say they’ve been offered a lower rate from another card).”³⁷ The fact that marketing analogies are so frequently used to introduce the topic of predictive analytics reflects both the pioneering role played by the commercial sector and what might be described as its ordinariness: the way in which the use of data mining has incorporated itself into our understanding of how the world works in the digital era. Customized recommendations on Amazon.com and targeted advertising on the Internet, not to mention targeted mailings and customized coupons in the supermarket, have become the commonplaces of everyday life in contemporary, information-rich societies. What once might have seemed slightly creepy – Google scanning our email, for example, to figure out how best to market to us – has become a normal and largely overlooked part of daily life for millions of email users. This level of normalcy helps to pave the way for forms of population-level police surveillance that might previously have seemed intrusive or otherwise inappropriate. As a report for the National Institute of Justice put it, “Walmart, for example, learned through analysis that when a major weather event is in the forecast, demand for three items rises: duct tape, bottled water and strawberry Pop-Tarts … Police can use a similar data analysis to help make their work more efficient … some in the field believe it has the potential to transform law enforcement by enabling police to anticipate and prevent crime instead of simply responding to it.”³⁸ If we are submitting to detailed monitoring to help enhance Pop-Tart sales, surely we can do it for public safety and national security. Viewed from a slightly different perspective, it is hard to avoid the notion that we are living in an era of rampant surveillance creep. Whereas once upon a time it might have seemed strange to allow police to scan and store license plate numbers of everyone who drives by a particular location, this now takes place as a matter of course. Predictive policing, in this regard, is just piggybacking on the “new normal” of digital, interactive monitoring. Reinforcing this normality are the claims made on behalf of predictive policing. In Boston, officials reported that serious crime in the Cambridge area in 2011 dropped to its lowest level in 50 years after police adopted a data-driven predictive policing program (tellingly, the claim does not distinguish between correlation and causation). The murder rate actually increased – but police said this was a result of domestic disputes that they could not (yet?) predict.³⁹ In Santa Cruz, police reported a significant drop in burglaries after adopting a predictive policing program developed by mathematicians, an anthropologist, and a criminologist based on models for predicting earthquake aftershocks.⁴⁰ In Memphis, officials reported a 15 percent drop in serious crime over four years after adopting a database-driven predictive policing program.⁴¹ Police are experimenting with a growing range of variables to predict crime, ranging from weather patterns to building code violations. In Arlington, Texas, police reported that every unit increase in physical decay of the neighborhood (measured by code violations) resulted in six more residential burglaries in the city.⁴² For the moment, however, the most common indicator seems to be past patterns of behavior. In Santa Cruz, for example, two women were taken into custody for peering into cars in a parking garage that the computer indicated would be at risk for burglaries that day: “One woman was found to have outstanding warrants; the other was carrying illegal drugs.”⁴³ If, for the moment, the methodologies seem relatively crude (but potentially effective – at least on occasion), it is worth keeping in mind that current systems rely on only a tiny current of the swelling information flood. However, recent regulatory shifts propose to make much more data available. As of this writing, legislators in the UK have proposed giving intelligence agencies access to the phone records, browsing details, emails, and text messages of all Britons without a warrant.⁴⁴ In the US, updated “guidelines” for the National Counter Terrorism Center allow the organization to collect data about any American without a warrant and keep it for up to five years. It also permits the center to data mine this information for the purposes of investigating terrorism.⁴⁵ Total Information Awareness as a named program may have disappeared, but as an unnamed initiative it continues to develop apace.

With increasing floods of information comes a widening power gap – those with access to bulk data gain advantage over those without it

Andrejevic 13 – Honorary Research Associate Professor, Centre for Critical and Cultural Studies; media scholar who writes about surveillance, new media, and popular culture (Mark, “InfoGlut,” Simulation as Deterrence) //RGP

The question recalls the post-9/11 data-driven plans of Admiral John Poindexter for a Total Information Awareness program that would sift through a giant database of databases in search of threat indicators. Indeed, the Wall Street Journal opens its op-ed piece about the Colorado shooting with the question, “Would Total Information Awareness have stopped James Eagan Holmes [the suspect in the Colorado shooting]?”² Put that way, the question sounds almost rhetorical: “total information awareness” implies a high degree of predictive power: if you could keep an electronic eye on everyone’s actions all the time, surely you could unearth the symptoms of eventual wrongdoing. Set aside for a moment that the version of security on offer requires willing submission to “total” surveillance and simply consider the fantasy of pre-emption opened up by the technology: “a future landscape of surveillance without limits – everything visible in advance, everything transparent, sterilized, and risk-free, nothing secret, absolute foreknowledge of events.”³ If this sounds futuristic and vaguely absurd, consider the claims that are currently being made on behalf of so-called predictive policing, which uses past crime patterns and related data to guide the deployment of police patrols: “It is now possible to predict the future when it comes to crime, such as identifying crime trends, anticipating hotspots in the community, refining resource deployment decisions, and ensuring the greatest protection for citizens in the most efficient manner.”⁴ It is perhaps a telling sign of the power of the promise of new information and communication technologies, based on their ability to collect, store, and process huge amounts of data, that one of our first reactions to the unexpected has become: “could the database have predicted it?” – and the automatic corollary: “could the database have prevented it?” Lurking in these two questions is an assumption about the character of knowledge in the digital era: the notion that the only limit on our predictive power is the ability to effectively organize all the available information. If this were indeed the case, then the development of technological information storage and processing technology might compensate for the shortcomings of the human brain by ushering in new forms of aggregate “knowledge” and predictive power. Such forms of “knowing” would, in a sense, exceed the limits of human comprehension. It would no longer be a question of comprehending the data or using it to understand, in referential fashion, the world to which it refers, but rather of putting the data to use. The promise of automated data processing is to unearth the patterns that are far too complex for any human analyst to detect and to run the simulations that generate emergent patterns that would otherwise defy our predictive power. The form of “knowledge” on offer is limited to those with access to the database and the processing power, and it replicates the logic of “knowing without knowing” insofar as it can serve as the basis for decisions while exceeding the processing power of any individual human brain. In keeping with the logic of digital convergence, this form of knowledge is portrayed by its proponents as universal insofar as it is generalizable across the political, economic, and social domains. It can be used to predict consumer behavior as well as the spread of disease, or the likelihood that someone will need to be hospitalized within the coming year. Keeping this convergent background in mind, this chapter will focus on the somewhat narrower example of policing and security in order to explore the knowledge practices associated with data mining and predictive analytics in the era of “big data.” In particular, the focus will be upon the version of distributed, predictive “knowledge” that emerges from the database. As McCue puts it in her discussion of the use of predictive analytics for security purposes, “With data mining we can perform exhaustive searches of very large databases using automated methods, searching well beyond the capacity of human analysts or even a team of analysts.”⁵ In the wake of the development of database technology, there is an emerging tendency to devalue individual comprehension in comparison with the alleged predictive power derived from “super-crunching” tremendous amounts of data. This development has significant implications for the promise that because new information and communication technologies are less or non-hierarchical, they are therefore forces for democratization and user empowerment: if the (allegedly) more powerful and productive forms of knowledge associated with “big data” are limited to those with access to the database and processing power, digital-era knowledge practices

could prove to be even more exclusive and asymmetrical than those they promise to displace. Widespread access to digital media would go hand-in-hand with what might be described as the emergence of a “big data” divide – one that could not be ameliorated by any relatively simple technological fix (such as more widespread broadband access) or by enhanced forms of education and training. In this respect, the knowledge practices associated with big data represent a profoundly un-democratic shift insofar as they are reliant upon access to huge and costly databases as well as to the processing power and technological know-how to make use of the data.

Something about Baudrillard

Andrejevic 13 – Honorary Research Associate Professor, Centre for Critical and Cultural Studies; media scholar who writes about surveillance, new media, and popular culture (Mark, “InfoGlut,” Simulation as Deterrence) //RGP

The French cultural theorist Jean Baudrillard famously defined simulation as a form of deterrence, taking as his model the Cold War logic of “mutually assured destruction” (MAD). The deterrent effect of simulation has been a recurring theme in popular science fiction that received perhaps its most iconic pop-culture treatment in the movie War Games, which portrays a computer game that goes awry, accessing the United States missile defense system and transforming a game of simulated nuclear war into the real thing. Disaster is averted when the program considers all possible outcomes of the “game” of global thermonuclear war and discovers that, as in tic-tac-toe, if both sides play rationally, attempting to win, there can be no winner. The computer, which is programmed to learn, describes its assessment of “global thermonuclear war” in the movie’s finale: “A strange game! The only winning move is not to play.” Or, more accurately, the only right way to play is by not playing: the game is already being played, as it were, prior to any missile attack. The logic of mutual assured destruction relies on the ability to avoid a possible future by modeling it. Simulation stands in for a kind of knowledge about the future that exerts control in the present: “What stirs in the shadow of this posture under the pretext of a maximal ‘objective’ menace, and thanks to that nuclear sword of Damocles, is the perfection of the best system of control which has never existed.”⁶ Simulation as deterrence, then, operates in a paradoxically counterfactual realm: that of the proven negative. On the one hand is the promise of information as control that stipulates a kind of mechanistic causality, on the other is the claim to intervene in the mechanism of causality itself. This is why, taken to their limits, strategies of simulation invoke both total control and its eclipse: a kind of smothering stasis in which all possibilities are fully saturated – everything has been modeled in advance, including the modeling process itself. As Baudrillard puts it in his discussion of the virtualization of reality via simulation, “What is the idea of the Virtual? It seems that it would be the radical effectuation, the unconditional realization of the world, the transformation of all our acts, of all historical events, of all material substance and energy into pure information. The ideal would be the resolution of the world by the actualization of all facts and data.”⁷ The apparent obstacle to such a resolution is the limit of human perceptions, analytic ability, and time. The ability to overcome such limits is relegated to the realm of the superhuman. As Laplace, the pioneer of mathematical probability, put it, “Given for one instant an intelligence which could comprehend all the forces by which nature is animated and the respective situation of the beings who compose it – an intelligence sufficiently vast to submit these data to analysis ... for it, nothing would be uncertain and the future, as the past, would be present to its eyes.”⁸ The name for that intelligence, viewed through one historical lens, would be God. In the digital era, it is the computer and the database. In the era of predictive analytics, popular fiction continues to experiment with the paradoxes of simulation. Consider, for example, the television show Person of Interest, in which a renegade computer programmer taps into the government’s data-mining apparatus (which he created) in order to predict when and where life-threatening crimes will occur. The show’s premise is that automated surveillance has become both ubiquitous and multifaceted – all spaces and practices are monitored via technologies ranging from smart cameras equipped with facial recognition technology to telephones with embedded voice-stress analyzers. The seemingly distributed network of commercial, public, and personal sensors and communication devices (closed-circuit surveillance cameras, Webcams, smart phones, and so on) has been covertly colonized by a centralized monitoring apparatus. This apparatus – which becomes increasingly “subjectivized” over the course of the series – can watch, listen, and communicate with the main cast members through the full range of networked devices. It is as if all of our various smart devices have teamed up to create an emergent machine intelligence. The show’s opening sequence represents the monitoring process at work by portraying the view from the perspective of the all-seeing surveillance apparatus. We see quick intercut shots of people viewed in

grainy surveillance video overlaid with terms meant to suggest the various forms of monitoring at work: “voice capture stress percentage”; “GPS (global positioning system): active, tracking location”; “searching: all known databases”; etc. In this world, the environment itself has been redoubled as both setting and spectator. No one in particular is watching, but everyone is watched all the time. The result is what Bogard describes as “the impersonal domination of the hypersurveillance assemblage.”⁹ On the show, this assemblage comes to serve as a technologized version of the mutant, prescient “pre-cogs” in Steven Spielberg’s 2002 movie Minority Report, based on the Philip K. Dick story that envisions a world in which crime is prevented before it takes place. Dick’s story stages the paradox of simulated deterrence in a discussion between two officials engaged in fighting “pre-crime”: “You’ve probably grasped the basic legalistic drawback to precrime methodology. We’re taking in individuals who have broken no law … So the commission of the crime itself is absolute metaphysics. We claim they’re culpable. They, on the other hand, eternally claim they’re innocent. And, in a sense, they are innocent.”¹⁰ The difference between the modeling of possible futures proposed by Minority Report and the strategies of simulated deterrence currently under development in the United States and elsewhere is that between determinism and probability. The fictional portrayals envision a contradictory world in which individual actions can be predicted with certainty and effectively thwarted. They weave oracular fantasies about perfect foresight. Predictive analytics, by contrast, posits a world in which probabilities can be measured and resources allocated accordingly. Because forecasts are probabilistic, they never attain the type of certitude that would, for example, justify arresting someone for a crime he or she has not yet committed. Rather, they distribute probabilities across populations and scenarios. The mobilization of such forms of data mining are anticipated in Michel Foucault’s description of the rise of apparatuses of security, governed by questions such as “How can we predict statistically the number of thefts at a given moment, in a given society, in a given town, in the town or in the country, in a given social stratum, and so on? Second, are there times regions, and penal systems that will increase or reduce this average rate? Will crises, famines, or wars, severe or mild punishment, modify something in these proportions? … What is the cost of suppressing these thefts … What therefore is the comparative cost of theft and of its repression …?”¹¹ What emerges is a kind of actuarial model of crime: one that lends itself to aggregate considerations regarding how best to allocate resources under conditions of scarcity – a set of concerns that fits neatly with the conjunction of generalized threat and the constriction of public-sector funding. The algorithm promises not simply to capitalize on new information technology and the data it generates, but simultaneously to address reductions in public resources. The challenges posed by reduced manpower can be countered (allegedly) by more information. As in other realms, enhanced information processing promises to make the business of policing and security more efficient and effective. However, it does so according to new surveillance imperatives, including the guidance of targeted surveillance by comprehensive monitoring, the privileging of prediction over explanation (or causality), and new forms of informational asymmetry. The data-driven promise of prediction, in other words, relies upon significant shifts in cultures and practices of information collection.\

Authenticity

The glut of information that is fed to us by the surveillance state makes authenticity impossible – instead we wait to be told what to desire

Horning 14 (Rob, Executive Editor of The New Inquiry and author of Marginal Utility, citing Mark Andrejevic, author of Infoglut, 7/10, “No Life Stories,”
<http://thenewinquiry.com/essays/no-life-stories//Tang>)

Purveyors of targeted marketing often try to pass off these sorts of intrusion and filtering as a kind of manufactured serendipity. Andrejevic cites a series of examples of marketing hype inviting us to imagine a world in which retailers know what consumers want before the consumers do, as though this were a long-earned-for miracle of convenience rather than a creepy effort to circumvent even the limited autonomy of shopping sovereignty. “In the world of database-driven targeting,” Andrejevic argues, “the goal is, in a sense, to pre-empt consumer desire.” This is a strange goal, given that desire is the means by which we know ourselves. In hoping to anticipate our desires, advertisers and the platforms that serve ads work to dismantle our sense of self as something we must actively construct and make desire something we experience passively, as a fait accompli rather than a potentially unmanageable spur to action. Instead of constructing a self through desire, we experience an overload of information about ourselves and our world, which makes fashioning a coherent self seem impossible without help. If Big Data’s dismantling the intrinsic-self myth helped people conclude that authenticity was always an impossibility, a chimera invented to sustain the fantasy that we could consume our way to an ersatz uniqueness, that would be one thing. But instead, Big Data and social media foreground the mediated, incomplete self not to destroy the notion of the true self altogether but to open us to more desperate attempts to find our authentic selves. We are enticed into experiencing our “self” as a product we can consume, one that surveillance can supply us with. The more that is known about us, the more our attention can be compelled and overwhelmed, which in turn leads to a deeper reliance on the automatic filters and algorithms, a further willingness to let more information be passively collected about us to help us cope with it all. But instead of leading to resolution, a final discovery of the “authentic” self, this merely accelerates the cycle of further targeted stimulation. The ostensible goal of anticipating consumer desire and sating it in real time only serves the purpose of allowing consumers to want something else faster. So as surveillance becomes more and more total, Andrejevic argues, we experience our increasingly specified and information-rich place in this matrix as confusion, a loss of clarity or truth about the world and ourselves. Because excess information is “pushed” at us rather than something we have to seek out, we are always being reminded that there is more to know than we can assimilate, and that what we know is a partial representation, a construct. Like a despairing dissertation writer, we cannot help but know that we can’t assimilate all the knowledge it’s possible to collect. Each new piece of information raises further questions, or invites more research to properly contextualize it. Ubiquitous surveillance thus makes information overload everyone’s problem. To solve it, more surveillance and increasingly automated techniques for organizing the data it collects are authorized. In a series of chapters on predictive analytics, prediction markets, and body-language analysis and neuromarketing, Andrejevic examines the variety of emerging technology-driven methods meant to allow data to “speak for itself.” By filtering data through algorithms, brain scans, or markets, an allegedly unmediated truth contained within it can be unveiled, and we can bypass the slipperiness of discursive representation and slide directly into the real. Understanding why outcomes occur becomes unnecessary, as long as the probabilities of the correlations hold to make accurate predictions.

Deliberation/identity

Big Data kills democratic deliberation and social identity

Horning 14 (Rob, Executive Editor of The New Inquiry and author of Marginal Utility, citing Mark Andrejevic, author of Infoglut, 7/10, “No Life Stories,” <http://thenewinquiry.com/essays/no-life-stories//Tang>)

Far from being neutral or objective, data can be stockpiled as a political weapon that can be selectively deployed to eradicate citizens’ ability to participate in deliberative politics. Many researchers have pointed out that “raw data” is an oxymoron, if not a mystification of the power invested in those who collect it. Subjective choices must continually be made about what data is collected and how, and about any interpretive framework to deploy to trace connections amid the information. As sociologists Kate Crawford and danah boyd point out, Big Data “is the kind of data that encourages the practice of apophenia: seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions.” The kinds of “truths” Big Data can unveil depends greatly on what those with database access choose to look for. As Andrejevic notes, this access is deeply asymmetrical, undoing any democratizing tendency inherent in the broader access to information in general. In his 2007 book iSpy: Surveillance and Power in the Interactive Era, he argues that “asymmetrical monitoring allows for a managerial rather than democratic relationship to constituents.” Surveillance makes the practice of “making one’s voice heard” basically redundant and destroys its link to any intention to engage in deliberative politics. Instead politics operates at the aggregate level, conducted by institutions with the best access to the databases. These data sets will be opened to elite researchers and the big universities that can afford to pay for access, Crawford and boyd point out, but everyone else will be mostly left on the sidelines, unable to produce “real” knowledge. As a result, institutions with privileged access to databases will have ability to determine what is true. This plays out not only with events but also with respect to the self. Just as politics necessarily requires interminable intercourse with other people who don’t automatically see things our way and who least acknowledge alternate points of view only after protracted and often painful efforts to spell them out, so does the social self. It is not something we declare for ourselves by fiat. I need to negotiate who I am with others for the idea to even matter. Alone, I am no one, no matter how much information I may consume. In response to this potentially uncomfortable truth, we may turn to the same Big Data tools in search of a simpler and more directly accessible “true self,” just as politicians and companies have done. Identity then becomes a probability, even to ourselves. It ceases to be something we learn to instantiate through interpersonal interactions but becomes something simply revealed when sufficient data exists to simulate our future personality algorithmically. One is left to act without any particular conviction while awaiting report from various recommendation engines on who we really are. In this sense, Big Data incites what Andrejevic, following Žižek, calls “interpassivity,” in which our belief in the ideology that governs us is automated, displaced onto a “big other” that does the believing for us and alleviates us of responsibility for our complicity. Surrendering the self to data processors and online services make it a product to be enjoyed rather than a consciousness to be inhabited. The work of selfhood is difficult, dialectical, requiring not only continual self-criticism but also an aware- ness of the degree to which those around us shape us in ways we can’t control. We must engage them, wrestle with one another for our identities, be willing to make the painful surrender of our favorite ideas about ourselves and be vulnerable enough to becoming some of what others see more clearly about us. The danger is that we will settle for the convenience of technological work-arounds and abnegate the duty to debate the nature of the world we want to live in together. Instead of the collective work of building the social, we can settle for an automatically generated Timeline and algorithmically generated prompts for what to add to it. Data analysts can detect a correlation between two seemingly random points—intelligence and eating curly fries, say, as in a 2012 PNAS research paper by Michal Kosinski, David Stillwell, and Thore Graepel that made the rounds on Tumblr and Twitter in January—and potentially kick off a wave of otherwise inexplicable behavior. “I don’t know why I am eating curly fries all of a sudden, but that shows

how smart I am!" Advertisers won't need a plausible logic to persuade us to be insecure; they can let spurious data correlations speak for them with the authority of science. Unlike the Facebook mood-manipulation paper, the curly-fries paper enjoyed a miniviral moment in which it was eagerly reblogged for its novelty value, with only a mild skepticism, if any, attached. This suggests the seductive entertainment appeal these inexplicable correlations can provide—they tap the emotional climate of boredom to spread an otherwise inane finding that can then reshape behavior at the popular level. We're much more likely to laugh about the curly fries paper and pass it on than to absorb any health organization's didactic nutrition information. Our eagerness to share the news about curly fries corresponds with our willingness to accept it as true without being able to understand why. It's WTF incomprehensibility enhances its reach and thus its eventual predictive power. Likewise, the whimsical reblogging of the results from patently ridiculous online tests hints at how we may opt in to more “entertaining” solutions to the problem of self If coherent self-presentation that considers the need of others takes work and a willingness to face our own shortcomings, collaborating with social surveillance and dumping personal experience into any and all of the available commercial containers is comparatively easy and fun. It returns to us an “objective” self that is empirically defensible, as well as an exciting and novel object for us to consume as entertainment. We are happily the audience and not the author of our life story. Thus the algorithm becomes responsible for our political impotence, an alibi for it that lets us enjoy its dubious fruits. By trading narratives for Big Data, emotions are left with no basis in any belief system. You won't need a reason to feel anything, and feeling can't serve as a reliable guide to action. Instead we will experience the fluctuation of feeling passively, a spectator to the spectacle of our own emotional life, which is now contained in an elaborate spreadsheet and updated as the data changes. You can't know yourself through introspection or social engagement, but only by finding technological mirrors, whose reflection is systematically distorted in real time by their administrators. Let's hope we don't like what we see.

Truth testing

Information overload makes testing truth claims impossible – its used as a tool to protect power

McVey 13 (Alex, University of North Carolina at Chapel Hill, Communication Studies and Cultural Studies, Graduate Student, Book Review: Infoglut, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/andrejevic/infoglut_review//Tang)

Mark Andrejevic's Infoglut offers a theoretically rich account of the modern information landscape, examining how the massive proliferation of information transfer and storage through modern technology impacts our understanding of both communication and critique. The hyperproliferation of information in the era of the internet and computer data storage has contributed to a form of information overload called 'Infoglut'. This state of information overload marks what Slavoj Zizek calls the 'decline of symbolic efficiency,' in which the proliferation and accumulation of competing narratives and truth claims ultimately calls all claims to truth into question. Whereas power once operated through the establishment of a dominant narrative and the suppression of alternative narratives, the perpetual availability of competing claims to truth now makes old strategies of controlling information irrelevant. Where the task of the powerful was once to prevent new information from circulating that could hurt their interests, the task of the powerful is now to circulate so much information that any claim to truth can ultimately be called into question by mobilizing enough data. Controlling information no longer requires preventing new information from circulating but rather controlling access to databases and infrastructure capable of storing, monitoring, and analyzing massive quantities of data. Critical practices of the pre-infoglut era, rooted in theories of representation, are now reduced to conspiracy theories that dispel all claims to expertise as a form of hidden ideology, all while positing a new ideological claim under the postideological guise of prediction or affective certainty. Andrejevic sets out to examine how Our modern condition of infoglut both changes the relationship between power and knowledge and calls for a re-examination of the role of critique in a time of postnarrative uncertainty. A variety of case studies demonstrate that, in response to the decline of symbolic efficiency, practices of analyzing data emerge that displace communication and deliberation by appealing either to the supposedly value-free calculations of an algorithm or the market place or to pre-cognitive affect in body language and neuroscience. Andrejevic looks at the way information is gathered, stored, analyzed, automated and deployed to shine light on the varied landscapes of modern information processing, including the way inequalities manifest in the architectures of data storage and analysis. Andrejevic offers a critique of the democratizing spirit of the internet as a means for the mass distribution of information, arguing that consumers now take part in ubiquitous acts of data sharing in which their behaviors are monitored, analyzed and used both to predict future behavior and to help shape future behavior. Looking at the phenomenon of 'digital convergence,' the process by which formerly distinct bodies of digital information converge, Andrejevic points out how ubiquitous information storage is becoming across the social field. By looking at the convergence of data analysis in marketing, politics, surveillance, security, policing and popular culture, Andrejevic mounts a convincing argument for information management as an all-encompassing and quotidian element of modern power. However, Andrejevic is quick to warn readers against reading the decline of symbolic efficiency as a totalizing or all-encompassing fact of modern existence. Far from the perfect crime predicting capacities foretold by the movie Minority Report, Andrejevic reminds readers that there are imperfections and probabilities distributed across these systems. Not all narratives can be disturbed through the proliferation of counter-information, and the decline of symbolic efficiency is far from complete. Yet despite this caveat, it is possible to detect some totalizing tendencies in Andrejevic's account of information overload. For example, in his discussion of data mining, Andrejevic argues that modern forms of information gathering have displaced old forms of targeting and surveillance because whereas in old regimes the target had to first be identified in order to be surveyed, in the modern era of infoglut, data gathering and analysis of every possible variable allows data experts to predict who potential suspects may be. As a result, Andrejevic argues, 'emerging surveillance strategies will continue to push for data access at the level of entire populations' as opposed to, say, that of suspicious (or, from a marketing perspective, desirable) groups or individuals' (36). While Andrejevic is right to argue that surveillance practices have taken on new forms in an era of modern infoglut, it would be a mistake to overemphasize these new forms

as a break from previous surveillance strategies. Doing so would miss the way in which surveillance still works to disproportionately target differently racialized, gendered and abled bodies. While it is true that more and more members of the population increasingly participate in data transfers that are stored, monitored and analyzed by data experts, racial, gender, class and other values can nevertheless be inscribed into the information processing systems Andrejevic describes. Future scholars should build on Andrejevic's work by pointing to how these axes of difference influence modern conditions of infoglut. Andrejevic's book should likewise be required reading for those attempting to engage in leftist politics in a digital age. Andrejevic argues that the 'postmodern right' has coopted the process of critique in the name of conspiracy theory and encouraged the proliferation of multiple truths in order to swamp any attempt to make a claim to a truth against the right. Examining, for example, the strategies of the Bush administration in Iraq, Andrejevic argues that the postmodern right relies on what Žižek calls the 'Borrowed Kettle' strategy in order to dispel criticism. In the face of critiques of the Bush's handling of the war in Iraq, the administration offers multiple contradictory accounts in order to preclude the possibility of locating one as true and thus being able to pin down the administration's failures. Additionally, Andrejevic looks at Glen Beck's mobilization of conspiracy theories rooted in affective claims to understanding reality that dispel the knowledge of so-called 'experts.' Far from challenging the logic of the postmodern right, strategies that focus on critiquing their narratives and offering counteracting truth claims merely feed into the information economy that sustains the postmodern right's existence. Additionally, Andrejevic shows how the convergence of data works as a conduit of both capitalism and the state, as a method of studying populations to predict and intervene on human behavior. Data mining gathers and stores massive amounts of consumer data, which in turn gets stored in databases that can be used for police and security measures. Prediction markets are used to bypass deliberative processes by depicting the market as a neutral arbiter capable of rising above the clutter of information overload, cementing antidemocratic, capitalist practices while laboring under the banner of a market based populism. These interlocking inequities and power dynamics are all at play in Infoglut. Andrejevic similarly offers a fruitful interrogation of the role affect plays in negotiating the decline of symbolic efficiency. If the proliferation of competing claims to truth in an age of infoglut makes representation unreliable, affect offers a way of cutting through the fog of data by reading and analyzing the body's pre-cognitive processes of decision making. Andrejevic examines how new social media technologies prompt new ways of attempting to analyze and interpret emotion. Here, affective economies encourage the monitoring of social media both in order to predict and intervene to help shape popular sentiments. Chapter four studies how the logic of the market comes to function as a sort of 'affective fact' that continues to function even in the face of the failure of the markets which dispel its main narrative. Andrejevic similarly locates the study of affect in popular culture representations of the reading of body language, such as the TV shows Lie to Me or the World Series of Poker. In all of these case studies, affect offers a means of bypassing the unreliable plane of discourse and representations to give way to a prediscursive understanding of the subject's desires, feelings, and behaviors. While much of Andrejevic's work on affect describes how affect works in a historical context of infoglut, Andrejevic also offers a bold theoretical move by critiquing affect theory, with its focus on pre-cognitive intensities rather than rationality and reason, as implicated in the strategies of neuroscience and neuromarketing used by the powerful in response to the decline of symbolic efficiency. While this theoretical claim is perhaps one of the more interesting in the book, Andrejevic seems rushed to lump the entire theoretical trajectory of affect theory together with the practices of neuromarketing. While both affect theory and neuroscience share an interest in the precognitive elements of human behavior, it remains to be seen how the particularities of affect theory either permit or challenge the practices of neuromarketing. While Andrejevic ultimately points toward a more nuanced role for affect theory by arguing for a mode of affect that is neither incompatible nor identical with reason, more scholarly work should be devoted to studying the links between affect theory and forms of capitalist advertising and marketing practices that work at the level of affect. Infoglut is an important read for scholars interested in big data, affect theory, psychoanalysis, Surveillance Studies, and the relationship between data and communication studies. This book is a must read for communication scholars because it interrogates the ways that strategies of managing information overload attempt to bypass discourse, representation and deliberation. In the face of an infoglut which thwarts traditional modes of criticism, Andrejevic calls on scholars to 'gain control over the forms of postcomprehension knowledge that promise to populate the databases and contest their displacement of comprehension, models, theories, and narratives' (164). Infoglut begins this project and marks an outstanding move in that direction.

AT Abusive Probable Cause Determinations Reviewed by the Courts

Courts won't define probable cause and have reduced their review of probable cause determinations

Erica Goldberg, 2013, law professor, Penn State Dickinson School of Law, Lewis & Clark Law Review, Getting Beyond Intuition in the Probable Cause Inquiry,"

http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1033&context=fac_works, p. 799-800

Currently, courts apply a "nontechnical conception" n46 of probable cause at all levels of review, allowing for flexibility in application of the standard but providing little guidance for police officers and magistrate judges. The result is, as one scholar noted, that "although the Court has stressed the importance of a "single uniform standard' of probable cause for criminal investigatory conduct, it has not defined that standard in a manner that is particularly illuminating to those charged with enforcing and interpreting the criminal law." Relatively recent developments in Fourth Amendment law have compounded this problem because they have undermined judicial review of probable cause determinations, making it even more necessary to clarify the standard. As mentioned above, law enforcement officers must make practical commonsense judgments in areas of uncertainty, when they do not know if a suspect is actually committing a crime. Because police officers are not, as the Supreme Court often reminds us, "legal technicians," the probable cause standard must allow police officers to make educated guesses. If such a guess is reasonable but incorrect, and the police ultimately find either no evidence of the criminal activity they were looking for or evidence of entirely unrelated criminal activity, then the standard must also provide room for courts to defer to a police officer's expertise, but prevent unreasonable intrusions. To accommodate the myriad interactions between police and individuals without creating rules that unduly stifle a police officer's exercise of her intuition, courts generally assess probable cause given the totality of the circumstances. n52 This flexibility allows courts to take all of the facts into account and make an intuitive judgment when issuing a warrant or upholding a search instead of having to strictly adhere to rigid rules about what constitutes probable cause. n53 For example, the totality-of-the-circumstances test that governs whether an informant's tip can supply probable cause balances factors like the reliability of the informant, the basis for the informant's information, and the extent to which the police have corroborated the tip. n54 A judge may disregard the fact that a confidential informant's criminal record or drug addiction undermines her reliability if other factors point towards her truthfulness. n55 There are many ways to interpret the same set of facts, and an innocent explanation for the evidence presented does not necessarily negate probable cause. With great flexibility, however, comes great uncertainty. n57 The Supreme Court has remarked that "reasonable minds frequently may differ on the question whether a particular [warrant] affidavit establishes [*801] probable cause." n58 Scholars have noted "wildly different outcomes" based on similar fact patterns when determining probable cause and reasonable suspicion. n59 Part of the problem is that no one knows how high a hurdle the standard actually presents. The Supreme Court explicitly refuses to assign probable cause a numerical value, equating it instead to a "fair probability" that evidence will be found. n60 Judges, scholars, and practitioners hold varying views as to the burden imposed by probable

cause, with the largest number of judges clustering in the range between 30% and 60%. n61 Disagreement among scholars and practitioners even exists as to whether probable cause is a lighter or equivalent burden to the preponderance of the evidence standard. n62 The recognition that reasonable minds may easily differ on whether probable cause is satisfied often makes reviewing courts loathe to second-guess probable cause determinations by either the police or magistrate [*802] judges. n63 This has led to increasingly deferential review of probable cause decisions, which then in turn contributes to the elusiveness of the probable cause standard. For example, in the case of searches where a warrant is required, the police affidavit must contain information allowing a person of reasonable caution to believe that evidence will be found in the place to be searched. n64 Then, the magistrate judge must find that, "given all the circumstances set forth in the affidavit ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." n65 Great deference is later given to the magistrate's issuance of a warrant by a reviewing court, n66 which determines whether the magistrate's decision is supported by "a substantial basis." n67

This deference, combined with a vague standard, does not promote uniformity in magistrate judges' decisions. n68 The deference might be appropriate if reviewing courts were simply deferring to a magistrate judge's assessment as to whether the facts at issue, based on the totality of the circumstances, surpassed a known probable cause threshold. However, because the probable cause hurdle is so vague, reviewing courts cannot know the degree of suspicion on which the magistrate judge relied in issuing a warrant. n69 Is that magistrate basing his ruling on the [*803] fact that a reasonable officer has to believe that evidence will be found by greater than 50%, and a "fair probability" determination by the magistrate judge allows for some room for disagreement among reasonable police officers? n70 Reviewing courts, which decide whether a "substantial basis" supports the magistrate's decision, n71 do not even know how much suspicion the magistrate believed was required before rendering his decision.

The probable cause standard's imprecision at various levels of review is also partially responsible for the "good-faith exception" to the exclusionary rule, n72 which, in turn, contributes to the indeterminacy of the standard. Although the exclusionary rule requires the "fruits" of unlawful searches to be suppressed at trial, the good faith exception permits the admission of evidence found pursuant to a search warrant not supported by probable cause, so long as law enforcement reasonably relied on the warrant. n73 A reviewing court can therefore find under certain circumstances that even if a substantial basis did not exist for the magistrate's determination, any evidence found may still form the basis of a criminal conviction. n74 The good faith exception means all evidence found pursuant to a warrant will be admitted unless the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." n75

The good faith exception thus almost entirely insulates a magistrate judge's issuance of a warrant from review at the trial or appellate levels. Many reviewing courts simply find that the good faith exception applies [*804] without considering whether the warrant was supported by probable cause. n76 This stymies the development of the law surrounding the probable cause standard in favor of admission of a great deal more evidence. n77 Given that the review of a magistrate judge's probable cause determination is already so deferential, it is difficult to determine in a particular case if probable cause is actually lacking unless it is so obviously lacking that a court must exclude the evidence despite the good faith exception. Although Leon's exception applies only in the warrant context, one scholar has found that searches

conducted pursuant to warrants are much more likely to produce evidence than searches conducted where no warrant is required. n78 Leon's good faith exception, and its progeny, n79 may lead to an erosion of the extra protections that warrants offer. n80 The good faith exception focuses on what a reasonable officer would believe, not whether the probable cause standard was actually met based on the warrant application, n81 thereby bypassing the magistrate's oversight as intermediary between law enforcement's own determination of probable cause and the resulting search. **Unscrupulous or overextended police officers and magistrate judges can easily exploit the uncertainty in the probable cause standard,** [*805] especially when combined with the exceptional deference offered to the initial probable cause determination. n83 Given the lack of oversight over probable cause decisions, the flexibility afforded by the current application of the probable cause standard may not always be a virtue, and may place too much discretion in the hands of police officers at the expense of privacy interests. n84 **According to Professor Ronald Bacigal, "the inability to formulate clear rules or precise probability levels governing probable cause has lead [sic] the Court to adopt one over-arching rule for the police - just use your common sense and act reasonably."** n85 To some extent, this standard contravenes the purpose of the Fourth Amendment, which is to limit police discretion. n86 Although reasonableness is part of the standard, an undefined legal hurdle leads to variability in how much suspicion is deemed "reasonable," allowing for perhaps unjustified amounts of police discretion.

AT But We Use Reasonable Suspicion

Reasonable suspicion is an even lower standard than probable cause

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, *37 Sw. U. L. Rev. 1091, 1124-31*, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15

Roughly defined, individualized suspicion is the idea that the state should judge each citizen based upon his own unique actions, character, thoughts, and situation.⁵ The state should not base its judgments on stereotypes, assumptions, guilt-by-association, or other generalities.⁶ As central as individualized suspicion is to defining probable cause, however, such suspicion also plays a role in cognate concepts, primarily “reasonable suspicion.”⁷ Accordingly, fully understanding individualized suspicion requires examining both probable cause and its junior partner, reasonable suspicion. That partner is generally defined as a sort of “probable cause light,” resting on a lower level of certainty and weaker data sources than probable cause, but otherwise retaining its core commitment to individualized treatment.⁸ Understanding the Court’s approach to such matters sets the stage for the conceptual discussion that follows.

Reasonable suspicion is almost no standard at all

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, *37 Sw. U. L. Rev. 1091, 1124-31*, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15

Yet the Court, as well as lower courts, pays “lip service” in other cases too, insisting that it is retaining and vigorously applying a rule of individualized suspicion while doing no such thing. For example, the Court sometimes finds a small number of generalizations alone sufficient to establish individualized reasonable suspicion, as it infamously did in holding that unprovoked flight from the police in high-crime (generally meaning poor, predominantly racialminority-populated) areas, but not low-crime ones, alone establishes reasonable suspicion to stop a suspect.⁵² Generalizations whose accuracy are themselves belied by empirical evidence, at least according to the dissenters in that case and to several commentators.⁵³ Lower courts seem to have taken this and other holdings of the Court as a signal, repeatedly finding “individualized” reasonable suspicion on the most general of evidence.

Reasonable suspicion only requires showing a “moderate chance” of finding evidence

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, *37 Sw. U. L. Rev. 1091, 1124-31, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15*

The United States Supreme Court found a violation of Savana's Fourth Amendment rights. The Court relied specifically on its probable-cause jurisprudence, at least concerning how reliable, credible, and specific the information upon which the state relied had to be to establish the necessary individualized suspicion.¹⁷ The Court did note, however, that probable cause requires sufficient proof of a “substantial chance” of discovering evidence of criminality, while the lesser school-searches standard of reasonable suspicion “could as readily be described as a moderate chance of finding evidence of wrongdoing.”¹

Reasonable suspicion is a lesser standard than probable cause

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, *37 Sw. U. L. Rev. 1091, 1124-31, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15*

Moreover, despite the particularly intrusive nature of the strip search,³² the Court has applied a similarly vigorous approach to individualized suspicion in several other less-troubling circumstances.³³ Redding would also suggest that the Court is likely to even more aggressively defend the individualized-suspicion requirement in probable-cause cases because reasonable suspicion is a lesser standard than probable cause.

Courts won't even require reasonable suspicion as long as the government says it was an administrative search

Andrew E. Taslitz, 2008, law professor, Howard, Wrongly Accused Redux: How Race Contributes to Convicting the Innocent: The Informants' Example, 37 *Sw. U. L. Rev.* 1091, 1124-31, http://dh.howard.edu/cgi/viewcontent.cgi?article=1011&context=law_fac, DOA: 7-29-15

The Court itself has often readily dispensed entirely with an individualized-suspicion mandate. At first, it did this largely in “special needs” or “administrative search” cases, those whose “primary objective programmatic purpose” was other than criminal investigation.³⁵ Examples include random drug testing for individuals in safety-sensitive jobs, health and safety inspections, and inventory searches.³⁶ Next, it expanded these “special needs” searches and seizures to contexts that would seem to the layperson to be at least partly criminal investigation but that the Court insisted “primarily” involved other purposes. These searches and seizures included drunk-driving roadblocks, searches of automobile junkyards for stolen property, and even searches of probationers and parolees for contraband (likely resulting in revocation of their probation or parole and prosecution for a new offense) or evidence of other crimes.³⁷ The Court has also eliminated any individualized-suspicion requirement for some clear criminal searches, such as searches incident to arrest and consent searches,³⁸ and has repeatedly expanded the arguably watered-down version of individualized suspicion, namely reasonable suspicion, from its roots in *Terry v. Ohio* “stop-and-frisks”³⁹ to a wide range of other contexts.⁴⁰

The government will just say it is an administrative search

David Kravitz, August 28, 2012, Wired, “We Don’t Need No stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena,” <http://www.wired.com/2012/08/administrative-subpoenas/>

When Golden Valley Electric Association of rural Alaska got an administrative subpoena from the Drug Enforcement Administration in December 2010 seeking electricity bill information on three customers, the company did what it usually does with subpoenas — it ignored them.

That's the association's customer privacy policy, because administrative subpoenas aren't approved by a judge.

But by law, utilities must hand over customer records — which include any billing and payment information, phone numbers and power consumption data — to the DEA without court warrants if drug agents believe the data is "relevant" to an investigation. So the utility eventually complied, after losing a legal fight earlier this month.

Meet the administrative subpoena (.pdf): With a federal official's signature, banks, hospitals, bookstores, telecommunications companies and even utilities and internet service providers — virtually all businesses — are required to hand over sensitive data on individuals or corporations, as long as a government agent declares the information is relevant to an investigation. Via a wide range of laws, Congress has authorized the government to bypass the Fourth Amendment — the constitutional guard against unreasonable searches and seizures that requires a probable-cause warrant signed by a judge.

In fact, there are roughly 335 federal statutes on the books (.pdf) passed by Congress giving dozens upon dozens of federal agencies the power of the administrative subpoena, according to interviews and government reports. (.pdf)

"I think this is out of control. What has happened is, unfortunately, these statutes have been on the books for many, many years and the courts have acquiesced," said Joe Evans, the utility's attorney.

Anecdotal evidence suggests that federal officials from a broad spectrum of government agencies issue them hundreds of thousands of times annually. But none of the agencies are required to disclose fully how often they utilize them — meaning there is little, if any, oversight of this tactic that's increasingly used in the war on drugs, the war on terror and, seemingly, the war on Americans' constitutional rights to be free from unreasonable government trespass into their lives.

That's despite proof that FBI agents given such powers under the Patriot Act quickly began to abuse them and illegally collected Americans' communications records, including those of reporters. Two scathing reports from the Justice Department's Inspector General uncovered routine and pervasive illegal use of administrative subpoenas by FBI anti-terrorism agents given nearly carte blanche authority to demand records about Americans' communications with no supervision.

When the 9th U.S. Circuit Court of Appeals, perhaps the nation's most liberal appeals court based in San Francisco, ordered Golden Valley to fork over the data earlier this month, the court said the case was "easily" decided because the records were "relevant" to a government drug investigation.

With the data the Alaska utility handed over, the DEA may then use further administrative subpoenas to acquire the suspected indoor-dope growers' phone records, stored e-mails, and perhaps credit-card purchasing histories — all to build a case to acquire a probable-cause warrant to physically search their homes and businesses.

But the administrative subpoena doesn't just apply to utility records and drug cases. Congress has spread the authority across a huge swath of the U.S. government, for investigating everything from hazardous waste disposal, the environment, atomic energy, child exploitation, food stamp fraud, medical insurance fraud, terrorism, securities violations, satellites, seals, student loans, and for breaches of dozens of laws pertaining to fruits, vegetables, livestock and crops.

Not one of the government agencies with some of the broadest administrative subpoena powers Wired contacted, including the departments of Commerce, Energy, Agriculture, the Drug Enforcement Administration and the FBI, would voluntarily hand over data detailing how often they issued administrative subpoenas

AT “Nothing to Hide”

Privacy is not about hiding bad deeds, but is essential for individuality and self-determination,

Richards, 2015,

Neil M., Professor of Law, Washington University. “Four Privacy Myths” Revised form, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2427808>

A second reason why the “Nothing to Hide” argument is misleading is that it reduces privacy to an individual’s right to hide big secrets. Such a crude reduction of the issue ignores both the complexity of privacy, as well as the social value that comes from living in a society that not everything about us is publicly available all of the time. This is the insight of legal scholar Daniel Solove in his book “Nothing to Hide.” Solove shows how thinking of privacy as the hiding of discreditable secrets by individuals is a mistake because privacy is about more than hiding secrets, and can mean a wide variety of things. Moreover, he notes that “privacy is “often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone.”⁶⁴ Privacy, in this view, is a social value rather than merely an individual one. Rather than thinking about privacy as merely the individual right to hide bad deeds, we should think more broadly about the kind of society we want to live in. A society in which everyone knew everything about everyone else would be oppressive because it would place us all under the glare of publicity all the time; there would be no “free zones for individuals to flourish.”⁶⁵ Legal scholar Julie Cohen goes further, arguing that privacy is necessary for humans to be able to decide who they are. In Cohen’s account, our selves are fluid, constantly being built and changed by our activities, thoughts, and interactions with other people. Privacy, in her view, shelters the development of our dynamic selves “from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable.” Privacy protects our ability to manage boundaries between ourselves and others so that self-determination is possible.⁶⁶ It helps us avoid the calculating, quantifying tyranny of the majority. **Privacy is thus essential for individuality and self-determination, with substantial benefits for society.**

AT “Posner – Balancing Good”

The Constitution enshrines fundamental principles as side constraints that guide cost-benefit policy analysis. It’s not just a question of balancing — Posner is wrong.

Cole 7 — David Cole, Professor at Georgetown University Law Center, has litigated many significant constitutional cases in the Supreme Court, holds a J.D. from Yale Law School, 2007 (“How to Skip the Constitution”: An Exchange,” *New York Review of Books*, January 11th, Available Online at <http://www.nybooks.com/articles/archives/2007/jan/11/how-to-skip-the-constitution-an-exchange/>, Accessed 06-28-2015)

More generally, Judge Posner shies away from his own constitutional theory when he says that to declare a practice constitutional is not the same as saying that it is desirable as a policy matter. That is certainly true as a theoretical matter, at least where one’s constitutional theory is not reducible to one’s policy preferences. But as my review points out, Posner views questions of constitutionality as simply a matter of weighing all the costs and benefits, which is surely the same utilitarian calculus the policymaker would use to determine whether a practice is desirable. Under Posner’s approach, then, it’s hard to see why there would be any room between what is desirable and what is constitutional. Judge Posner accuses me, in effect, of subscribing to the same constitutionalism-as-policy approach that he uses by asserting, without evidentiary support, that my constitutional views simply track my own policy preferences; “the rest is rhetoric.” But I believe that there is a critical distinction between constitutionalism and mere policy preferences. In fact, our Constitution gives judges the authority to declare acts of democratically elected officials unconstitutional on the understanding that they do not simply engage in the same cost-benefit analyses that politicians and economists undertake. My own view is that the very sources Judge Posner dismisses—text, precedent, tradition, and reason—are absolutely essential to principled constitutional decision-making. Posner suggests that because none of these elements necessarily provides a determinate answer to difficult questions, we may as well abandon them for his seat-of-the-pants, cost-benefit approach. It is true that text, precedent, tradition, and reason do not determine results in some mechanistic way. That is why we ask judges, not machines, to decide constitutional cases. But these sources are nonetheless critically important constraints on and guides to constitutional decision-making. They are what identify those principles that have been deemed fundamental—and therefore constitutional—over our collective history. That there are differences over principle in no way excludes the need for reasoned argument about them. There is a reason the framers of the Constitution did not simply say “the government may engage in any practice whose benefits outweigh its costs,” as Judge Posner would have it, but instead struggled to articulate a limited number of fundamental principles and enshrine them above the everyday pragmatic judgments of politicians. They foresaw what modern history has shown to be all too true—that while democracy is an important antidote to tyranny, it can also facilitate a particular kind of tyranny—the tyranny of the majority. Constitutional principles protect those who are likely to be the targets of such tyranny, such as terror suspects, religious and racial minorities, criminal defendants, enemy combatants, foreign nationals, and, especially in this day and age, Arabs and Muslims. Relegating such individuals to the mercy of the legislature—whether it be Republican or Democratic—denies that threat. The Constitution is about more than efficiency, and more than democracy; it is a collective commitment to the equal worth and dignity of all human beings. To call that mere “rhetoric” is to miss the very point of constitutional law.

AT Corporate privacy violations are worse

Government surveillance is much more important than private surveillance – it has a greater reach and far more powerful consequences attached.

Heymann 2015,

Philip B. James Barr Ames Professor of Law, Harvard Law School. Professor Heymann served as Deputy Attorney General in the first Clinton Administration. “An Essay On Domestic Surveillance” Lawfare Research Paper Series Vol 3.2, <http://www.lawfareblog.com/wp-content/uploads/2013/08/Lawfare-Philip-Heymann-SURVEILLANCE-for-publ-10-May-2015.pdf>

Is Government Surveillance Particularly Important? Why should we care particularly about government surveillance in a world where private surveillance on the internet and the information and predictions that can be derived from a mass of such information are driving much of the economy of the internet as companies seek knowledge useful for developing and selling new products? Government surveillance has far greater reach, FBI and other law enforcement agents can – without any need of a predicate or judicial warrant – do whatever private individuals are allowed to do to discover information, using one of the “not-a-search” exceptions. But they can do much more. They can demand, with the assistance of a federal prosecutor, any records that “might” be useful to a grand jury – a standard much more far-reaching than probable cause or reasonable suspicion. The government can be, and is, empowered to demand access to any records kept by third parties, including the vast array of electronic records now kept by businesses about their customers. What private businesses can obtain by requiring a waiver of privacy rights as a condition of access to their goods or services, the government can also obtain without even that strained form of consent and without the alerting knowledge that consent gives to the individual being monitored. The government is allowed to use informants and undercover agents in a way that is not available to businesses. The government can and does develop technology, such as drones, which can greatly increase its powers to observe the activities of individuals. All of this can be done without any special showing of need and without getting a judge’s certificate that a required predicate such as “probable cause” is met. With a predicate and a judicial warrant, the government can search places or activities, such as electronic communications, that no private individual can search without consent. The government also has capacities to use information it acquires in ways far more frightening and more likely to be hostile than those of a company seeking to make you a loyal customer. It can turn suspicions into investigations, arrest and search with probable cause; it can deny appointments or other discretionary benefits, insist on cumbersome formalities when you cross U.S. borders, and influence the actions of others by making obvious its suspicion of, or attention to, particular individuals. It can store data to be used for any of these purposes or for noncriminal forms of regulation. The special powers of the government to obtain information and the special dangers to individuals associated with discretionary uses of that information go far to explain why we have a 4th and a 5th Amendment in the Bill of Rights. The history of the 4th and 5th Amendments is a history of enduring fears of governmental surveillance.

Government surveillance is worse – there's no opt-out and government force carries greater weight.**Fung '13**

Brian Fung covers technology for The Washington Post, focusing on telecom, broadband and digital politics. Before joining the Post, he was the technology correspondent for National Journal and an associate editor at the Atlantic. “Yes, there actually is a huge difference between government and corporate surveillance” – Washington Post - November 4, 2013 - <http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/yes-there-actually-is-a-huge-difference-between-government-and-corporate-surveillance/>

Yes, there actually is a huge difference between government and corporate surveillance When it comes to your online privacy — or what little is left of it — businesses and governments act in some pretty similar ways. They track your credit card purchases. They mine your e-mail for information about you. They may even monitor your movements in the real world. Corporate and government surveillance also diverge in important ways. Companies are looking to make money off of you, while the government aims to prevent attacks that would halt that commercial activity (along with some other things). But the biggest difference between the two has almost no relation to who's doing the surveillance and everything to do with your options in response. Last week, we asked you whether you'd changed your online behavior as a result of this year's extended national conversation about privacy — and if so, which form of snooping annoyed you more. Looking through the responses so far, this one caught my eye: The government because I can't *choose* not to be spied on by them. The government also has the power to kill or imprison me which no private company has. I am a firm believer that our founding fathers created a system that respected individual privacy and to see it eroded by the federal government concerns me deeply. I am a strong believer in the 1st, 2nd, 4th and 5th amendments. Putting aside the government's power to capture or kill, your inability to refuse the government is what distinguishes the NSA from even the nosiest companies on Earth. In a functioning marketplace, boycotting a company that you dislike — for whatever reason — is fairly easy. Diners who object to eating fake meat can stop frequenting Taco Bell. Internet users that don't like Google collecting their search terms can try duckduckgo, an anonymous search engine. By contrast, it's nearly impossible to simply pick up your belongings and quit the United States. For most people, that would carry some significant costs — quitting your job, for instance, or disrupting your children's education, or leaving friends and family. Those costs can be high enough to outweigh the benefits of recovering some hard-to-measure modicum of privacy. Besides, leaving the country would ironically expose you to even greater risk of surveillance, since you'd no longer be covered by the legal protections granted to people (even foreign terror suspects) that arrive to U.S. shores. There are still some ways to shield yourself from the NSA. To the best of our knowledge, the government has yet to crack the encryption protocols behind Tor, the online traffic anonymizing service. But Tor's users are also inherently the object of greater suspicion precisely because they're making efforts to cover their tracks. In the business world, no single company owns a monopoly over your privacy. The same can't really be said about the government.

Government violations are worse. Even if they're now - corporate privacy violations shouldn't condone government violations.**Sklansky '2,**

David A. Sklansky is an Associate Dean and Professor of Law. UCLA School of Law. “BACK TO THE FUTURE: KYLLO, KATZ, AND COMMON LAW” - University of California, Los Angeles School of Law Research Paper Series. Mississippi Law Journal, Forthcoming Research Paper No. 02-17 - July 27. 2002 - www.isrcl.org/Papers/sklansky.pdf

There are two relatively straightforward ways out of this dilemma, but both would require the Supreme Court to rethink certain aspects of Fourth Amendment law.²⁵² The first and simplest way out would be to recognize that government surveillance differs from private snooping, and therefore that the latter, no matter how common, should not eliminate protection against the former. This was the approach one lower court took when it found that government agents intruded on a reasonable expectation of privacy by using a telescope to peer into a suspect's apartment. The court expressly rejected the government's claim that any expectation of privacy was rendered unreasonable by the widespread use of telescopes by private citizens to spy on people living in high-rises. Private snooping, the court reasoned, had "no bearing" on the legality of government surveillance, because the government spies "for different purposes than private citizens." and sometimes "with more zeal." Accordingly, a person's "lack of concern about intrusions from private sources has little to do with an expectation of freedom from systematic governmental surveillance," and "[t]he fact that Peeping Toms abound does not license the government to follow suit."²⁵³

AT Privacy Invasions Inevitable

Privacy isn't dead. Privacy protections happen all the time, its just a question of where we expect privacy.

Neil M. Richards, Professor of Law, Washington University, **04-24-14**

A World Without Privacy: Four Privacy Myths Pgs. 5-7

This brings us to the present day, in which we understand that another series of threats to privacy to signal another Death of Privacy. The continued growth of digital technologies after the 1960s produced the personal computer boom of the 1980s, the Web boom of the late 1990s, and the explosion of cell and smart phones in the 2000s. We are now witnessing the beginnings of the “Internet of Things,” in which millions and then billions of electronic devices will connect to the Internet, collecting and relaying unimaginably large amounts of data. At the same time, the terrorist attacks of 9/11 and 7/7, among others, have energized security services across the democratic world. Today we see levels of surveillance of the citizens of democratic societies that would previously have been politically and technically unimaginable. Edward Snowden and Glenn Greenwald’s revelations about the scale of surveillance by the National Security Agency have prompted a global debate about surveillance and privacy that has produced front-page news for over six months. But surely privacy is really dead now? Surely we face the end of any notions of privacy, right? No. I’d like to suggest, to the contrary, that Privacy Is Not Dead. Privacy is one of the most important questions facing us as a society.

Privacy is actually very much alive. But it all depends on what we mean by “privacy.” Privacy can of course mean many things. If we mean merely “how much information people know about us,” then privacy is shrinking. But this is a very narrow and unhelpful way of understanding privacy. Let’s take a step back from the Internet of Things and digital privacy Armageddon for a moment. Certainly, many of the kinds of things we call “privacy” aren’t currently threatened by new digital technologies and are very much alive. At a general level, we still put locks on our houses, we still wear clothes, and we still use doors to keep the general public out of our bathroom and bedroom. We require the government to get a warrant before it enters our home and (NSA revelations notwithstanding) wiretaps our phone, and reads our mail (whether electronic or paper). We expect our lawyers and our therapists to keep our confidences in trust, and expect our accountant and our bank to do the same with our financial details. We expect our doctors to do the same with information about our health, and while we realize that many of our health records are now electronic, we don’t expect them to become available on a Google search or left lying carelessly around on a laptop at the airport. The fact that data breaches are newsworthy (and cause substantial personal, legal and business harm) supports these expectations rather than diminishes them. What about the argument that information technology is inevitably gobbling up privacy, causing the zone of our privacy to dwindle to almost nothing? To answer that question, let’s look at our previous privacy panics. Warren and Brandeis were worried about gossip columnists and so-called “Kodakers lying in wait.”¹⁸ These phenomena still exist today, but they were managed by changes in law and social norms, and by the passage of time. Today, we have rules governing journalistic breaches (though in the United States such rules sometimes conflict with the First Amendment), and we have rules preventing stalking or overzealous tactics by the paparazzi. Similarly, commentators in the 1960s were worried by wiretapping, the creation of data banks, and the processing of personal data. These phenomena exist today, but they have also been managed (at least in their pre-internet forms) by changes in law and social norms, and by the passage of time. I’d like to suggest that our ongoing worries about the Death of Privacy (privacy’s century-old melodramatic death throes) are really an ongoing social and legal conversation about how to manage some of the costs caused by changes in information technologies.

Privacy is not dead, its just complex – we need to figure out the balance.

Richards, 2015,

Neil M., Professor of Law, Washington University. “Four Privacy Myths” Revised form, "A

"World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2427808>

My purpose in these examples is not to pick on these organizations. On the contrary, when used appropriately, privacy rules like trade and government secret protection can advance important social interests. I am trying instead to make a point that is easy to overlook: When the very entities that are used as exemplars of the “Death of Privacy” use suites of robust legal tools to preserve their own privacy, it makes no sense to claim that privacy is dead. On the contrary, these examples show that privacy is a complex phenomenon, and that we should be talking about the balance between different kinds of privacies and different rules for managing flows of information rather than privacy’s demise. When viewed from this perspective, neither Facebook nor the NSA reject privacy; on the contrary, they have a complicated relationship to privacy, embracing (like to many other people and institutions) privacy for themselves but somewhat less privacy for others, especially where they have institutional incentives to make money or protect government interests.

AT Liberalist Conception of Privacy is Bad

Privacy isn't just about individual rights.

Cohen, 2013 Julie E., Professor Georgetown University Law Center “What Privacy Is For.” Harvard Law Review, Vol. 126, 2013. Available at SSRN: <http://ssrn.com/abstract=2175406>

Privacy rights protect individuals, but to understand privacy simply as an individual right is a mistake. The ability to have, maintain, and manage privacy depends heavily on the attributes of one's social, material, and informational environment. Recall that privacy in the dynamic sense is "an interest in breathing room to engage in socially situated processes of boundary management. That interest has distinct structural entailments that efforts to design effective legal protection for privacy must acknowledge. In addition, privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy. The paradigm of "new privacy governance" that has been evolving within the U.S. legal system is unlikely to serve individual or public interests in privacy well, because it is rooted in a regulatory ideology that systematically downplays the need to hold market actors accountable for harms to the public interest. Effective privacy protection must target the qualities of seamlessness and opacity that together enable modulation.

Privacy is necessary for overlapping humanistic, political, and instrumental concerns

Bennet 8 (Colin J., “The Privacy Advocates”, Chapter 1: Framing the Problem, p. 4-5)

It is therefore useful to reflect on the purposes for the assertion of privacy claims. In previous work, I have distinguished among three overlapping dimensions of the problem: humanistic, political, and instrumental (Bennett 1992, 22–37). Fundamentally, privacy claims are made for humanistic reasons. Here the essential concern is to protect the dignity, individuality, integrity, or private personality of each and every one of us, regardless of wider implications or consequences. This notion corresponds broadly to what James 1(11)e and his colleagues mean by an “aesthetic” conception of privacy or “the restriction of personal information as an end in itself” (Rule et al. 19X0, 22). The fundamental issue is loss of human dignity, respect, and autonomy that results when one loses control over the circumstances under which one’s space, behavior, decisions, or personal information is intruded upon. These conceptions are at the heart of the privacy movement in virtually every democratic state. A second dimension, however, is explicitly political. Privacy plays important functions within liberal democratic societies by preventing the total politicizing of life; it promotes the freedom of association it shields scholarship and science from unnecessary interference by government; it permits and protects the use of a secret ballot; it restrains improper police conduct such as compulsory self-incrimination and “unreasonable searches and seizures”; and it serves also to shield those institutions, such as the press, that operate to keep government accountable (Westin 1967, 25). In a similar vein, Paul Schwartz (1999) has advanced a similar theory of “constitutive privacy” to protect the ability of individuals to speak freely and participate in public life on the Internet. A third, and somewhat different, purpose is an instrumental, functional, or strategic one. The promotion of privacy may also serve to ensure that, in Paul Sieghart’s terms, “the right people use the right data for the right purposes” (1976, 76). When anyone of those conditions is absent, critical rights, interests, and services might be jeopardized. This is an

explicit concern about information, but it expresses a fundamental assumption that if you can protect the information on which decisions are made about individuals, you can also protect the fairness, integrity, and effectiveness of that decision-making process. In contrast to the first two concerns, this aspect of the problem stems not so much from the collection of personal data as from its use and dissemination. In this view, organizations can collect as much personal information as they like, provided there are adequate procedures in place to make sure that the “right people use it for the right purposes.”

AT Government Won't Abuse Collected Data

Past surveillance has targeted people for their political beliefs

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Frank Church's mid-1970s investigation into the FBI's spying shockingly found that the agency had labeled half a million US citizens as potential "subversives," routinely spying on people based purely on their political beliefs. (The FBI's list of targets ranged from Martin Luther King to John Lennon, from the women's liberation movement to the anti-Communist John Birch Society.) Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 65-68). Henry Holt and Co.. Kindle Edition.

History and human nature prove surveillance will be abused unless it is kept in check

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Frank Church's mid-1970s investigation into the FBI's spying shockingly found that the agency had labeled half a million US citizens as potential "subversives," routinely spying on people based purely on their political beliefs. (The FBI's list of targets ranged from Martin Luther King to John Lennon, from the women's liberation movement to the anti-Communist John Birch Society.) But the plague of surveillance abuse is hardly unique to American history. On the contrary, mass surveillance is a universal temptation for any unscrupulous power. And in every instance, the motive is the same: suppressing dissent and mandating compliance. Surveillance thus unites governments of otherwise remarkably divergent political creeds. At the turn of the twentieth century, the British and French empires both created specialized monitoring departments to deal with the threat of anticolonialist movements. After World War II, the East German Ministry of State Security, popularly known as the Stasi, became synonymous with government intrusion into personal lives. And more recently, as popular protests during the Arab Spring challenged dictators' grasp on power, the regimes in Syria, Egypt, and Libya all sought to spy on the Internet use of domestic dissenters. Investigations by Bloomberg News and the Wall Street Journal have shown that as these dictatorships were overwhelmed by protestors, they literally went shopping for surveillance tools from Western technology companies. Syria's Assad regime flew in employees from the Italian surveillance company Area SpA, who were told that the Syrians "urgently needed to track people." In Egypt, Mubarak's secret police bought tools to penetrate Skype encryption and eavesdrop on activists' calls. And in Libya, the Journal reported, journalists and rebels who entered a government monitoring center in 2011 found "a wall of black refrigerator-size devices" from the French surveillance company Amesys. The equipment "inspected the Internet traffic" of Libya's main Internet service provider, "opening emails, divining passwords, snooping on online chats and mapping connections among various suspects." The ability to eavesdrop on people's communications vests immense power in those who do it. And unless such power is held in check by rigorous oversight and accountability, it is almost certain to be abused. Expecting the US government to operate a massive surveillance machine in complete secrecy without falling prey to its temptations runs counter to every historical example. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 83-84). Henry Holt and Co.. Kindle Edition.

In Europe, collected data has been used to harm innocent civilians

News & Observer, May 16, 2014, <http://www.newsobserver.com/2014/05/16/3867496/drescher-who-owns-your-personal.html> DOA: 2-22-15

The German reaction to the NSA leaks reveals a sharp difference between Europeans and Americans on issues related to technology and personal data, said Ralf Poscher, a law professor at Albert-Ludwigs-University of Freiburg. “Americans don’t understand Europeans’ outrage,” Poscher told a group of German and U.S. journalists gathered by the Robert Bosch Foundation of Germany last week. “Europeans don’t understand Americans’ indifference.” Europeans view their personal data as their own property, Poscher said. Their experiences with totalitarian regimes cause them to anticipate harm. This is especially true in Germany, where the Gestapo (the secret police of Nazi Germany) and the Stasi (the ruthlessly effective East German police) used personal information to harm people they viewed as dangerous or political opponents.

Americans haven’t had the same widespread experiences with secret police. Europeans want a legal remedy that prevents future abuse of personal information. Americans, Poscher said, are more inclined to address these types of privacy problems as they arise, confident that their legal system will resolve them.

Metadata is the basis of decisions used to kill people abroad

Press TV, May 14, 2014, <http://www.presstv.ir/detail/2014/05/14/362621/nsa-metadata-abuse-of-us-public-rights/> DOA: 2-20-15

NSA claims that this is permissible since the content of the calls are not collected, while the opponents of the program say the metadata alone is more than enough to reveal vast amounts of personal information. On Tuesday, former CIA director, Michael Hayden, admitted that Washington uses the metadata as the basis for killing people. Metadata is a reference to the information collected by the NSA from American citizens and “suspected militants” in other countries. The US uses the data to select targets for drone strikes around the world.

According to documents leaked by former NSA contractor, Edward Snowden, the agency analyzes metadata as well as mobile-tracking technology to determine targets, without employing human intelligence to confirm a suspect’s identity.

Government abusing power now

Conor Friedersdorf, May 14, 2014, The Atlantic, “No Place to Hide: A Conservative Critique of the Radical NSA,” <http://www.theatlantic.com/politics/archive/2014/05/on-nsa-surveillance-glenn-greenwald-is-not-the-radical/370830/>

So why is he widely considered a radical? In part because the press in America largely refuses to entertain the possibility that the U.S. government itself has taken a radical turn. Under this logic, someone criticizing the Bush and Obama administrations with harsh, extreme language must be the radical. Never mind that since September 11, 2001, the U.S. has tortured prisoners, indefinitely detained innocents without charges or trial, invaded and occupied a country on false pretenses, used the Espionage Act to prosecute more Americans than all former administrations combined, engaged in illegal warrantless wiretapping, and created a clandestine kill list that includes Americans. Strident, outraged dissents from those policies are not radical—the policies themselves are radical. Opposing them is traditionally conservative and classically liberal. As Cole eloquently explains, "the NSA is an agency out of control. In some sense, it has always been ... mostly operating abroad, under limited constraints. But in the old days, if law didn't much constrain it, technical limitations did. These documents show that the digital age has exponentially increased the NSA's technical ability to track the details of our most private lives. What is now needed are laws that ensure that the NSA can do the work it needs to do while respecting the privacy rights of Americans and non-Americans alike. Greenwald offers no solutions, but effectively raises the alarm. But if we don't come up with solutions, the data revolution will render privacy a rusty relic of a bygone era."

Mass surveillance was abused in Germany

Los Angeles Times, May 5, 2014, <http://www.latimes.com/business/la-fi-lazarus-20140506-column.html> DOA: 2-20-15

Who are these radical opponents? And given how marginalized and powerless they are, how could they possibly pose just as great a threat to our liberties as the types who uncritically supported surveilling everyone from Martin Luther King to anti-war protestors to virtually every American who places telephone calls? It's easy to find even more horrific abuses of surveillance in world history. Germany alone had the Nazis and the Stasi. What's the most actual harm that's been done by radical opponents of government surveillance? Any equivalence here is false.

Many with dissenting views, not just bad people, have been placed under surveillance

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

But that view radically misunderstands what goals drive all institutions of authority. "Doing something wrong," in the eyes of such institutions, encompasses far more than illegal acts, violent behavior, and terrorist plots. It typically extends to meaningful dissent and any genuine challenge. It is the nature of authority to equate dissent with wrongdoing, or at least with a threat. The record is suffused with examples of groups and individuals being placed under government surveillance by virtue of their dissenting views and activism—Martin Luther King, the civil rights movement, antiwar activists, environmentalists. In the eyes of the government and J. Edgar Hoover's FBI, they were all "doing something wrong": political activity that threatened the prevailing order. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2524-2526). Henry Holt and Co.. Kindle Edition.

Hoover used surveillance against dissent

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Given those guarantees, Hoover instituted a system to prevent dissent from developing in the first place. The FBI's domestic counterintelligence program, COINTELPRO, was first exposed by a group of antiwar activists who had become convinced that the antiwar movement had been infiltrated, placed under surveillance, and targeted with all sorts of dirty tricks. Lacking documentary evidence to prove it and unsuccessful in convincing journalists to write about their suspicions, they broke into an FBI branch office in Pennsylvania in 1971 and carted off thousands of documents. Files related to COINTELPRO showed how the FBI had targeted political groups and individuals it deemed subversive and dangerous, including the National Association for the Advancement of Colored People, black nationalist movements, socialist and Communist organizations, antiwar protesters, and various right-wing groups. The bureau had infiltrated them with agents who, among other things, attempted to manipulate members into agreeing to commit criminal acts so that the FBI could arrest and prosecute them. The FBI succeeded in convincing the New York Times to suppress the documents and even return them, but the Washington Post published a series of articles based on them. Those revelations led to the creation of the Senate Church Committee, which concluded: [Over the course of fifteen years] the Bureau conducted a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence. Many of the techniques used would be intolerable in a democratic society even if all of the targets had been involved in violent activity , but COINTELPRO went far beyond that. The unexpressed major premise of the programs was that a law enforcement agency has the duty to do whatever is necessary to combat perceived threats to the existing social and political order. One key COINTELPRO memo explained that "paranoia" could be sown among antiwar activists by letting them believe there was "an F.B.I. agent behind every mailbox." In this way, dissidents, always convinced that they were being watched, would drown in fear and refrain from activism. Unsurprisingly, the tactic worked. In a 2013 documentary entitled 1971, several of the activists described how Hoover's FBI was "all over" the civil rights movement with infiltrators and surveillance , people who came to meetings and reported back . The monitoring impeded the movement's ability to organize and grow. At the time, even the most entrenched institutions in Washington understood that the mere existence of government surveillance, no matter how it is used, stifles the ability to dissent. The Washington Post, in a March 1975 editorial on the break-in, warned about precisely this oppressive dynamic: The FBI has never shown much sensitivity to the poisonous effect which its surveillance, and especially its reliance on faceless informers, has upon the democratic process and upon the practice of free speech. But it must be self-evident that discussion and controversy respecting governmental policies and programs are bound to be inhibited if it is known that Big Brother, under disguise, is listening to them and reporting them.

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2557-2559). Henry Holt and Co.. Kindle Edition.

Surveillance was abused in the past

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

COINTELPRO was far from the only surveillance abuse found by the Church Committee. Its final report declared that “millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.” Moreover, “some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups” during one CIA operation, CHAOS (1967– 1973). Additionally, “an estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid-1960’s and 1971” as well as some 11,000 individuals and groups who were investigated by the Internal Revenue Service “on the basis of political rather than tax criteria.” The bureau also used wiretapping to discover vulnerabilities, such as sexual activity, which were then deployed to “neutralize” their targets. These incidents were not aberrations of the era. During the Bush years, for example, documents obtained by the ACLU revealed, as the group put it in 2006, “new details of Pentagon surveillance of Americans opposed to the Iraq war, including Quakers and student groups.” The Pentagon was “keeping tabs on non-violent protestors by collecting information and storing it in a military anti-terrorism database.” The ACLU noted that one document, “labeled ‘potential terrorist activity,’ lists events such as a ‘Stop the War NOW!’ rally in Akron, Ohio.” The evidence shows that assurances that surveillance is only targeted at those who “have done something wrong” should provide little comfort, since a state will reflexively view any challenge to its power as wrongdoing. The opportunity those in power have to characterize political opponents as “national security threats” or even “terrorists” has repeatedly proven irresistible. In the last decade, the government, in an echo of Hoover’s FBI, has formally so designated environmental activists, broad swaths of antigovernment right-wing groups, antiwar activists, and associations organized around Palestinian rights. Some individuals within those broad categories may deserve the designation, but undoubtedly most do not, guilty only of holding opposing political views. Yet such groups are routinely targeted for surveillance by the NSA and its partners. Indeed, after British authorities detained my partner, David Miranda, at Heathrow airport under an antiterrorism statute, the UK government expressly equated my surveillance reporting with terrorism on the ground that the release of the Snowden documents “is designed to influence a government and is made for the purposes of promoting a political or ideological cause. This therefore falls within the definition of terrorism.” This is the clearest possible statement of linking a threat to the interests of power to terrorism.

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2581-2582). Henry Holt and Co.. Kindle Edition.

Muslims subject to warrantless surveillance abuse

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

None of this would come as any surprise to the American Muslim community , where the fear of surveillance on the grounds of terrorism is intense and pervasive, and for good reason. In 2012, Adam Goldman and Matt Apuzzo of the Associated Press exposed a joint CIA/ New York Police Department scheme of subjecting entire Muslim communities in the United States to physical and electronic surveillance without the slightest whiff of any suggestion of wrongdoing. American Muslims routinely describe the effect of spying on their lives: each new person who shows up at a mosque is regarded with

suspicion as an FBI informant; friends and family stifle their conversations for fear of being monitored and out of awareness that any expressed view deemed hostile to America can be used as a pretext for investigation or even prosecution. One document from the Snowden files, dated October 3, 2012, chillingly underscores the point. It revealed that the agency has been monitoring the online activities of individuals it believes express “radical” ideas and who have a “radicalizing” influence on others. The memo discusses six individuals in particular, all Muslims, though it stresses that they are merely “exemplars.” The NSA explicitly states that none of the targeted individuals is a member of a terrorist organization or involved in any terror plots. Instead, their crime is the views they express, which are deemed “radical,” a term that warrants pervasive surveillance and destructive campaigns to “exploit vulnerabilities.” Among the information collected about the individuals, at least one of whom is a “U.S. person,” are details of their online sex activities and “online promiscuity”—the porn sites they visit and surreptitious sex chats with women who are not their wives. The agency discusses ways to exploit this information to destroy their reputations and credibility.

Greenwald, Glenn (2014-05-13). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Kindle Locations 2593-2596). Henry Holt and Co.. Kindle Edition.

Personal information that is stored is abused

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, Kindle edition

As the ACLU’s deputy legal director, Jameel Jaffer, observed, the NSA databases “store information about your political views, your medical history, your intimate relationships and your activities online.” The agency claims this personal information won’t be abused, “but these documents show that the NSA probably defines ‘abuse’ very narrowly.” As Jaffer pointed out, the NSA has historically, at a president’s request, “used the fruits of surveillance to discredit a political opponent, journalist, or human rights activist.” It would be “naive,” he said, to think the agency couldn’t still “use its power that way.”

Greenwald, Glenn (2014-05-13). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Kindle Locations 2600-2602). Henry Holt and Co.. Kindle Edition.

US government targets Anonymous and Hacktivists

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, Kindle edition

The treatment of Anonymous, as well as the vague category of people known as “hacktivists,” is especially troubling and extreme. That’s because Anonymous is not actually a structured group but a loosely organized affiliation of people around an idea: someone becomes affiliated with Anonymous by virtue of the positions they hold. Worse still, the category “hacktivists” has no fixed meaning: it can mean the use of programming skills to undermine the security and functioning of the Internet but can also refer to anyone who uses online tools to promote political ideals. That the NSA targets such broad categories of people is tantamount to allowing it to spy on anyone anywhere, including in the United States, whose ideas the government finds threatening. Gabriella Coleman, a specialist on Anonymous at McGill University, said that the group “is not a defined” entity but rather “an idea that mobilizes activists to take collective action and voice political discontent. It is a broad-based global social movement with no centralized or official organized leadership structure. Some have rallied around the name to engage in digital civil disobedience, but nothing remotely resembling terrorism.” The majority who have embraced the idea have done so “primarily for ordinary political expression. Targeting Anonymous and hacktivists amounts to targeting citizens for expressing their political beliefs, resulting in the stifling of legitimate dissent,” Coleman explained. Yet Anonymous has been targeted by a unit of the GCHQ that employs some of the most

controversial and radical tactics known to spycraft: “false flag operations,” “honey-traps,” viruses and other attacks , strategies of deception, and “info ops to damage reputations.” One PowerPoint slide presented by GCHQ surveillance officials at the 2012 SigDev conference describes two forms of attack: “information ops (influence or disruption)” and “technical disruption.” GCHQ refers to these measures as “Online Covert Action,” which is intended to achieve what the document calls “The 4 D’s: Deny/ Disrupt/ Degrade/ Deceive.”

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2629-2634). Henry Holt and Co.. Kindle Edition.

Surveillance undermines the presumption of innocence

Noam Chomsky, MIT, June, 2014, A Surveillance State Beyond Imagination Is Being Created in One of the World's Freest Countries, <http://www.alternet.org/civil-liberties/noam-chomsky-surveillance-state-beyond-imagination-being-created-one-freest> DOA: 2-20-15

As the colossus fulfills its visions, in principle every keystroke might be sent to President Obama's huge and expanding databases in Utah. In other ways too, the constitutional lawyer in the White House seems determined to demolish the foundations of our civil liberties. The principle of the presumption of innocence, which dates back to Magna Carta 800 years ago, has long been dismissed to oblivion. Recently The New York Times reported the "anguish" of a federal judge who had to decide whether to allow the force-feeding of a Syrian prisoner who is on a hunger strike to protest his imprisonment.

AT Conception of Privacy is Sexist

Privacy isn't sexist

Lever 12

[Annabelle Lever is an associate professor if Normative Political Theory at the University of Geneva in Switzerland; 2012]

But while MacKinnon is right that legal protections of privacy have often had these effects, it is less clear that this makes privacy inherently, and irremediably, sexist, as she implies. On the contrary, many feminists have been moved by Virginia Woolf's claim, in A Room of One's Own, that women's lack of privacy has been a major obstacle to their self-development and self-expression and a potent sign of their second-class status.⁹ So, one could think that MacKinnon is largely right about the way that established philosophical and legal views of privacy have disadvantaged women compared to men—in part, by denying them privacy within their marital and sexual relationships—without supposing that this is unalterable or an inescapable feature of claims to privacy. We therefore seem to be faced with the question whether it is possible to draw any conclusions about the value of privacy, or will we just find that any claims we make about its value—however tentative and provisional—are doomed to failure? The answer to the first question, I think, is 'yes', and to the second question, is 'no'. Specifically, I will suggest that we can construct a democratic perspective on privacy out of fairly familiar ideas about what makes governments democratic rather than undemocratic, and some widely shared assumptions about the reasons to favor the former over the latter. This will give us some much needed points of agreement with which to examine competing claims about the nature and value of privacy, and can help us to see which disagreements about privacy we might be able to resolve, and what types of information, reflection or action we would need to resolve them.

AT Security First

Can't trade privacy for security, rights are presumptively more important. Moore, 2011

Adam D. "Privacy, security, and government surveillance: WikiLeaks and the new accountability." *Public Affairs Quarterly* (2011): 141-156.

A counterpart to the "just trust us" view is the "nothing to hide" argument.²³ According to this argument we are to balance the potential for harm of data mining and the like with the security interests of detecting and preventing terrorist attacks. I suppose we could weaken this further by merely referencing "security interests," which would include, but not be limited to, "terrorist attacks." The idea is that our security interests are almost always more weighty than the minimal costs of surveillance—privacy intrusions are a mere nuisance and are easily traded for increases in security. A formal version of the argument might go something like this: P1 When two fundamental interests conflict, we should adopt a balancing strategy, determine which interest is more compelling, and then sacrifice the lesser interest for the greater. If it is generally true that one sort of interest is more fundamental than another, then we are warranted in adopting specific policies that seek to trade the lesser interest for the greater interest. P2. In the conflict between privacy and security, it is almost always the case that security interests are weightier than privacy interests. The privacy intrusions related to data mining or National Security Agency (NSA) surveillance are not as weighty as our security interests in stopping terrorism, and so on—these sorts of privacy intrusions are more of a nuisance than a harm. C3. So it follows that we should sacrifice privacy in these cases and perhaps adopt policies that allow privacy intrusions for security reasons. One could easily challenge Premise 2—there are numerous harms associated with allowing surveillance that are conveniently minimized or forgotten by the "nothing to hide" crowd. Daniel Solove notes that "privacy is threatened not by singular egregious acts but by a slow series of small, relatively minor acts, which gradually begin to add up."²⁴ Solove also points out, as I have already highlighted, that giving governments too much power undermines the mission of providing for security—the government itself becomes the threat to security. The point was put nicely by John Locke: "This is to think, that Men are so foolish, that they take care to avoid what Mischiefs may be done them by Pole-Cats, or Foxes, but are content, nay think it Safety, to be devoured by Lions."²⁵ It is also important to note the risk of mischief associated with criminals and terrorists compared to the kinds of mischief perpetrated by governments—even our government. In cases where there is a lack of accountability provisions and independent oversight, governments may pose the greater security risk. Moreover, there is sensitive personal information that we each justifiably withhold from others, not because it points toward criminal activity, but because others simply have no right to access this information. Consider someone's sexual or medical history. Imagine someone visiting a library to learn about alternative lifestyles not accepted by the majority. Hiding one's curiosity about, for example, a gay lifestyle may be important in certain contexts. This is true of all sorts of personal information like religious preferences or political party affiliations. Consider a slight variation of a "nothing to hide" argument related to what might be called physical privacy. Suppose there was a way to complete body cavity searches without harming the target or being more than a mere nuisance. Perhaps we search the targets after they have passed out drunk. Would anyone find it plausible to maintain a "nothing to hide" view in this case? I think not—and the reason might be that we are more confident in upholding these rights and policies that protect these rights than we are of almost any cost-benefit analysis related to security. Whether rights are viewed as strategic rules that guide us to the best consequences, as Mill would argue, or understood as deontic constraints on consequentialist sorts of reasoning, we are more confident in them than in almost any "social good" calculation. I am not saying that rights are absolute—they are just presumptively weighty. This line of argument is an attack on the first premise of the "nothing to hide" position. Rights are resistant to straightforward cost-benefit or consequentialist sort of arguments. Here we are rejecting the view that privacy interests are the sorts of things that can be traded for security.

Security does not trump privacy.

Moore, 2011

Adam D. "Privacy, security, and government surveillance: WikiLeaks and the new accountability." *Public Affairs Quarterly* (2011): 141-156.

The "Nothing to Hide" Argument

According to what might be called the “security trumps” view, whenever privacy and security conflict, security wins—that is, security is more fundamental and valuable than privacy. First, without arguments, it is not clear why a “security trumps” view should be adopted over a “privacy trumps” view. Privacy or perhaps self-ownership seems at least as fundamental or intuitively weighty as security. Foreshadowing things to come, it is not at all clear—at least in some cases—that privacy does not enhance security and vice versa. Suppose that rights afforded their holders specific sorts of powers. For example, Fred’s privacy rights generate in him a god-like power to completely control access to his body and to information about him. If we had such powers, we would also have increased security. Furthermore, if we had complete security in our bodies and property, including informational security, we would have secured privacy as well. The tension between privacy and security arises because these values cannot be protected by individuals acting alone. Nevertheless, it is important to note that as these services are contracted out to other agents, like governments, we grant these parties power over us—power that may undermine security and privacy. Continuing with the “security trumps” argument, it would seem odd to maintain that any increase in security should be preferred to any increase in privacy or any decrease in privacy is to be preferred to any decrease in security. Such a view would sanction massive violations of privacy for mere incremental and perhaps momentary gains in security. Also, given that others will provide security and power is likely a necessary part of providing security, we have strong prudential reasons to reject the “security trumps” view. If those who provide security were saints, then perhaps there would be little to worry about. The cases already presented are sufficient to show that we are not dealing with saints.\

AT Don't Do Things You Shouldn't Do

Things people do in private aren't all wrong

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

As the experiments showed , there are all sorts of things people do that they are eager to keep private, even though these sorts of things do not constitute doing “something wrong.” Privacy is indispensable to a wide range of human activities. If someone calls a suicide hotline or visits an abortion provider or frequents an online sex website or makes an appointment with a rehabilitation clinic or is treated for a disease, or if a whistle-blower calls a reporter, there are many reasons for keeping such acts private that have no connection to illegality or wrongdoing. In sum, everyone has something to hide. Reporter Barton Gellman made the point this way: Privacy is relational. It depends on your audience. You don’t want your employer to know you’re job hunting. You don’t spill all about your love life to your mom, or your kids. You don’t tell trade secrets to your rivals. We don’t expose ourselves indiscriminately and we care enough about exposure to lie as a matter of course. Among upstanding citizens, researchers have consistently found that lying is “an everyday social interaction” (twice a day among college students, once a day in the Real World).... Comprehensive transparency is a nightmare.... Everyone has something to hide. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2505-2507). Henry Holt and Co.. Kindle Edition.

AT People Don't Care About Privacy

Actions demonstrate that people value their privacy

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

The same contradiction is expressed by the many ordinary citizens who dismiss the value of privacy yet nonetheless have passwords on their email and social media accounts. They put locks on their bathroom doors; they seal the envelopes containing their letters. They engage in conduct when nobody is watching that they would never consider when acting in full view. They say things to friends, psychologists, and lawyers that they do not want anyone else to know. They give voice to thoughts online that they do not want associated with their names. The many pro-surveillance advocates I have debated since Snowden blew the whistle have been quick to echo Eric Schmidt's view that privacy is for people who have something to hide. But none of them would willingly give me the passwords to their email accounts, or allow video cameras in their homes.

Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2328-2329). Henry Holt and Co.. Kindle Edition.

Americans fear surveillance

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

Ample polling data reflected this shift. At the end of July 2013, the Pew Research Center released a poll showing that the majority of Americans disbelieved the defenses offered for the NSA's actions. In particular, “a majority of Americans—56%—say that federal courts fail to provide adequate limits on the telephone and Internet data the government is collecting as part of its anti-terrorism efforts.” And “an even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism.” Moreover, “63% think the government is also gathering information about the content of communications.” Most remarkably, Americans now considered the danger of surveillance of greater concern than the danger of terrorism: Overall, 47% say their greater concern about government anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties, while 35% say they are more concerned that policies have not gone far enough to protect the country. This is the first time in Pew Research polling that more have expressed concern over civil liberties than protection from terrorism since the question was first asked in 2004. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2720-2724). Henry Holt and Co.. Kindle Edition.

AT Metadata Disclosure Doesn't Violate Privacy

Meta data collection at least as intrusive as content collection

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle edition

These disingenuous arguments obscure the fact that metadata surveillance can be at least as intrusive as content interception, and often even more so. When the government knows everyone you call and everyone who calls you, plus the exact length of all those phone conversations; when it can list every single one of your email correspondents and every location from where your emails were sent, it can create a remarkably comprehensive picture of your life, your associations, and your activities, including some of your most intimate and private information. In an affidavit filed by the ACLU challenging the legality of the NSA's metadata collection program, Princeton computer science and public affairs professor Edward Felten explained why metadata surveillance can be especially revealing: Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother ; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call. Even for a single phone call, the metadata can be more informative than the call's content. Listening in on a woman calling an abortion clinic might reveal nothing more than someone confirming an appointment with a generic-sounding establishment ("East Side Clinic" or "Dr. Jones's office"). But the metadata would show far more than that: it would reveal the identity of those who were called. The same is true of calls to a dating service, a gay and lesbian center, a drug addiction clinic, an HIV specialist, or a suicide hotline. Metadata would likewise unmask a conversation between a human rights activist and an informant in a repressive regime, or a confidential source calling a journalist to reveal high-level wrongdoing. And if you frequently call someone late at night who is not your spouse, the metadata will reveal that, too. What's more, it will record not only all the people with whom you communicate and how often, but also all the people with whom your friends and associates communicate, creating a comprehensive picture of your network of contacts. Indeed, as Professor Felten notes, eavesdropping on calls can be quite difficult due to language differences, meandering conversations, the use of slang or deliberate codes, and other attributes that either by design or accident obfuscate the meaning. "The content of calls are far more difficult to analyze in an automated fashion due to their unstructured nature," he argued. By contrast, metadata is mathematical : clean, precise, and thus easily analyzed. And as Felten put it, it is often "a proxy for content": Telephony metadata can ... expose an extraordinary amount about our habits and our associations. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations. In sum, writes Felten, "mass collection not only allows the government to

learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals." Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2061-2063). Henry Holt and Co.. Kindle Edition.

Feinstein (a Congressperson who supports surveillance) won't release her metadata

Glenn Greenwald, attorney & journalist who broke the NSA spying story, May 2014, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Kindle editio

When the Senate Intelligence Committee's chair, Dianne Feinstein, insisted that the NSA's collection of metadata does not constitute surveillance— because it does not include the content of any communication— online protesters demanded that she back up her assertion with action: Would the senator, each month, publish a full list of people she emailed and called, including the length of time they spoke and their physical locations when the call was made? That she would take up the offer was inconceivable precisely because such information is profoundly revealing; making it public would constitute a true breach of one's private realm. Greenwald, Glenn (2014-05-13). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Kindle Locations 2332-2334). Henry Holt and Co.. Kindle Edition.

NSA targeting innocent Americans

Medfa with a Conscience, May 23, 2014, <http://mwcnews.net/focus/politics/41017-america-spies.html>

According to the May 26 issue of "The Nation," whistleblower Snowden thought NSA had become "a runaway surveillance train...without an emergency brake on the inside" and so passed the documentary evidence of its vast wrong-doing on to journalist Glenn Greenwald and documentary film maker Laura Poitras, to be made public. Defending NSA in Capitol Hill testimony, its former Director Gen. Keith Alexander said, "Take away the National Security Agency's ability to tap into telephone records, and the nation is left unsecure." Journalist James Bamford said that when he visited Greenwald in Rio, he was shown a memo (apparently uncovered by Snowden) in which Gen. **Alexander suggested going not after terrorists or criminals but "radicalizers," including innocent Americans, by searching the Internet for their vulnerabilities, such as visits to porn sites.**" Then, by secretly leaking this information, Alexander said, "the NSA could discredit them in the eyes of their followers." (Doesn't a response this foolish make you wonder how the man ever got to run an intelligence agency?) Of course, **many Americans think, "I've done nothing wrong.** Why should I care if the NSA taps my phone?" **This response, however, puts their private information in the hands of officials who secretly break the law daily.** Their repeated crimes against the innocent, at home and abroad, make them dangerous. The question Americans should be asking, is, "Do I want the staffs of these high officials monitoring my private

conversations and those of my children?" Remember, President Obama has already killed Americans without legal authorization. John Whitehead of the Rutherford Institute, a civil liberties organization based in Charlottesville, Va., says, "Thanks to an insidious partnership between Google and the National Security Agency (NSA) that grows more invasive and more subtle with every passing day, "we the people" have become little more than data consumer commodities to be bought, sold and paid for over and over again." Whitehead warns, "With every smartphone we buy, every GPS device we install, every Twitter, Facebook, and Google account we open, every frequent buyer card we use for purchases—whether at the grocer's, the yogurt shop, the airlines or the department store, and every credit and debit card we use to pay for our transactions, **we're helping Corporate America build a dossier for its government counterparts on who we know, what we think, how we spend our money, and how we spend our time.**" As for the benefits of NSA's vast spy operation, they have yet to appear. Activist David Swanson of Charlottesville, asserts, "Obama's own panel and every other panel that has looked into it found zero evidence that the new abusive NSA programs have prevented any violent attacks." "Far from halting or apologizing for the abuses of the NSA, Obama defends them as necessitated by the danger of a new 911," says Swanson, of "War is a Crime.org". "While drones over Yemen and troops in Afghanistan and 'special' forces in three-quarters of the world are widely understood to endanger us, and while alternatives that upheld the rule of law and made us safer would not require secrecy or human rights violations, Obama wants to continue the counterproductive and immoral militarism while holding off all blowback through the omniscience of Big Brother." Swanson adds, "Massive bulk collection of everybody's data will continue unconstitutionally."

AT Private Sector Conducts Surveillance

Yes, but the government can kill you and put you in prison

The Drum, May 14, 2014, <http://www.thedrum.com/news/2014/05/15/many-more-nsa-revelations-come-glenn-greenwald-tells-al-jazeera-snowden-very-happy-0>

The NSA revelations have touched off a heated debate in the U.S. about privacy, security and whether the U.S. government was overstepping its bounds in sacrificing the former in favour of the latter. **Greenwald said that the main difference is that the government “can put you into prison,” “can take your property” and can even “kill you.” He said this is why “the Bill of Rights and the Constitution limits what the government can do, because we've always looked at government and state power as particularly and uniquely threatening.”**

AT Kritiks of Privacy

We've captured their offense – privacy protects the right to criticize itself

Boling, (Professor of Philosophy, Purdue University), 1996 (Patricia, *PRIVACY AND THE POLITICS OF INTIMATE LIFE*, , p.15)

Although Pateman, Okin, Young, and others nod in the direction of acknowledging that privacy may be a useful concept, they nonetheless focus overwhelmingly on its role in depriving issues, people, and perspectives of public importance. Such an approach does little to further our thinking about the various roles privacy plays in contemporary political, legal, and social life. Of course we need to criticize privacy and public-private distinctions when they silence and obscure oppressive practices and arrangements. But we also need to recognize that privacy can play a protective, empowering role, and to think about what makes the distinction between public and private life important as well as what makes it oppressive

De-legitimating “privacy” does not resolve the public/private distinction

Gavison, (Professor of law Hebrew University) 92 (Ruth, Feminism and the Public/Private Distinction, Stanford Law Review, 45 Stan. L. Rev. 1, November, pg. 35-36)

Domestic violence. Domestic violence is another frequently cited example of the bad consequences resulting from the public/private distinction. Here, the argument is that family relations are seen as paradigmatically private. In part, this is based upon the assumption that family relationships are voluntary and equal. Consequently, there is a presumption that these private relations should be free from external interference. Often people, incorrectly, jump from the accurate description of family relationships as private to the conclusion that no interference is justified, without examining the truth of the initial assumptions or contrary considerations which might defeat the presumption. Such a leap constitutes an obvious mistake in practical reasoning. In part, this mistake results from equivocation, and thus may be attributed to language or terminology. As we saw in Part II, the key term "private" may be used in at least three different senses. First, "private" may indicate the highly personal and intimate reasons for the presumptive entitlement of families to be free from interference. Second, ascription of private-ness may be an invocation of the presumptive entitlement, to be weighed against other features of the situation. Third, its usage may indicate a conclusion that, all things considered, the activity should not be interfered with. Public treatment of domestic violence is plagued by dubious uses of the notion of privacy. The police are often extremely reluctant to interfere in domestic disputes, even when violence is alleged. Often, the reason offered for this reluctance is the private nature of the marital relationship. The potential for confusion generated by this variety of uses is not unique to the public/private distinction or to the feminist context. In fact, this kind of problem is pervasive in legal reasoning, especially when the conclusion must be justified in terms of interpretations of authoritative texts. Moreover, the confusion appears in many different fields of the law. Although these mistakes should be avoided, a reform of the language and the terminology is not necessarily the cure. Reforming the language by delegitimizing the use of "private" and "privacy" will not clarify distinctions between descriptive and normative claims. The descriptive-normative

ambiguity exists for all alternative candidates. Some terms, such as "highly personal," may not have a purely descriptive sense, because what is central to one's self-identity is probably a matter of constitutive rules and expectations. But all substitute terms have uses which refer to people's wishes and perceptions, as well as senses which refer to the conclusions of normative arguments. Adopting words other than "private" and "public" to discuss what should be free from state regulation may help us to avoid some potential sources of mistakes, but the new terms may generate their own ambiguities and risks.

AT Surveillance Solves Discrimination

No, Mass Surveillance is discriminatory – privacy is critical to stop this. **Richards, 2015,**

Neil M., Professor of Law, Washington University. "Four Privacy Myths" Revised form, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2427808>

The segmenting power of data analytics suggests a third power effect that personal data can enable – the power to sort. In an influential 1993 book, sociologist Oscar Gandy described the digital privacy revolution as ushering in something he called “The Panoptic Sort.”⁷⁵ Gandy used this term to mean the use of large datasets by government and private bureaucracies to classify, assess, and sort individuals for analysis and control – a system of power based upon personal information. More recently, Joseph Turow has illustrated the even more powerful sorting ability that two decades of computer and data science have enabled. Today, personal data is used to classify and sort us all.⁷⁶ On the one hand, the increased efficiency of sorting enabled by the information revolution has many useful applications. Large dataset analytics has many powerful applications that don’t even use personal data, such as weather and traffic forecasting, the design of better automotive components, spell-checkers, and search engines.⁷⁷ Analytics based on personal data are useful, too, enabling better decisions in the medical, credit and insurance contexts, as well as the prevention of terrorism and other crimes.⁷⁸ But this increased power to sort can be used for bad or morally ambiguous purposes as well. Lawyers have another word for this kind of sorting, which is “discrimination.” Consider the use of consumer profiles to determine the likelihood we would buy products at a given price. Such relatively simple analytic techniques could enable a website (say, like Amazon.com) in which all prices were optimized to the highest value we might be willing to pay. Sophisticated analytics could also raise the spectre of a new kind of “redlining” – the denial or discrimination of services to people on the basis of race or other suspect criteria. Of course, predictive analytics need not use race directly; they could be designed to ignore race and use other variables that correlate with race. Or perhaps such algorithms might not use race indirectly, but impose a brutal individualized economic rationalism upon us all as consumers and citizens. Thankfully, the strong form of that society is not upon us yet, but some of its weaker cousins are. And if we dismiss the problems caused by privacy or personal data as nothing more than bad people hiding bad deeds, we will miss the transformative power effects of the digital revolution entirely. For better or worse, we use the term “privacy” as a shorthand to capture all of the issues raised by personal data. As a result, privacy is not just for those of us with something to hide. Of course, we all have something to hide. But more fundamentally, questions of privacy include many of the most fundamental questions of civil liberties, economic, and political power in a digital society. From that perspective, privacy is for everyone.

Surveillance exacerbates existing inequality.

Magi, 2011

Trina J. Librarian, University of Vermont, Burlington. "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature1." The Library 81.2 (2011).

Privacy helps prevent sorting of people into categories that can lead to lost opportunities and deeper inequalities.—Many scholars are concerned that the gathering of data about individuals and the sorting of people into categories can lead to lost opportunities, deeper inequalities, destabilized political action, and victimization by error, oversimplification, and decontextualization. Using the panopticon metaphor, Gandy discusses what he calls the “panoptic sort,” a “discriminatory process that sorts individuals on the basis of their estimated value or worth” and “reaches into every aspect of individuals’ lives in their roles as citizens, employees, and consumers” [33, p. 1]. Gandy claims the panoptic sort is a defensive technology more concerned with avoiding risk and loss than with realizing a gain [33, p. 17]. Such sorting has been facilitated by computer technology that has made it cost-effective to collect, store, and analyze data,

and match it with other data sets. Gandy is troubled by the fact that those in power use this information to predict future behavior of an individual not on the basis of the behavior of that particular individual but rather on the more general basis of the past behavior of other individuals in the group or class to which the person has been assigned based on some attributes [33, p. 144]. Based on this sorting, individuals will be presented with limited options from which to choose, leading to an increased knowledge gap between the haves and the have-nots and a generalized lowering of the average level of public understanding [33, p. 2]. Reiman agrees that the panopticon is a more fitting metaphor than the fishbowl for this new threat to privacy, because the modern means of collecting information gathers various publicly observable activities that are dispersed over space and time and makes them visible from a single point [27, p. 196]. Many writers express concern about the way administrative systems for collecting data about people must necessarily oversimplify the nature of individuals and communities. James Scott says “a human community is surely far too complicated and variable to easily yield its secrets to bureaucratic formulae” [35, p. 23], yet when governments collect standardized records and documents, the information in these records easily becomes the only information to be considered by the state. “An error in such a document can have far more power—and for far longer—than can an unreported truth,” he says [35, p. 83].

AT “Nothing To Hide”

The “nothing to hide” argument is selfish and wrong.

Snowden 15 — Edward Snowden, NSA whistleblower, Member of the Board of Directors of the Freedom of the Press Foundation, former Central Intelligence Agency officer and National Security Agency contractor, 2015 (“Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU’s Jameel Jaffer. AUA.,” Reddit Ask Me Anything with Edward Snowden, May 21st, Available Online at https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_and/crglgh2, Accessed 06-16-2015)

Jameel is right, but I think the central issue is to point out that regardless of the results, the ends (preventing a crime) do not justify the means (violating the rights of the millions whose private records are unconstitutionally seized and analyzed).

Some might say "I don't care if they violate my privacy; I've got nothing to hide." Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they "need" a right: the burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can't give away the rights of others because they're not useful to you. More simply, the majority cannot vote away the natural rights of the minority.

But even if they could, help them think for a moment about what they're saying. Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

A free press benefits more than just those who read the paper.

* Jameel = Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union and Director of the ACLU's Center for Democracy

Privacy is not about hiding wrongdoing. We all have “something to hide.”

Greenwald 14 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, 2014 (“The Harm of Surveillance,” *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Published by Metropolitan Books, ISBN 9781627790734, p. ebook)

As the experiments showed, there are all sorts of things people do that they are eager to keep private, even though these sorts of things do not constitute doing “something wrong.” Privacy is indispensable to a wide range of human activities. If someone calls a suicide hotline or visits an abortion provider or frequents an online sex website or makes an appointment with a

rehabilitation clinic or is treated for a disease, or if a whistle-blower calls a reporter, there are many reasons for keeping such acts private that have **no connection** to illegality or wrongdoing.

Even if we don't, others do.

Shackford 13 — Scott Shackford, Associate Editor at *Reason*, former Editor of *Freedom Communications*—a libertarian media organization, 2013 (“3 Reasons the ‘Nothing to Hide’ Crowd Should Be Worried About Government Surveillance,” *Reason*, June 12th, Available Online at <https://reason.com/archives/2013/06/12/three-reasons-the-nothing-to-hide-crowd>, Accessed 06-17-2015)

The “nothing to hide” crowd's involvement in political activism is likely limited. That's perfectly fine. Nobody should feel obligated to join the Occupy movement or a Tea Party organization or be the kind of person who might end up on a politician's enemies list. But to say “I have nothing to hide” is a **fundamentally selfish declaration**. What about parents, sisters, brothers, partners, and other loved ones? Can we say the same for them? You don't have to have an illness whose suffering can be eased with the use of medical marijuana to be concerned about the way the federal government treats this industry. Would you say, “I don't need medical marijuana so I don't care if they imprison those who do”? Sadly, some people do. Fundamentally, saying “I have nothing to hide,” is similar to saying “**I don't care about those who do.**”

AT “No Chilling Effect”

Social science research confirms: surveillance produces conformity.

Greenwald 14 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, 2014 (“The Harm of Surveillance,” *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Published by Metropolitan Books, ISBN 9781627790734, p. ebook)

The pernicious controlling power of ubiquitous surveillance and the self-censorship that results are confirmed in a range of social science experiments and extend far beyond political activism. **Ample studies** show how this dynamic works at **the deepest personal and psychological levels**.

One team of researchers, publishing their findings in the journal *Evolutionary Psychology*, presented their subjects with morally questionable actions, such as keeping a sizeable amount of money found in a wallet on the street or knowing that a friend had added false information to his résumé. The subjects were asked to assess the degree of wrongdoing. The study noted that subjects who were shown images hinting at surveillance, such as a large pair of staring eyes, rated the actions as more “reprehensible” than those who were shown a neutral image. The researchers concluded that surveillance encourages those who are being watched to “affirm their endorsement of prevailing social norms” as they attempt to “actively manage their reputations.”

A comprehensive experiment conducted in 1975 by Stanford University psychologists Gregory White and Philip Zimbardo, entitled “The Chilling Effects of Surveillance,” sought to assess whether being watched had an impact on the expression of controversial political opinions. The impetus for the study was Americans’ concerns about surveillance by the government:

The Watergate scandal, revelations of White House bugging, and Congressional investigations of domestic spying by the Central Intelligence Agency have served to underscore the developing paranoid theme of American life: Big Brother may be watching you! Proposals for national data banks, uses of surveillance helicopters by urban police forces, the presence of observation cameras in banks and supermarkets, and airport security searches of person and property are but some of the [...] anxiety and inhibition.

White and Zimbardo noted in their conclusion that the “threat or actuality of government surveillance may psychologically inhibit freedom of speech.” They added that while their “research design did not allow for the possibility of ‘avoiding assembly,’ ” they expected that “the anxiety generated by the threat of surveillance would cause many people to totally avoid situations” in which they might be monitored. “Since such assumptions are limited only by one’s imagination and are encouraged daily by revelations of government and institutional invasion of privacy,” they wrote, “the boundaries between paranoid delusions and justified cautions indeed become tenuous.”

Surveillance undermines intellectual privacy.

Richards 13 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2013 (“The Dangers of Surveillance,” *Harvard Law Review* (126 Harv. L. Rev. 1934), May, Available Online to Subscribing Institutions via Lexis-Nexis)

At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called “intellectual privacy.” n5 A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

Surveillance threatens freedom of thought.

Richards 13 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2013 (“The Dangers of Surveillance,” *Harvard Law Review* (126 Harv. L. Rev. 1934), May, Available Online to Subscribing Institutions via Lexis-Nexis)

V. Conclusion

The challenge to our law posed by the Age of Surveillance is immense. The justifications for surveillance by public and private actors are significant, but so too are the costs that the rising tide of unfettered surveillance is creating. Surveillance can sometimes be necessary, even helpful. But unconstrained surveillance, especially of our intellectual activities, threatens a cognitive revolution that cuts at the core of the freedom of the mind that our political institutions presuppose. Therefore, surveillance must be constrained by legal and social rules. The technological, economic, and geopolitical changes of the past twenty years have whittled away at those rules, both formally on their substance (for example, the Patriot Act and the expansion of National Security [*1965] Letter jurisdiction) and in practice (for example, the pressure that the technological social practices of the Internet have exerted on privacy). By thus recognizing the harms of surveillance and crafting our laws accordingly, we can obtain many of its benefits without sacrificing our vital civil liberties or upending the power balance between individuals on the one hand and companies and governments on the other.

AT “No Threshold for Privacy”

The “threshold” for harm is low. Without privacy, the chilling effect from mass surveillance crushes free expression.

Abdo 13 — Alex Abdo, Staff Attorney in the Speech, Privacy and Technology Project at the American Civil Liberties Union, former Attorney at the ACLU National Security Project where he was involved in the litigation of cases concerning the Patriot Act, the Foreign Intelligence Surveillance Act, the International Emergency Economic Powers Act, and the treatment of detainees in Guantánamo Bay, Afghanistan, Iraq, and the Navy brig in South Carolina, holds a J.D. from Harvard Law School, 2013 (“You May Have ‘Nothing to Hide’ But You Still Have Something to Fear,” *MSNBC*, August 2nd, Available Online at <https://www.aclu.org/blog/you-may-have-nothing-hide-you-still-have-something-fear>, Accessed 06-17-2015)

In the wake of recent news that the NSA is spying on Americans, I have been particularly struck by the argument that "if you've got nothing to hide, you've got nothing to fear."

At first blush, this argument might seem sound – after all, if the government is merely conducting anti-terrorism surveillance, non-terrorists shouldn't be affected, right? But if you look more closely, you'll see this idea is full of holes.

The "nothing to hide" argument mistakenly suggests that privacy is something only criminals desire. In fact, we choose to do many things in private – sing in the shower, make love, confide in family and friends – even though they are not wrong or illegal. Who would not be embarrassed if all of their most intimate details were exposed? Fences and curtains are ways to ensure a measure of privacy, not indicators of criminal behavior. Privacy is a fundamental part of a dignified life.

The "nothing to hide" argument also has things backwards when it suggests that we are all worthy of suspicion until proven otherwise. Our system of justice treats us all as innocent until proven guilty. That applies in everyday life – when the government wants to spy on our daily activities and private conversations – as much as it applies in court. The state bears the burden of showing there is a good reason for suspicion, not the other way around. The refrain "nothing to hide" should not be a license for sweeping government surveillance.

Even if you think you have nothing to hide, you may indeed have something to fear. You might fear for yourself. As Kafka so chillingly illustrates in "The Trial," the prospect of unwarranted government pursuit is terrifying. Or you might fear for our society. Living under the constant gaze of government surveillance can produce long-lasting social harm: if citizens are just a little more fearful, a little less likely to freely associate, a little less likely to dissent – the aggregate chilling effect can close what was once an open society.

Government surveillance can also have a direct harm on others – think of human rights workers or journalists who must work with people who fear government scrutiny, not because of wrongdoing but for political reasons. Imagine a liberal group arguing that in the wake of the recent IRS scandal, it has nothing to fear because the IRS is interested only in conservative groups. This argument would be myopic, missing the wider risks of government overreaching. (Need proof? The IRS has now admitted that it scrutinized liberal groups, too.)

Perhaps you remain unconvinced. You are sure that you have nothing to hide and you never will. You think my concerns about chilled speech and democratic accountability are overblown, and you think privacy concerns are exaggerated and unlikely to affect you or our society in any case.

But – and this is the biggest hole in the "nothing to hide, nothing to fear" argument – how can you know for sure?

In fact, you have no idea if you have something to fear or not, because you do not know what the government does with the data it collects. If the government keeps secret what it is collecting about you or why, you cannot correct potential errors. And if you know anything about our justice system, you know that errors are common. Transparency is partly about making sure the government's actions – its outputs – can be evaluated; but transparency is also about making sure the government's information – its inputs – is accurate.

When the government operates in secret, it is hard to know anything with confidence. There is, however, one thing you can say with 100% confidence: we need to know more.

We need to know more about what information the government is collecting about millions of innocent Americans. We need to know more about the secret legal interpretations that the government is relying on to monitor our communications. And we need to know more about what the government does with the trillions of bits of electronic data it is amassing in its files. We need these answers because, even if we have nothing to hide, that does not mean we want to live in a society where nothing is private.

AT “Privacy Not Key To New Ideas”

Surveillance makes idea formation impossible and undermines freedom of thought.

Richards 15 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2015 (“A Theory of Intellectual Privacy,” *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Published by Oxford University Press, ISBN 9780199946143, p. 103-104)

All Western societies share a foundational commitment to the freedom of speech on public matters—a belief that new ideas should be aired and given their say. 16 But if we are interested in freedom of speech and the ability to express new and possibly heretical ideas, we should care about the social processes by which these ideas are originated, nurtured, and developed. After all, a society that cares about the free exchange of ideas should be committed to producing new ideas and not just in shouting the same old ones as loudly as possible.

How Intellectual Privacy Works

Intellectual privacy rests on the intuition that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy—protection from surveillance or interference—is necessary to promote this kind of intellectual freedom. It rests on the belief that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.

Intellectual privacy is vital to freedom of thought.

Richards 8 — Neil M. Richards, Professor of Law at the Washington University School of Law, former law clerk to Chief Justice William H. Rehnquist, holds a J.D. and an M.A. in Legal History from the University of Virginia, 2008 (“Intellectual Privacy,” *Texas Law Review* (87 Tex. L. Rev. 387), December, Available Online to Subscribing Institutions via Lexis-Nexis)

Each of the four strands of intellectual privacy contributes to the generation of new ideas and new ways of thinking about the world. Without free thought, the freedom to think for ourselves, to entertain ideas that others might find ridiculous or offensive, we would lack the ability to reason, much less the capacity to develop revolutionary or heretical ideas about (for instance) politics, culture, or religion. Engaging in these processes requires a space, physical and psychological, where we can think for ourselves without others watching or judging. But despite the prevailing cultural myth of the creator toiling alone, few of our ideas come from the operation of a single mind. The freedom of intellectual exploration allows us to read and to receive exposure to the ideas of others so we can evaluate them and improve or adapt them for ourselves. And at a certain point, when our ideas are ready to share with others but not yet developed enough for widespread dissemination, we might want to communicate our ideas to a few trusted friends in confidence. The freedom of confidential communications affords us this opportunity.

The theory of intellectual privacy I have articulated nurtures the cognitive and communicative processes by which we as individuals can come to think for ourselves. It allows us to imagine,

test, and develop our ideas free from the deterring gaze or interfering actions of others. Without intellectual privacy, we would be less willing to investigate ideas and hypotheses that might turn out to be wrong, controversial, or deviant. Intellectual privacy thus permits us to experiment with ideas in relative seclusion without having to disclose them before we have developed them, considered them, and decided whether to adopt them as our own.

AT “No Risk of Tyranny”

The risk of tyranny is high.

Glenon 14 — Michael J. Glennon, Professor of International Law at the Fletcher School of Law and Diplomacy at Tufts University, Member of the Council on Foreign Relations, former Legal Counsel to the Senate Foreign Relations Committee, holds a J.D. from the University of Minnesota, 2014 (“National Security and Double Government,” *Harvard National Security Journal* (5 Harv. Nat'l Sec. J. 1), Available Online to Subscribing Institutions via Lexis-Nexis)

The trivial risk of sudden despotism, of an abrupt turn to a police state or dictatorship installed with coup-like surprise, has created a false sense of security in the United States.⁶¹⁸ That a strongman of the sort easily visible in history could suddenly burst forth is not a real risk. The risk, rather, is the risk of slowly tightening centralized power, growing and evolving organically beyond public view, increasingly unresponsive to Madisonian checks and balances. Madison wrote, “There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations.”⁶¹⁹ Recent history bears out his insight. Dahl has pointed out that in the 20th century—the century of democracy’s great triumph—some seventy democracies collapsed and quietly gave way to authoritarian regimes.⁶²⁰ That risk correlates with voter ignorance; the term Orwellian has little meaning to a people who have never known anything different, who have scant knowledge of history, civics, or public affairs, and who in any event have likely never heard of George Orwell. “If a nation expects to be ignorant and free, in a state of civilization,” Thomas Jefferson wrote, “it expects what never was and never will be.”⁶²¹ What form of government ultimately will emerge from the United States’ experiment with double government is uncertain. The risk is considerable, however, that it will not be a democracy.

AT Small Harm from a Privacy Violation

Severe harm from multiple privacy violations

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Individual privacy harms, mean while, are often small and dispersed. Of course, revealing nude photographs or highly embarrassing or discreditable facts can generate substantial emotional distress. But many privacy violations are akin to a bee sting. Despite this fact, it would be wrong to conclude that they ought to be ignored. One bee sting can be shrugged off, but a hundred or a thousand can be lethal. Harm from privacy violations can develop gradually over time, but decisions about privacy must be made individually, in isolation, and far in advance.

AT Nothing To Hide

The “nothing to hide” argument is selfish and wrong.

Snowden 15 — Edward Snowden, NSA whistleblower, Member of the Board of Directors of the Freedom of the Press Foundation, former Central Intelligence Agency officer and National Security Agency contractor, 2015 (“Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU’s Jameel Jaffer. AUA.,” Reddit Ask Me Anything with Edward Snowden, May 21st, Available Online at https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_and/crglgh2, Accessed 06-16-2015)

Jameel is right, but I think the central issue is to point out that regardless of the results, the ends (preventing a crime) do not justify the means (violating the rights of the millions whose private records are unconstitutionally seized and analyzed).

Some might say "I don't care if they violate my privacy; I've got nothing to hide." Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they "need" a right: the burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can't give away the rights of others because they're not useful to you. More simply, the majority cannot vote away the natural rights of the minority.

But even if they could, help them think for a moment about what they're saying. Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

A free press benefits more than just those who read the paper.

* Jameel = Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union and Director of the ACLU's Center for Democracy

Privacy is not about hiding wrongdoing. We all have “something to hide.”

Greenwald 14 — Glenn Greenwald, journalist who received the 2014 Pulitzer Prize for Public Service for his work with Edward Snowden to report on NSA surveillance, Founding Editor of *The Intercept*, former Columnist for the *Guardian* and *Salon*, recipient of the Park Center I.F. Stone Award for Independent Journalism, the Online Journalism Award for investigative work on the abusive detention conditions of Chelsea Manning, the George Polk Award for National Security Reporting, the Gannett Foundation Award for investigative journalism, the Gannett Foundation Watchdog Journalism Award, the Esso Premio for Excellence in Investigative Reporting in Brazil, and the Electronic Frontier Foundation’s Pioneer Award, holds a J.D. from New York University School of Law, 2014 (“The Harm of Surveillance,” *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Published by Metropolitan Books, ISBN 9781627790734, p. ebook)

As the experiments showed, there are all sorts of things people do that they are eager to keep private, even though these sorts of things do not constitute doing “something wrong.” Privacy is indispensable to a wide range of human activities. If someone calls a suicide hotline or visits an abortion provider or frequents an online sex website or makes an appointment with a

rehabilitation clinic or is treated for a disease, or if a whistle-blower calls a reporter, there are many reasons for keeping such acts private that have no connection to illegality or wrongdoing.

Even if we don't, others do.

Shackford 13 — Scott Shackford, Associate Editor at *Reason*, former Editor of *Freedom Communications*—a libertarian media organization, 2013 (“3 Reasons the ‘Nothing to Hide’ Crowd Should Be Worried About Government Surveillance,” *Reason*, June 12th, Available Online at <https://reason.com/archives/2013/06/12/three-reasons-the-nothing-to-hide-crowd>, Accessed 06-17-2015)

The “nothing to hide” crowd's involvement in political activism is likely limited. That's perfectly fine. Nobody should feel obligated to join the Occupy movement or a Tea Party organization or be the kind of person who might end up on a politician's enemies list. But to say “I have nothing to hide” is a fundamentally selfish declaration. What about parents, sisters, brothers, partners, and other loved ones? Can we say the same for them? You don't have to have an illness whose suffering can be eased with the use of medical marijuana to be concerned about the way the federal government treats this industry. Would you say, “I don't need medical marijuana so I don't care if they imprison those who do”? Sadly, some people do. Fundamentally, saying “I have nothing to hide,” is similar to saying “I don't care about those who do.”

AT No Risk of Tyranny

The risk of tyranny is high.

Glenon 14 — Michael J. Glennon, Professor of International Law at the Fletcher School of Law and Diplomacy at Tufts University, Member of the Council on Foreign Relations, former Legal Counsel to the Senate Foreign Relations Committee, holds a J.D. from the University of Minnesota, 2014 (“National Security and Double Government,” *Harvard National Security Journal* (5 Harv. Nat'l Sec. J. 1), Available Online to Subscribing Institutions via Lexis-Nexis)

The trivial risk of sudden despotism, of an abrupt turn to a police state or dictatorship installed with coup-like surprise, has created a false sense of security in the United States.⁶¹⁸ That a strongman of the sort easily visible in history could suddenly burst forth is not a real risk. The risk, rather, is the risk of slowly tightening centralized power, growing and evolving organically beyond public view, increasingly unresponsive to Madisonian checks and balances. Madison wrote, “There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations.”⁶¹⁹ Recent history bears out his insight. Dahl has pointed out that in the 20th century—the century of democracy’s great triumph—some seventy democracies collapsed and quietly gave way to authoritarian regimes.⁶²⁰ That risk correlates with voter ignorance; the term Orwellian has little meaning to a people who have never known anything different, who have scant knowledge of history, civics, or public affairs, and who in any event have likely never heard of George Orwell. “If a nation expects to be ignorant and free, in a state of civilization,” Thomas Jefferson wrote, “it expects what never was and never will be.”⁶²¹ What form of government ultimately will emerge from the United States’ experiment with double government is uncertain. The risk is considerable, however, that it will not be a democracy.\

AT Government Not Collecting the Data

Government spying through home IoT

Spencer Ackerman, February 9, 2016, Guardian, US intelligence chief: We might use the Internet to spy on you, <https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper>

The US intelligence chief has acknowledged for the first time that agencies might use a new generation of smart household devices to increase their surveillance capabilities. As increasing numbers of [devices connect to the internet and to one another](#), the so-called internet of things promises consumers increased convenience – the remotely operated thermostat from Google-owned Nest is a leading example. But as home computing migrates away from the laptop, the tablet and the smartphone, experts warn that the security features on the coming wave of automobiles, dishwashers and alarm systems lag far behind. In an appearance at a Washington thinktank last month, the director of the National Security Agency, Adm Michael Rogers, said that it was time to consider making the home devices “more defensible”, but did not address the opportunities that increased numbers and even categories of connected devices provide to his surveillance agency. However, James Clapper, the US director of national intelligence, was more direct in testimony submitted to the Senate on Tuesday as part of an assessment of threats facing the United States. “In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials,” Clapper said. Clapper did not specifically name any intelligence agency as involved in household-device surveillance. But security experts examining the internet of things take as a given that the US and other surveillance services will intercept the signals the newly networked devices emit, much as they do with those from cellphones. Amateurs are already interested in easily compromised hardware; computer programmer John Matherly’s search engine [Shodan](#) indexes thousands of completely unsecured web-connected devices.

AT De-Identification Solves

Information can be re-identified

Melissa W. Bailey, J.D. Candidate, 2016, Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things, TEXAS LAW REVIEW
<http://www.texasrev.com/wp-content/uploads/2016/04/Bailey.FinalPDF.pdf>

As the IoT grows larger, so do concerns about consumer privacy. Because the datasets produced by each device are unique to the user, any release of this information poses the danger of associating it with the individual user.⁴⁸ One way that companies attempt to have the best of both worlds—that is, mitigate privacy concerns while still selling data—is by “deidentifying” the data.⁴⁹ De-identification is a “process to prevent a personal identifier from being connected with information.”⁵⁰ This process allows some bits of data to be compiled while excluding the information that identifies a particular dataset’s owner, such as the individual’s name.⁵¹ For example, GPS devices can track the aggregate speed on a road and release real-time traffic updates without compiling the name of each driver currently on that road.⁵² But de-identification is not a perfect solution because in most of the de-identified datasets, the information can be re-identified.⁵³ This means that even if data were released “anonymously,” it could be reassociated with an individual user, thwarting the de-identification process.⁵⁴ Re-identification could reveal private Internet searches, health and hospitalization history, movie-watching history, and more.⁵⁵ While some companies include a clause in their sales contracts that prohibit reidentification,⁵⁶ the data that could be used to re-identify the information are still attached, meaning that the third-party buyer could breach the contract and re-identify the data; the contract also does not prevent a hacker from accessing the datasets and re-identifying them. Although the actual likelihood of re-identification is still contested,⁵⁷ the potential for danger is high: once a user’s private information is released, it cannot be recalled.

AT Regulations Solve

No effective privacy protecting IoT regulations

Melissa W. Bailey, J.D. Candidate, 2016, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, TEXAS LAW REVIEW
<http://www.texasrev.com/wp-content/uploads/2016/04/Bailey.FinalPDF.pdf>

These three examples shed light onto how IoT devices can be manipulated to reveal the privacy of the user. Despite the potential dangers of privacy trading, users continue to buy IoT products, and more products enter the market at an ever-increasing rate.⁷⁰ Because there currently exists no broad-sweeping regulation about the Internet of Things,⁷¹ consumers must rely on the protections offered by older, untailored federal regulations or by individualized state regulations. Some states have already begun passing legislation about the IoT, but each state's laws vary and may not cover all data-privacy concerns.⁷² While the U.S. Department of Health and Human Services requires that anyone with personal health information de-identify this data,⁷³ de-identification is merely recommended—not required—in other spheres.⁷⁴ Furthermore, there does not currently exist federal regulation requiring manufacturers to notify consumers about when or what types of data are collected when the collected information is used for a purpose consistent with the transaction.⁷⁵ The FTC has explicitly announced that it will not recommend requiring manufacturers to notify consumers about data collection in such instances, reasoning that “these data uses are generally consistent with consumers’ reasonable expectations.”⁷⁶ Both houses of Congress have similarly rejected the idea of legislation; the predominant concern seems to be ensuring that the IoT has room to develop. The Senate held a hearing about the IoT in February of 2015, but ultimately decided against regulation because “consumers and entrepreneurs [should] decide where [the Internet of Things] goes.”⁷⁷ In April of 2015, the House of Representatives saw a resolution that “the United States should develop a national strategy to encourage the development of the [IoT]”; however, this resolution did not include any reference to regulating the IoT or hint toward any future consumer protection laws.⁷⁸ With no federal regulations, consumers will likely be bound to the manufacturer’s terms through contract law.⁷⁹ Many contracts will be in the form of a “clickwrap” agreement, defined as an agreement in which the consumer clicks “I agree” to the manufacturer’s standard contract terms.⁸⁰ Courts that have considered the issue have generally found clickwrap agreements to be enforceable, with the caveat that the user must know that he is consenting to terms—even if the user does not know what those terms actually are.⁸¹ This means that any rights a user has under a standard IoT contract are merely those afforded to him by the manufacturer or seller, and the only recourse to a user who prefers not to share his data is to refrain from purchasing an IoT device. Consumer protections for those who do purchase IoT devices vary from state to state.⁸² California and Delaware, for example, both require that operators of Internet websites or services conspicuously post their privacy policies online.⁸³ New York requires that state agencies that collect personal information post a privacy policy online, but remains silent about requirements for private actors.⁸⁴ Nebraska does not require that operators of websites post their privacy policies, but does prohibit false or misleading statements in any privacy policy.⁸⁵ Other states have no protection at all.⁸⁶ Such lack of protection may prove problematic in the IoT sphere because even if a consumer is aware that IoT devices come with some terms attached, these terms are

ambiguous. Privacy policies usually will “provide little real guidance” to the consumer because they do not provide clear disclosure about how the user’s data can be “shared with or sold to third parties.”⁸⁷ When consumers receive no notice about what type of data are being collected or to whom these data are being sold, it may be difficult for consumers to form any expectations—much less reasonable ones—about how the data will be used. A consumer might neither comprehend the full extent of the data collected nor understand why a third party would want to purchase the data. In the ever-growing world of the Internet of Things, the lack of both notification and regulation may be a dangerous combination for consumers.

Government will use the IoT for surveillance

Susan Hennessey, is Fellow in National Security in Governance Studies at the Brookings Institution, March 25, 2016, Alternative Perspectives on the Internet of Things, <https://www.brookings.edu/blog/techtank/2016/03/25/alternative-perspectives-on-the-internet-of-things/> DOA: 10-21-16

Director of National Intelligence James Clapper agrees that IoT has some surveillance potential. He recently **testified** before Congress that “[i]n the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.”

Government will get the data

Catherine Crump is a staff attorney with the ACLU’s Speech, Privacy, and Technology Project. She is a non-residential fellow with the Stanford Center for Internet and Society and an adjunct professor of clinical law at NYU, 2014, Mach 25, The Grows Around Us, http://www.tomdispatch.com/post/175822/tomgram%3A_crump_and_harwood%2C_the_net_closes_around_us/

Techno-evangelists have a nice catchphrase for this future utopia of machines and the never-ending stream of information, known as Big Data, it produces: the Internet of Things. So abstract. So inoffensive. Ultimately, so meaningless.

A future Internet of Things does have the potential to offer real benefits, but the dark side of that seemingly shiny coin is this: companies will increasingly know all there is to know about you. Most people are already aware that virtually everything a typical person does on the Internet is tracked. In the not-too-distant future, however, real space will be increasingly like cyberspace, thanks to our headlong rush toward that Internet of Things. With the rise of the networked device, what people do in their homes, in their cars, in

stores, and within their communities will be monitored and analyzed in ever more intrusive ways by corporations and, by extension, the government.

Data used in drug enforcement operations

Catherine Crump is a staff attorney with the ACLU's Speech, Privacy, and Technology Project. She is a non-residential fellow with the Stanford Center for Internet and Society and an adjunct professor of clinical law at NYU, 2014, Mach 25, The Grows Around Us,

http://www.tomdispatch.com/post/175822/tomgram%3A_crump_and_harwood%2C_the_net_closes_around_us/

The result: more and more of what happens behind closed doors will be open to scrutiny by parties you would never invite into your home. After all, the Drug Enforcement Administration already **subpoenas** utility company records to determine if electricity consumption in specific homes is consistent with a marijuana-growing operation. What will come next? Will eating habits collected by smart fridges be repackaged and sold to healthcare or insurance companies as predictors of obesity or other health problems -- and so a reasonable basis for determining premiums? Will smart lights inform drug companies of insomniac owners?

AT “Privacy Laws Solve”

Privacy law won’t limit abuse

Scott Pepper, Professor of Law, University of Colorado School of Law, August 2015, Regulating the Internet of Things: First Steps, <http://www.texasrev.com/wp-content/uploads/2015/08/Pepper-93-1.pdf>

The Legal Problem: Privacy Law Is Unprepared.—The inherent sparsity of Internet of Things data means that protecting privacy through anonymization is particularly unlikely to succeed. The legal implications are dramatic. Ohm has catalogued the huge number of privacy laws that rely on anonymization.²⁷⁸ Many distinguish “personally identifiable information” (PII)—usually defined as name, address, social-security number, or telephone number—from other data that is presumed not to reveal identity.²⁷⁹ The threat of re-identification of sparse sensor-based datasets makes questionable this distinction between PII and other data. Information-privacy scholarship has begun to debate how to address the threat of re-identification. Ohm proposes abandoning the idea of PII completely;²⁸⁰ Paul Schwartz and Daniel Solove have recently resisted this approach, arguing instead that we should redefine PII along a continuum between identified information, identifiable information, and nonidentifiable information.²⁸¹ The “identified” category pertains to information that is clearly associated with an individual.²⁸² The “non-identifiable” pertains to information that carries only a very “remote risk” of connection to an individual.²⁸³ In the middle are data streams for which there is a nontrivial possibility of future re-identification.²⁸⁴ Schwartz and Solove argue that the law should treat differently information in these three categories. For merely identifiable information that has not yet been associated with an individual, “[f]ull notice, access, and correction rights should not be granted.”²⁸⁵ In addition, “limits on information use, data minimization, and restrictions on information disclosure should not be applied across the board to identifiable information.”²⁸⁶ Data security, however, should be protected when dealing with identifiable information.²⁸⁷ Others have adopted a similar approach.²⁸⁸ According to the FTC, three considerations are most relevant: “as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the [FTC’s proposed] framework.”²⁸⁹ The FTC is trying to distinguish, in short, between data that are “reasonably identifiable” and data that are not, as well as between firms that are taking reasonable steps to prevent re-identification. Although Schwartz and Solove—and the FTC—are trying to use this new, third category of identifiable information to prevent the complete conceptual collapse of all data into the category of PII, that collapse may be inevitable in the Internet of Things context. If sensor datasets are so sparse that easy re-identification is the norm, then most Internet of Things data may be “reasonably identifiable.” The FTC’s standard—and the Schwartz and Solove solution—may mean that in the end all biometric and sensor-based Internet of Things data need to be treated as PII. That, however, would require a radical re-working of current law and practice. As we will see below, Internet of Things firms currently try to treat sensor data as “nonpersonal.”²⁹⁰ Corporate counsel, regulators, and legislators have not yet faced the reality that Internet of Things sensor data may all be identifiable. In short, privacy law—both on the books and on the ground—is unprepared for the threats created by the Internet of Things.

AT “People Can Opt Out”

You can't opt out in your home

Catherine Crump is a staff attorney with the ACLU’s Speech, Privacy, and Technology Project. She is a non-residential fellow with the Stanford Center for Internet and Society and an adjunct professor of clinical law at NYU, 2014, Mach 25, The Grows Around Us,

http://www.tomdispatch.com/post/175822/tomgram%3A_crump_and_harwood%2C_the_net_closes_around_us/

A future Internet of Things does have the potential to offer real benefits, but the dark side of that seemingly shiny coin is this: companies will increasingly know all there is to know about you. Most people are already aware that virtually everything a typical person does on the Internet is tracked. In the not-too-distant future, however, real space will be increasingly like cyberspace, thanks to our headlong rush toward that Internet of Things. With the rise of the networked device, what people do in their homes, in their cars, in stores, and within their communities will be monitored and analyzed in ever more intrusive ways by corporations and, by extension, the government. And one more thing: in cyberspace it is at least theoretically possible to log off. In your own well-wired home, there will be no “opt out.” You can almost hear the ominous narrator’s voice from an old “Twilight Zone” episode saying, “Soon the net will close around all of us. There will be no escape.” Except it’s no longer science fiction. It’s our barely distant present.

Consumers won't even know the devices are collecting information about them

Scott Pepper, Professor of Law, University of Colorado School of Law, August 2015, Regulating the Internet of Things: First Steps, <http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf>

Even Internet of Things devices far more innocuous than the Breathometer can generate data that present difficult issues. Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through “Big Data” analytics,¹⁹ these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities. I can tell a lot about you if I know that you often leave your oven on when you leave the house, fail to water your plants, don’t exercise, or drive recklessly.²⁰ As Federal Trade Commission (FTC) Commissioner Julie Brill recently stated: On the Internet of Things, consumers are going to start having devices, whether it’s their car, or some other tool that they have, that’s connected and sending information to a number of different entities, and the consumer might not even realize that they have a connected device or that the thing that they’re using is collecting information about them.²¹ These are the real challenges of

the Internet of Things: what information do these devices collect, how might that information be used, and what—if any—real choice do consumers have about such data?

Policies don't have enough information for consumers to make an informed choice

Scott Pepper, Professor of Law, University of Colorado School of Law, August 2015, Regulating the Internet of Things: First Steps, <http://www.texaslrev.com/wp-content/uploads/2015/08/Pepper-93-1.pdf>

Next, subpart II(D) considers the ways in which consumer protection law is also unprepared for the Internet of Things. In particular, I present the first survey in the legal literature of Internet of Things privacy policies and show the ways in which such policies currently fail consumers.⁴⁰ Internet of Things devices generally have no screen or keyboard, and thus giving consumers data and privacy information and an opportunity to consent is particularly challenging. Current Internet of Things products often fail to notify consumers about how to find their relevant privacy policy, and once found, such policies are often confusing, incomplete, and misleading. My review shows that such policies rarely clarify who owns sensor data, exactly what biometric or other sensor data a device collects, how such data are protected, and how such information can be sold or used. Both state and federal consumer protection law has not yet addressed these problems or the general issues that the Internet of Things creates for consumer consent.

You can't opt out of most of the information collected to enable the devices

Mark Lowenthal, June 30, 2014, Information Week, Internet of Things: Current Privacy Policies Don't Work, <http://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925>

The Internet of Things has gone mainstream. Consumers can use devices to control things in their houses from appliances to pet-food dispensers. Applications on mobile devices can measure how far and how fast the wearer has run or walked and can track heart rate and blood pressure. Connected sensors and devices, and their potential uses, are proliferating. But discussions about the data created are far more likely to focus on how *touse* the data rather than how to *protect* it. While devices and applications are generally designed and implemented with data protection in mind, that is unlikely to be enough. Developers and users must consider the broader implications for individual privacy as vast amounts of information -- about health, browsing history, purchasing habits, social and religious preferences, and finances, among other things -- accumulates. Internet of Things data, for now, is collected indiscriminately, and users have little inkling about how the data collected can be used for marketing, identification, and tracking. They typically ignore the privacy notices or terms of use, and the mechanisms for delivering the notices are often awkward, inconvenient, and unclear. The crucial question for the owner of the app or the device is whether data collection is limited to an identified purpose. The crucial question for users is whether they can determine when, how, and to what extent their information is communicated to others. Traditional privacy notions rely upon the Fair Information Practice Principles. While we can certainly look to FIPPs for guidance, they can't adequately address the issues posed by the Internet of Things because the traditional ways to deliver privacy guidelines -- posting

them online, mailing them, and online click-through mechanisms -- don't really work with IoT. Today, the data being collected on these devices is largely invisible to us. For instance, a driver behind the wheel has little discretion over traffic sensors that transmit speed, license-plate numbers, and location. Given the number of devices transmitting information during the course of a day, requiring notice and choice quickly becomes unwieldy, and innovation suffers.

FTC privacy notices useless to the IoT

Mark Lowenthal, June 30, 2014, Information Week, Internet of Things: Current Privacy Policies Don't Work, <http://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925>

The Federal Trade Commission has taken the position that developers of devices and apps must consider both use and collection restrictions and, in conjunction with the development of devices and apps, consider privacy by design, simplified choice, and transparency -- i.e., address the privacy issues by incorporating the core principles of FIPPs. That FTC expectation is difficult to meet in practice. Use restrictions are generally ineffective because they depend upon self-enforcement or third-party enforcement, and confidential information can't be retrieved once it is released. The same is true of collection restrictions: It is impossible to monitor every device to confirm that the data being collected is consistent with the purpose intended. Enforcement is complicated because there are multiple players -- the manufacturer, service networks, advertisers, and carriers, to start with -- and only the most egregious offenders are likely to attract regulators' attention. Developers and users can address some of the questions that the IoT raises by studying new approaches to protecting privacy, starting with those that account for the continuous communication of individual information. New approaches to IoT privacy should: Abandon traditional forms of privacy notices and instead adopt codes of conduct and terms of use based upon usage. Consider establishing frameworks for different types of connected devices. For example, common terms-of-use for any devices tied to smart grids that track electricity and water usage might be used to reward individuals for conservation and assist in determining utility pricing. Clearly and completely state the purpose for collection and the related context, including potential benefits to the individual. Collecting personal health data such as pulse rate, blood pressure, activity, and other vital statistics might be expected when it is being transmitted to an individual's healthcare provider which, in turn, may lead to more efficient medical and health treatment. But individuals may not know that a fitness bracelet or a mobile phone app that transmits such data might also be used to market other products or medications to them. Make personally identifiable data anonymous whenever possible in ways that prevent re-identification, so that users don't need to be concerned about the nature and use of data gathered by IoT devices. Explain the criteria used to gather and retain data, and communicate whether data is being retained to improve products, enhance further research, enhance security, etc. This sounds easy in the context of traditional privacy notices, but it may be problematic with products like Google Glass that gather data from all kinds of sources in the surrounding environment, making it

impossible to state with specificity what is being gathered and retained by the user. Finding ways to keep personally identifiable data anonymous with these types of devices may be the way to address this problem. Monitor data transmissions so that misuses can be blocked or trigger notices to affected users. Provide users reasonable access to their personally identifiable information, and give them the ability to change or correct it. The traditional privacy notice did not conceive of an Internet of Things. As the number of connected devices expands, the data collected will undoubtedly yield social benefits. However, the challenge will be finding a privacy paradigm that respects individual rights and accommodates choice and makes sure that the social benefits don't come at the cost of individual privacy. Progress won't wait for us to develop new ways to deal with this challenge, which is why we must give serious consideration to new approaches now.

IoT devices know everything about you

- . Andrew Guthrie Ferguson, Professor, Law, University of the District of Columbia, The Internet of Things and the Fourth Amendment Effects, 2016, CALIFORNIA LAW REVIEW v. 104, August 1,
http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4326&context=california_lawreview

At the time of the American founding, “things” were tangible things. Books did not live on a cloud.¹ Horse-drawn buggies were not tracked by GPS.² The manor’s hearth did not report the hourly change in temperature.³ Today, with the advent of the “Internet of Things,” objects in your house, car, office, and smartphone communicate, interact, report, track, and provide vast amounts of data about the activities of their owners.⁴ Amazon’s Kindle knows the last page you read.⁵ General Motor’s “OnStar System” knows the speed, direction, and travel patterns of your car.⁶ The Nest Learning Thermostat knows your preferred temperature for sleeping and what time you leave home for the day.⁷ “Things” have become interactive devices as a result of the growing network of ubiquitous chips and sensors placed in our everyday objects.

Opt-in fails to protect privacy

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

The Failure of Opt-in Consent. — Some argue that the answer to the many problems of consent is to move to a more explicit and affirmative method of procuring consent: an opt-in rather than opt-out

regime. As stated by FTC Commissioner Jon Leibowitz, companies should move to a model where consumers “‘opt in’ when it comes to collecting information — especially when it comes to sharing consumer information with third parties and sharing it across various web-based services.”⁷⁹

Despite my early optimism about opt-in, I now believe it will fail. One reason is that many organizations will have the sophistication and motivation to find ways to generate high opt-in rates. They can do so simply by conditioning products, services, or access on opting in. As Schwartz has aptly noted, “many data-processing institutions are likely to be good at obtaining consent on their terms regardless of whether the default requires consumers to authorize or preclude information-sharing.”⁸⁰

Moreover, “consumers are likely to be far more sensitive to price terms, such as the cost of a checking account, than to nonprice terms like the financial institution’s privacy policies and practices.”⁸¹ In-deed, agreeing to clickwrap contracts and end-user license agreements is often a prerequisite for obtaining access to a website or to use a product or service. Consider the end-user license agreement to Apple’s iTunes Store.⁸² Periodically, this agreement pops up and people are required to agree. On an iPhone, the text of this agreement often ex-tends to more than fifty screens. If people want to download apps from the store, they have no choice but to agree. This requirement is akin to an opt-in system — affirmative consent is being sought. But hardly any bargaining or choosing occurs in this process. Thus, de-spite regulators’ best intentions, an opt-in system or a requirement of affirmative consent for most new uses of data will likely lead to more buttons to click and more forms to sign, but not to more meaningful privacy protection.

Terms of Service agreements are useless

Andrew W. Bagley, privacy counsel, CrowdStrike and Director of Operations, Secure Domain Foundation and Justin S. Brown, Limited Consumer Privacy Protections Against the Layers of Big Data, SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL v. 31, 2014-2015,
<http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1599&context=chtlj>

Digital consumers rarely review terms of service agreements with detailed scrutiny and those who do may not have the legal knowledge to understand them fully and thus self-manage their privacy.⁷³ If they read the agreements carefully, perhaps there would be a chilling effect on their behavior because of the agreements' broad and ambiguous terms.⁷⁴ Furthermore, sometimes service providers change terms without acquiring new informed consent from the users.⁷⁵ To make matters worse, terms of service agreements are generally not visually inviting to their intended audience.⁷⁶ The features of a website might even provide a user with apparent rights and privileges to affect data.⁷⁷ Commentators have suggested that such features should be considered in the interpretation and enforcement of online contracts,⁷⁸ but instead the plain language of the terms of service is given legal weight.⁷⁹ Despite all of these misgivings, a consenting user seems to be making a long-term commitment to the control of their data by other parties for uses that are unimaginable at the time of consent.⁸⁰ In effect, consent garnered quickly at one layer through a click-through agreement is being employed as a marketing and data collection tool for third parties to use throughout the layers of the Internet.

AT “You Don’t Have to Share Your Data”

You do in a smart city

Kelsey Finch, Westin Research Fellow, International Association of Privacy Professionals, 2015, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town,” FORDHAM URBAN LAW JOURNAL v. 41, <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2549&context=ulj>,

In the market, privacy can be a competitive differentiator, and users have some degree of control over when and how to exchange data for services. In a smart city, however, urbanites have few, if any, alternatives, particularly when it comes to essential infrastructure. Cities will have only one smart grid, one subway system, and one set of emergency services available to the public. Public services have captive populations who cannot opt out of information collection without paying a steep price in safety, convenience, and quality of life. Recommendations for how to stay off the grid include a host of antisurveillance techniques (e.g., paying only in cash, avoiding loyalty cards, doing without a mobile phone, limiting driving—and avoiding bridges, tolls, and major highways when doing so—and using maps instead of GPS)⁸⁸ and technologies (e.g., fingerprint gel, white noise generators, faraday cages to block mobile device signals, and LEDlined clothing to white out infrared signals).⁸⁹ Even services designed to help urbanites avoid CCTV cameras, such as i-SEE in Manhattan, can chart only “paths of least surveillance.”⁹⁰ Moreover, because smart cities deploy a wide array of sensors and monitoring technologies through shared infrastructure systems, even those city dwellers who select privacy-aware services will inevitably find their activities tracked in public by default

AT First Amendment Right to Exchange Information

The First Amendment Right to exchange information shouldn't protect data exchange

Julie E. Cohen, law professor, Georgetown, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000),
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub>

The First Amendment argument against data privacy protection begins by assuming that the collection, processing, and exchange of personally- identified data are “speech,” and then asserts that regulation of these activi- ties cannot survive the requisite scrutiny.¹³⁴ Both steps bear closer scrutiny. As applied to data privacy regulation, the standard balancing analysis has been categorical, driven by outcome- determining presuppositions about the expressive content and ownership status of personally-identified information. Closer attention to the competing interests that data privacy regulation seeks to balance might produce a different assessment of the constitutionality of generally-applicable protective measures. More fundamentally, though, there is reason to question whether the traditional modes of First Amendment review should apply in the same way, or at all, to regulation of commercial processing of personal information. Other approaches to theorizing about speech, and about information more generally, suggest different ways of thinking about the collection and exchange of personally-identified data and the role of these activities within the broader commercial fabric of society.

As an initial matter, a First Amendment analysis of data privacy protec- tion must consider how to characterize the sort of speech involved. Tradi- tionally, the threshold for regulation of speech classed as “commercial” has been lower than the threshold for regulation of other speech.¹³⁵ Both some advocates and some opponents of strong data privacy protection have as- sumed that the collection and exchange of personally-identified data by commercial entities is most appropriately classified as commercial speech, and the handful of courts that have addressed First Amendment challenges to data privacy regulations have

followed suit.¹

Many regulations on information exchange

Julie E. Cohen, law professor, Georgetown, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000),
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub>

As a society, we regulate the exchange of information as property all the time, and do so based on market-institutional considerations. In addition, the law routinely allows private parties to invoke property or contract rights to restrict others' speech. If collections of personally-identified data are like other sorts of regulated information, or if individuals have property or contractual interests that extend to (at least some) personally-identified information on an ongoing basis, the First Amendment landscape changes.

AT Privacy Undermines the Collective

Privacy strengthens the collective by making participation in democratic government more likely and more effective

Julie E. Cohen, law professor, Georgetown, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000),
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub>

The autonomy fostered by informational privacy also generates more concrete collective benefits.

Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions—political, economic, and social. The cornerstone of a democratic society is informed and deliberate self-governance. The formation and reformation of political preferences—essential both for reasoned public debate and informed exercise of the franchise—follows the pattern already discussed: Examination chills experimentation with the unorthodox, the unpopular,

and the merely unfinished. A robust and varied debate on matters of public concern requires the opportunity to experiment with self-definition in private, and (if one desires) to keep distinct social, commercial, and political associations separate from one another.¹⁹⁸ Here again the point is relative. People will still make choices under conditions of no-privacy, and targeted commercial advertising can be used to manufacture political preferences (or political apathy) as well. But if we do not wish to live in communities governed by apathy, impulse, or precautionary conformism, we must produce individuals capable of governing themselves.¹⁹⁹ The same qualities that produce the capacity for political self-government also produce innovation in markets and in the

governance of market institutions. I have argued that the welfare of markets is properly viewed as subordinate to the welfare of society as a whole, but it does not follow that markets are unimportant. The health of markets as institutions within a democratic society is vitally important to overall social welfare. And dynamic, competitive markets require inventors as well as consumers and entrepreneurs as well as audiences.²⁰⁰ Inventiveness and entrepreneurship, in turn, require the ability to think outside or around existing, predictable technological and social patterns. A regime built on pervasive practices of monitoring, prediction, and preference-shaping is far more likely to stifle these habits of independent thought than to stimulate them. At the same time, though, the insulation provided by informational

privacy also plays a subtler, more conservative role in reinforcing the existing social fabric. Sociologist Erving Goffman demonstrated that the construction of social facades to mediate between self and community is both instinctive and expected.²⁰¹ Alan Westin describes this social dimension of privacy as “reserve.”²⁰² This characterization, though, seems incomplete. On Goffman’s account, the

construction of social personae isn’t just about withholding information that we don’t want others to have. It is about defining the parameters of social interaction in ways that maximize social ease, and thus is about collective as well as individual comfort.²⁰³ We do not need, or even want, to know each other that well. Less information makes routine interactions easier; we are then free to choose, consensually and without embarrassment, the interactions that we wish to treat as less routine. Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of that term. Last, but hardly least, a societal commitment to informational

privacy has an important role to play in defining our collective vision of the role of information technologies, and technique more broadly, within society.²⁰⁴ Technological progress affords a yardstick for measuring human achievement, but not the only or most important one.²⁰⁵ To appreciate other measures of progress, we must be sensitive to the limits of technique, and recognize the hubris inherent in pretensions to total prediction and control.²⁰⁶ A protected zone of informational autonomy is valuable, in short, precisely because it reminds us what we cannot measure.

AT Good to Trade Privacy for Convenience

Life is about more than convenience

Jathan Sadowski, journalist, Why Does Privacy Matter? One Scholar's Answer, The Atlantic, February 26, 2013, www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/

In light of these considerations, what's really at stake in a feature like [Facebook's rumored location-tracking app](#)? You might think it is a good idea to willfully hand over your data in exchange for personalized coupons or promotions, or to broadcast your location to friends. But consumption -- perusing a store and buying stuff -- and quiet, alone time are both important parts of how we define ourselves. If how we do that becomes subject to ever-present monitoring it can, if even unconsciously, change our behaviors and self-perception.

AT Privacy Violations Undermine Usage of the IoT

Facebook denies – billions register despite privacy concerns

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-5B2013-George-Mason-Law-Rev%5D.pdf>

Moreover, the DOC's claim that "an erosion of trust will inhibit the adoption of new technologies"¹¹⁷ does not seem credible when more than one billion people have registered Facebook accounts¹¹⁸ despite the heightened privacy concerns surrounding that popular social networking site.¹¹⁹ Consumers are using many other online sites and services in record numbers despite privacy and security concerns. Survey data from the Pew Internet & American Life Project, which tracks consumer trends, shows that broadband adoption, digital device ownership, and online participation continue to grow steadily over time.¹²⁰ comScore has also noted that, in 2012, "[a] staggering 5.3 trillion display ad impressions were delivered in the U.S.," a 6 percent increase over the previous year, and that "more than 450 billion U.S. content video views occurred via a desktop computer, representing an all-time high and an increase of 7 percent over 2011."¹²¹ Also, a 2009 study of 2,600 consumers conducted by the National Retail Federation asked online shoppers the reasons they might not be spending as much online during the holiday season that year.¹²² Of those who said they would be spending less online, the leading reasons were expensive shipping charges (22.8%), a preference to see or handle items before they buy them (12.5%), or a preference for buying in physical stores (10.8%).¹²³ By contrast, consumers expressed far less concern about online security (1.1%), credit card theft (0.6%), privacy (0.1%), or concerns about retailers tracking online activity (0.1%).¹²⁴

AT Privacy is a Commodity, People Voluntarily Give it Up

Claims that it is good to let people give up information to get services sacrifices the poor who are less able to protect their interests

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

Markets also denigrate privacy by encouraging us to think of privacy as a commodity to be traded. In theory, you can make a market for anything.⁶⁵ Perhaps some people are fine with companies or the government knowing more about them, and they are happy to “pay” for content, security, or service with their privacy.⁶⁶ A considerable literature sees a problem with this privacy market because of how poor we are at managing our privacy;⁶⁷ we undervalue it, and we can be nudged by subtle framing or design into disclosing more information than may be good for us.⁶⁸ Recent work of social psychologists is highly instructive in this regard.⁶⁹

This turns people into commodities

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

Still others—including this author—worry that firms can and do abuse the power they hold over consumers by virtue of knowing so much about them. Thus, for instance, firms have an incentive to engage in individualized “market manipulation” whereby each consumer is targeted on the basis of his or her specific set of biases or approached at a time when he or she is most vulnerable.⁷² Alternatively, firms will use what they know to sort consumers into high priority targets to cultivate aggressively, or lower priority targets to discriminate against or ignore.

We shouldn't allow data to define the self

- . Ryan Calo, December 2015, Assistant Professor, Law and Assistant Professor, Information Science, University of Washington, Privacy and Markets: A Love Story, NOTRE DAME LAW REVIEW v. 91, <http://ndlawreview.org/wp-content/uploads/2013/05/ndl204.pdf>

AT Data is Speech

All speech is not protected by the First Amendment

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

The “data is speech” argument has a certain superficial appeal. After all, if the First Amendment is about protecting people’s ability to share ideas and information, and data is information, then the First Amendment should protect people’s ability to share data. The argument is clear, and it is consistent— everything is speech, and everything is protected. But this argument’s consistency is a foolish consistency. Just because something is “speech” doesn’t mean it is beyond regulation. Nor does the fact that something is labeled “speech” qualify it for special protection by the First Amendment. Humans do lots of things every day with words—we talk on the phone, we write books and emails and blogs, we sing in the shower. But people also use words to hire assassins, engage in insider trading, sexually harass subordinates in the workplace, and verbally abuse their children. All of these are “speech,” but many of them are well outside the main concerns of the First Amendment. We need to protect some, but we need to regulate others. This is a problem. Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (pp. 84-85). Oxford University Press. Kindle Edition.

Protecting data as speech produces enormous social inequality

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Rejecting Digital Lochner There’s a famous parable in constitutional law that has been taught to virtually every first-year law student for decades. The parable goes smething like this. In the late nineteenth and early twentieth centuries, the Industrial Revolution transformed American society. On the one hand, it produced great fortunes and technological innovation that made what had been impossible commonplace. These new innovations included factories, steam engines, railroads, cars, airplanes, and cheap textiles, and shaped the modern world into a form that we (or at least our parents) could recognize. But on the other hand, the Industrial Revolution produced enormous social costs, including huge wealth inequality, poverty, child labor, unsafe industrial working conditions, and pollution. Faced with these problems, Congress and the state legislatures tried to fix the issues of the perilous industrial workplace while preserving its benefits.

Progressive legislators passed laws preventing child labor, regulating unsafe working conditions, and imposing minimum wage and maximum hours laws, overtime requirements, product labeling laws, and antitrust laws.⁵⁴ But the Supreme Court struck many of these laws down as infringements on personal liberty. Afraid that laws regulating economic transactions could lead to wealth redistribution or socialism, the Court held that much of this economic regulation violated the Fourteenth Amendment’s Due Process Clause, infringing on the rights of workers and employers to what it called the “liberty of contract.”⁵⁵ This era in Supreme Court history is named after the infamous 1905 case of *Lochner v. New York*.⁵⁶ In *Lochner*, the Supreme Court struck down a New York law regulating the safety of bakers. *Lochner* was not the first Supreme Court case to protect economic rights against government regulation, nor was it the last, but it is

the case that has given its name to the era of strong constitutional protection of economic rights, lasting from the late nineteenth century until the late 1930s.⁵⁷ The Lochner Court's economic libertarianism rested on the idea that private property was the bulwark of political liberty, and that a government that has the power to redistribute wealth is a grave threat to liberty.⁵⁸ These ideas have a strong tradition in Anglo-American political thought, but there was a problem. A broad government power to regulate economic matters also allows regulations such as minimum wages, maximum hours, workplace safety, and the right to collective bargaining. During the Industrial Revolution, the conservative economic, libertarian view of the Constitution became inconsistent with the needs of a modern, industrial economy. This inconsistency became most apparent during the Great Depression, when Lochner-style doctrines were used to invalidate portions of the New Deal.⁵⁹ Thus, in the industrial era, a libertarian view of industrial economic liberty made needed regulation impossible. I fear that acceptance of the "data is speech" argument will repeat these errors of the Industrial Age for the Information Age. Today, great chunks of human society are being transformed into digital form, and we all leave digital footprints every day as we live our lives. It is essential that we preserve strong civil liberties in our digital future—much of this book is about how to do that in the context of thinking, reading, and speaking. But if the lessons of the twentieth century are that government regulation is sometimes necessary in an industrial economy, we should not forget those lessons in our information economy. In a 2005 article published before the Sorrell litigation, I made an argument along these lines.⁶⁰ Justice Breyer made a similar point in his Sorrell dissent, arguing that "[a]t best the Court opens a Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect a commercial message. At worst, it reawakens Lochner's pre-New Deal threat of substituting judicial for democratic decisionmaking where ordinary economic regulation is at issue."⁶¹ The many new uses to which we can put data create new possibilities, but also new problems. We need to make choices as a society about what kinds of data privacy rules we should have, and about when data should flow freely. In fact, we might ultimately decide that the best policy is to have very little data privacy. Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (p. 90). Oxford University Press. Kindle Edition.

If data is thought of as speech we will not be able to regulate social ills

Neil Richards, law professor, Washington University, 2015, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Kindle edition, page number at end of card

But however we as a society choose to regulate data flows, we must be able to choose. We must not be sidetracked by misleading First Amendment arguments, because the costs of not regulating the trade in commercial data are significant. As we enter the Information Age, where the trade in information is a multibillion-dollar industry, government should be able to regulate the huge flows of personal information as well as the uses to which this information can be put. Moreover, if our lives become digital, but if data is speech, regulation of many kinds of social problems will become impossible. There will certainly be cases at the borders, because of course data will sometimes be tied to important expression. But this is an insufficient reason to give up on regulation of our society as it digitizes. At the dawn of the Industrial Age, business interests persuaded the Supreme Court in the *Lochner* case that the freedom of contract should immunize them from regulation. We must reject the similar calls of modern advocates for digital *Lochner*.

Richards, Neil. Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (p. 90). Oxford University Press. Kindle Edition.

Negative Arguments

Terrorism

Terrorism DA

– Domestic surveillance successfully checks terror incidents now. Prefer longitudinal studies.

Boot '13

Max Boot is a Senior Fellow in National Security Studies at the Council on Foreign Relations. In 2004, he was named by the World Affairs Councils of America as one of "the 500 most influential people in the United States in the field of foreign policy." In 2007, he won the Eric Breindel Award for Excellence in Opinion Journalism. From 1992 to 1994 he was an editor and writer at the Christian Science Monitor. Boot holds a bachelor's degree in history, with high honors, from the University of California, Berkeley and a master's degree in history from Yale University. Boot has served as an adviser to U.S. commanders in Iraq and Afghanistan. He is the published author of *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present*. From the article: "Stay calm and let the NSA carry on" - LA Times – June 9th - <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

After 9/11, there was a widespread expectation of many more terrorist attacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon bombing), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's monitoring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terrorist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists. For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it. But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic, Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours. Which brings us to the current kerfuffle over two NSA monitoring programs that have been exposed by the Guardian and the Washington Post. One program apparently collects metadata on all telephone calls made in the United States. Another program provides access to all the emails, videos and other data found on the servers of major Internet firms such as Google, Apple and Microsoft. At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to "non-U.S. persons" who are abroad and thereby enjoy no constitutional protections. These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities. It's possible that like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these programs have been effective in disrupting terrorist plots. Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a "scandal," to use a term now loosely being tossed around. The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

Link – curtailing surveillance boosts terror risks. That risk's serious and underestimated.

Lewis '14

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy. Before joining CSIS, he worked at the US Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His diplomatic experience included negotiations on military basing in Asia, the Cambodia peace process, and the five-power talks on arms transfer restraint. Lewis received his Ph.D. from the University of Chicago. "Underestimating Risk in the Surveillance Debate" - CENTER FOR STRATEGIC & INTERNATIONAL STUDIES - STRATEGIC TECHNOLOGIES PROGRAM – December - <http://csis.org/publication/underestimating-risk-surveillance-debate>

Americans are reluctant to accept terrorism is part of their daily lives, but attacks have been planned or attempted against American targets (usually airliners or urban areas) almost every year since 9/11. Europe faces even greater risk, given the thousands of European Union citizens who will return hardened and radicalized from fighting in Syria and Iraq. The threat of attack is easy to exaggerate, but that does not mean it is nonexistent. Australia's then-attorney general said in August 2013 that communications surveillance had stopped four "mass casualty events" since 2008. The constant planning and preparation for attack by terrorist groups is not apparent to the public. The dilemma in assessing risk is that it is discontinuous. There can be long periods with no noticeable activity, only to have the apparent calm explode. The debate over how to reform communications surveillance has discounted this risk. Communications surveillance is an essential law enforcement and intelligence tool. There is no replacement for it. Some suggestions for alternative approaches to surveillance, such as the idea that the National Security Agency (NSA) only track known or suspected terrorists, reflect wishful thinking, as it is the unknown terrorist who will inflict the greatest harm.

Vigilance link - Strong intel gathering's key to discourages initiation of BW attacks.

Pittenger '14

US Rep. Robert Pittenger, chair of Congressional Task Force on Terrorism, "Bipartisan bill on NSA data collection protects both privacy and national security" - Washington Examiner, 6/9/14, http://washingtonexaminer.com/rep.-robert-pittenger-bipartisan-bill-on-nsa-data-collection-protects-both-privacy-and-national-security/article/2549456?custom_click=rss&utm_campaign=Weekly+Standard+Story+Box&utm_source=weeklystandard.com&utm_medium=referral

This February, I took that question to a meeting of European Ambassadors at the Organization for Security and Cooperation in Europe. During the conference, I asked three questions: 1. What is the current worldwide terrorist threat? 2. What is America's role in addressing and mitigating this threat? 3. What role does intelligence data collection play in this process, given the multiple platforms for attack including physical assets, cyber, chemical, biological, nuclear and the electric grid? Each ambassador acknowledged the threat was greater today than before 9/11, with al Qaeda and other extreme Islamist terrorists stronger, more sophisticated, and having a dozen or more training camps throughout the Middle East and Africa. As to the role of the United States, they felt our efforts

were primary and essential for peace and security around the world. Regarding the intelligence-gathering, their consensus was, “We want privacy, but we must have your intelligence.” As a European foreign minister stated to me, “Without U.S. intelligence, we are blind.” We cannot yield to those loud but misguided voices who view the world as void of the deadly and destructive intentions of unrelenting terrorists. The number of terrorism-related deaths worldwide doubled between 2012 and 2013, jumping from 10,000 to 20,000 in just one year. Now is not the time to stand down. Those who embrace an altruistic worldview should remember that vigilance and strength have deterred our enemies in the past. That same commitment is required today to defeat those who seek to destroy us and our way of life. We must make careful, prudent use of all available technology to counter their sophisticated operations if we are to maintain our freedom and liberties.

Terrorism Links

Bulk collection is vital to reduce terrorism risk – terrorists will use the plan’s privacy protection to hide communications

Lewis 5/28 – Director and Senior Fellow, Strategic Technologies Program (James Lewis, “What Happens on June 1?”, CSIS Strategic Technologies Program, [http://www.csistech.org/blog/2015/5/28/what-happens-on-june-1, 5/28/2015\) //MBB](http://www.csistech.org/blog/2015/5/28/what-happens-on-june-1, 5/28/2015) //MBB)

After a week or so, potential attackers will probably look for ways they can exploit newly unsurveilled space for operational advantage. Risk will increase steadily once they get over their shock, and then plateau two or three months out (when they've presumably adjusted their operations to reduced surveillance). How much risk increases will depend on whether the USG can compensate for the lost collection and whether attackers find ways to gain advantage.

All the propaganda about how this kind of collection "never stopped an attack" is divorced from reality. It is the the totality of collection that reduced risk. Reduce collection and risk increases. How much is unclear, and Americans may be willing to trade a small increase in risk for less government surveillance. 215 is probably the least valuable program, and ending it creates the least risk, but ending it is not risk free.

Adding some privacy advocates to the Foreign Intelligence Surveillance Court will also increase risk. We don't do this for any other kind of warrant process, and it will add delays. One of the problems with FISC that led to the 9/11 success (for the other side) was the slowness of its processes. Adding privacy advocates will return us to the bad old days of FISA. It's also insulting to the judges.

Attempting to preclude NSA ‘domestic’ surveillance guts their ability to do bulk collection – they lack the technological ability to distinguish

Donohue, 15 - Professor of Law, Georgetown University Law Center (Laura, “SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT” 38 Harv. J.L. & Pub. Pol'y 117, Winter, lexis)

In its October 2011 memorandum opinion, the court confronted two areas: first, targeting procedures as applied to the acquisition of communications other than Internet transactions -- that is, "discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection." n290 As in the past, the court found the targeting procedures with regard to non-Internet transactions to be sufficient. Second, the court considered de novo the sufficiency of the government's targeting procedures in relation to Internet transactions [*192] transactions. n291 Despite the acknowledgement by the government that it knowingly collected tens of thousands of messages of a purely domestic

nature, FISC found the procedures consistent with the statutory language that prohibited the intentional acquisition of domestic communications. n292

The court's analysis of the targeting procedures focused on upstream collection. n293 At the time of acquisition, the collection devices lacked the ability to distinguish "between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector." n294 The court continued: "As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it." n295 Because of the enormous volume of communications intercepted, it was impossible to know either how many wholly domestic communications were thus acquired or the number of non-target or U.S. persons' communications thereby intercepted. n296 The number of purely domestic communications alone was in the tens of thousands. n297

Despite this finding, FISC determined that the targeting procedures were consistent with the statutory requirements that they be "reasonably designed" to (1) "ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States" and (2) "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." n298

To reach this conclusion, the court read the statute as applying, in any particular instance, to communications of individuals "known at the time of acquisition to be located in the United [*193] States." n299 As the equipment did not have the ability to distinguish between purely domestic communications and international communications, the NSA could not technically know, at the time of collection, where the communicants were located. From this, the court was "inexorably led to the conclusion that the targeting procedures are 'reasonably designed' to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." n300 This was true despite the fact that the NSA was fully aware that it was collecting, in the process, tens of thousands of domestic communications. n301 As far as the targeting procedures were concerned, at least with regard to MCTs, the NSA had circumvented "the spirit" but not the letter of the law. n302

The court's reading led to an extraordinary result. The statute bans the knowing interception of entirely domestic conversations. The NSA said that it knowingly intercepts entirely domestic conversations. Yet the court found its actions consistent with the statute.

A few points here deserve notice. First, it is not immediately clear why the NSA is unable to determine location at the moment of intercept and yet can ascertain the same at a later point. Second, in focusing on the technical capabilities of any discrete intercept, the court encouraged a form of willful blindness--that is, an effort to avoid criminal or civil liability for an illegal act by intentionally placing oneself into a position to be unaware of facts that would otherwise create liability. n303 In light of the court's interpretation, [*194] the NSA has a diminished interest in determining at the point of intercept whether intercepted communications are domestic in nature. Its ability to collect more information would be hampered. So there is a perverse incentive structure in place, even though Congress intended the provision to protect individual privacy.

Restrictions on collection of data aid terrorism – protections against misuse of data solve better

Posner, 6 - judge on the United States Court of Appeals for the Seventh Circuit in Chicago and a Senior Lecturer at the University of Chicago Law School (Richard, Not a Suicide Pact: The Constitution in Time of National Emergency, p. 143-144)

Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: anonymity combined with the secure encryption of digitized data makes the Internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defense of national security. But if this is permitted, intelligence officers are going to be scrutinizing a mass of personal information about U.S. citizens. And we know that people don't like even complete strangers poring over the details of their private lives. But the fewer of these strangers who have access to those details and the more professional their interest in them, the less the affront to privacy. One reason people don't much mind having their bodies examined by doctors is that they know that doctors' interest in bodies is professional rather than prurient; we can hope that the same is true of intelligence professionals.

The primary danger of such data mining is leaks by intelligence personnel to persons inside or outside the government who might use the leaked data for improper purposes. Information collected by a national security data-mining program would have to be sharable within the national security community, which would include in appropriate cases foreign intelligence services, but not beyond. Severe sanctions and other security measures (encryption, restricted access, etc.) could and should be imposed in order to prevent—realistically, to minimize—the leakage of such information outside the community. My suggestion in the last chapter that the principle of the Pentagon Papers case be relaxed to permit measures to prevent the media from publishing properly classified information would reinforce protection of the privacy of information obtained by national security data mining.

I have said both that people value their informational privacy and that they surrender it at the drop of a hat. The paradox is resolved by noting that as long as people don't expect that the details of their health, love life, or finances will be used to harm them in their interactions with other people, they are content to reveal those details to strangers when they derive benefits from the revelation. As long as intelligence personnel can be trusted to use their knowledge of such details only for the defense of the nation, the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks.

– advance surveillance is necessary to generate enough information to target terrorists

Sales, 14 - Associate Professor of Law, Syracuse University College of Law (Nathan, I/S: A Journal of Law and Policy for the Information Society, “Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy” 10 ISJLP 523, Summer, lexis)

Programmatic surveillance thus can help remedy some of the difficulties that arise when monitoring covert adversaries like international terrorists. FISA and other particularized surveillance tools are useful when authorities want to monitor targets whose identities are already known. But they are less useful when authorities are trying to identify unknown targets. The problem arises because, in order to obtain a wiretap order from the FISA court, the government usually must demonstrate probable cause to believe that the target is a foreign power or agent of a foreign power. n39 This is a fairly straightforward task when the target's identity is already known--e.g., a diplomat at the Soviet embassy in Washington, DC. But the task is considerably more difficult when the government's reason for surveillance is to detect targets who are presently unknown--e.g., al-Qaeda members who operate in the shadows. How can you convince the FISA court that Smith is an agent of a foreign power when you know nothing about Smith--his name, nationality, date of birth, location, or even whether he is a single person or several dozen? The government typically won't know those things unless it has collected some information about Smith--such as by surveilling him. And there's the rub. Programmatic monitoring helps avoid the crippling Catch-22 that can arise under particularized surveillance regimes like FISA: officials can't surveil unless they show that the target is a spy or terrorist, but sometimes they can't show that an unknown target is a spy or terrorist unless they have surveilled him.

the government needs the widest possible net, including domestic surveillance

Posner, 6 - judge on the United States Court of Appeals for the Seventh Circuit in Chicago and a Senior Lecturer at the University of Chicago Law School (Richard, Not a Suicide Pact: The Constitution in Time of National Emergency, p. 94-96

According to the administration, these are just interceptions of communications to and from the United States in which one of the parties is suspected of terrorist connections, though the suspicion does not rise to the probable-cause level that would be required for obtaining a warrant. There may be more to the program, however. Most likely the next terrorist attack on the United States will, like the last one, be mounted from within the country but be orchestrated by leaders safely ensconced somewhere abroad. If a phone number in the United States is discovered to have been called by a known or suspected terrorist abroad, or if the number is found in the possession of a suspected terrorist or in a terrorist hideout, it would be prudent to intercept all calls, domestic as well as international, to or from that U.S. phone number and scrutinize them for suspicious content. But the mere fact that a suspected or even known terrorist has had a phone conversation with someone in the United States or has someone's U.S. phone number in his possession doesn't create probable cause to believe that the other person is also a terrorist; probably most phone conversations of terrorists are with people who are not themselves terrorists. The government can't get a FISA warrant just to find out whether someone is a terrorist; it has to already have a reason to believe he's one. Nor can it conduct surveillance of terrorist suspects who are not believed to have any foreign connections, because such surveillance would not yield foreign intelligence information.

FISA has yet another gap. A terrorist who wants to send a message can type it in his laptop and place it, unsent, in an e-mail account, which the intended recipient of the message can access by knowing the account name. The message itself is not communicated. Rather, it's as if the recipient had visited the sender and searched his laptop. The government, if it intercepted the e-

mail from the intended recipient to the account of the “sender,” could not get a FISA warrant to intercept (by e-mailing the same account) the “communication” consisting of the message residing in the sender’s computer, because that message had never left the computer.

These examples suggest that surveillance outside the narrow bounds of FISA might significantly enhance national security. At a minimum, such surveillance might cause our foreign terrorist enemies to abandon or greatly curtail their use of telephone, e-mail, and other means of communicating electronically with people in the United States who may be members of terrorist sleeper cells. Civil libertarians believe that this is bound to be the effect of electronic surveillance, and argue that therefore such surveillance is futile. There is no “therefore.” If the effect of electronic surveillance is to close down the enemy’s electronic communications, that is a boon to us because it is far more difficult for terrorist leaders to orchestrate an attack on the United States by sending messages into the country by means of couriers. But what is far more likely is that some terrorists will continue communicating electronically, either through carelessness—the Madrid and London bombers were prolific users of electronic communications, and think of all the drug gangsters who are nailed by wiretaps—or in the mistaken belief that by using code words or electronic encryption they can thwart the NSA. (If they can, the program is a flop and will be abandoned.) There are careless people in every organization. If al-Qaeda is the exception, civil libertarians clearly are underestimating the terrorist menace! In all our previous wars, beginning with the Civil War, when telegraphic communications were intercepted, our enemies have known that we might intercept their communications, yet they have gone on communicating and we have gone on intercepting. As for surveillance of purely domestic communications, it would either isolate members of terrorist cells (which might, as I said, have no foreign links at all) from each other or yield potentially valuable information about the cells.

FISA’s limitations are borrowed from law enforcement. When a crime is committed, the authorities usually have a lot of information right off the bat—time, place, victims, maybe suspects—and this permits a focused investigation that has a high probability of eventuating in an arrest. Not so with national security intelligence, where the investigator has no time, place, or victim and may have scant idea of the enemy’s identity and location; hence the need for the wider, finer-meshed investigative net. It is no surprise that there have been Leaks from inside the FBI expressing skepticism about the NSA program. This skepticism reflects the Bureau’s emphasis on criminal investigations, which are narrowly focused and usually fruitful, whereas intelligence is a search for the needle in the haystack. FBI agents don’t like being asked to chase down clues gleaned from the NSA’s interceptions; 999 out of 1,000 turn out to lead nowhere. They don’t realize that often the most that counterterrorist intelligence can hope to achieve is to impose costs on enemies of the nation (as by catching and “turning” some, or forcing them to use less efficient means of communication) in the hope of disrupting their plans. It is mistaken to think electronic surveillance a failure if it doesn’t intercept a message giving the time and place of the next attack.

Section 702 needed for pattern analysis that can identify future terrorist threats

Sales, 14 - Associate Professor of Law, Syracuse University College of Law (Nathan, I/S: A Journal of Law and Policy for the Information Society, “Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy” 10 ISJLP 523, Summer, lexis)

Programmatic surveillance initiatives like these differ in simple yet fundamental ways from the traditional forms of monitoring with which many people are familiar--i.e., individualized or particularized surveillance. Individualized surveillance takes place when authorities have some reason to think that a specific, known person is breaking the law. Investigators will then obtain a court order authorizing them to collect information about the target, with the goal of assembling evidence that can be used to establish guilt in subsequent criminal proceedings. Individualized surveillance is common in the world of law enforcement, as under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. n23 It is also used in national security investigations. FISA allows authorities to obtain a court order to engage in wiretapping if they demonstrate, among other things, probable cause to believe that the target is "a foreign power or an agent of a foreign power." n24

By contrast, programmatic surveillance has very different objectives and is conducted in a very different manner. It usually involves the government collecting bulk data and then examining it to identify previously unknown terrorists, spies, and other national security threats. A good example of the practice is link analysis, in [*528] which authorities compile large amounts of information, use it to map the social networks of known terrorists--has anyone else used the same credit card as Mohamed Atta?--and thus identify associates with whom they may be conspiring. n25 (It is also possible, at least in theory, to subject these large databases to pattern analysis, in which automated systems search for patterns of behavior that are thought to be indicative of terrorist activity, but it's not clear that the NSA is doing so here.) Suspects who have been so identified can then be subjected to further forms of monitoring to determine their intentions and capabilities, such as wiretaps under FISA or other authorities. In a sense, programmatic surveillance is the mirror image of individualized surveillance. With individualized monitoring, authorities begin by identifying a suspect and go on to collect information; with programmatic monitoring, authorities begin by collecting information and go on to identify a suspect.

Programmatic surveillance is a potentially powerful counterterrorism tool. The Ra'ed al-Banna incident is a useful illustration of how the technique, when coupled with old-fashioned police work, can identify possible threats who otherwise might escape detection. Another example comes from a 2002 Markle Foundation study, which found that authorities could have identified the ties among all 19 of the 9/11 hijackers if they had assembled a large database of airline reservation information and subjected it to link analysis. n26 In particular, two of the terrorists--Nawaf al-Hamzi and Khalid al-Mihdhar--were on a government watchlist after attending a January 2000 al-Qaeda summit in Malaysia. So they could have been flagged when they bought their tickets. Querying the database to see if any other passengers had used the pair's mailing addresses would have led investigators to three more hijackers, including Mohamed Atta, the plot's operational leader. Six others could have been found by searching for passengers who used the same frequent-flyer and telephone numbers as these suspects. And so on. Again, the Markle study concerns airline reservation data, not the communications data that are the NSA's focus. But it is still a useful illustration of the technique's potential.

The government claims that programmatic surveillance has been responsible for concrete and actual counterterrorism benefits, not just hypothetical ones. Officials report that PRISM has helped detect and [*529] disrupt about 50 terrorist plots worldwide, including ten in the United States. n27 Those numbers include Najibullah Zazi, who attempted to bomb New York City's subway system in 2009, and Khalid Ouazzani, who plotted to blow up the New York Stock

Exchange. n28 Authorities further report that PRISM played an important role in tracking down David Headley, an American who aided the 2008 terrorist atrocities in Bombay, and later planned to attack the offices of a Danish newspaper that printed cartoons of Mohamed. n29 The government also claims at least one success from the telephony metadata program, though it has been coy about the specifics: "The NSA, using the business record FISA, tipped [the FBI] off that [an] individual had indirect contacts with a known terrorist overseas. . . . We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity." n30 Quite apart from foiling attacks, the government also argues that the NSA programs can conserve scarce investigative resources by helping officials quickly spot or rule out any foreign involvement in a domestic plot, as after the 2013 Boston Marathon bombing. n31

These claims have to be taken with a few grains of salt. Some observers believe that the government could have discovered the plots using standard investigative techniques, and without resorting to extraordinary methods like programmatic surveillance. n32 The metadata program has elicited special skepticism: The President's Review Group on Intelligence and Communications Technologies bluntly concluded that "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained [*530] in a timely manner using conventional section 215 orders." n33 The Privacy and Civil Liberties Oversight Board reached the same conclusion. n34 (Judicial opinion is split on the program's value. One judge has expressed "serious doubts" about its utility, n35 while another has concluded that its effectiveness "cannot be seriously disputed.") n36 Furthermore, we should always be cautious when evaluating the merits of classified intelligence initiatives on the basis of selective and piecemeal revelations, as officials might tailor the information they release in a bid to shape public opinion. n37 But even if specific claimed successes remain contested, programmatic surveillance in general can still be a useful counterterrorism technique.

As these examples imply, effective programmatic surveillance often requires huge troves of information--e.g., large databases of airline reservations, compilations of metadata concerning telephonic and internet communications, and so on. This is why it typically will not be feasible to limit bulk collection to particular, known individuals who are already suspected of being terrorists or spies. Some officials have defended the NSA programs by pointing out that, "[i]f you're looking for the needle in a haystack, you have to have the haystack." n38 That metaphor doesn't strike me as terribly helpful; rummaging around in a pile of hay is, after all, a paradigmatic image of futility. But, the idea can be expressed in a more compelling way. Programmatic surveillance cannot be done in a particularized manner. The whole point of the technique is to identify unknown threats to the national security; by definition, it cannot be restricted to threats that have already been identified. We can't limit programmatic [*531] surveillance to the next Mohamed Atta when we have no idea who the next Mohamed Atta is--and when the goal of the exercise is indeed to identify the next Mohamed Atta.

Section 702 has empirically been used to stop terrorist attacks

Young 14– President and General Counsel of Ronin Analytics, LLC. and former NSA senior leader (Mark, “National Insecurity: The Impacts of Illegal Disclosures of Classified Information”, I/S: A Journal of Law and Policy for the Information Society, 2014,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Young-Article.pdf>//DBI

The Deputy Attorney General has noted that the Federal Bureau of Investigation benefited from NSA's Section 702 collection in the fall of 2009. Using Section 702 collection and "while monitoring the activities of Al Qaeda terrorists in Pakistan, the National Security Agency (NSA) noted contact from an individual in the U.S. that the Federal Bureau of Investigation (FBI) subsequently identified as Colorado-based Najibulla Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with Al Qaeda, as well as identify any foreign or domestic terrorist links."⁴⁴

"The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi, upon indictment, pled guilty to conspiring to bomb the NYC subway system. Compelled collection (authorized under Foreign Intelligence Surveillance Act, FISA, Section 702) against foreign terrorists was critical to the discovery and disruption of this threat against the U.S."⁴⁵ Regardless of the accuracy of the information released by Snowden, the types of programs described by the material contribute to national security and its release, regardless of its validity, will negatively impact US security.

Removing section 702 means probable cause requirements would be applied to foreign investigations

Cordero, 15 - Director of National Security Studies, Georgetown University Law Center, Adjunct Professor of Law (Carrie, "The Brennan Center Report on the FISA Court and Proposals for FISA Reform" 4/2, Lawfare, <http://www.lawfareblog.com/brennan-center-report-fisa-court-and-proposals-fisa-reform>

Which brings us to the second question I posed above—what are the alternatives if Section 702 authority, were, as the Brennan Center recommends, repealed? One option is to revert to the pre-2008 practice: obtaining Court approval based on probable cause for non-U.S. persons located outside the United States. The operational result would be to forego collection on legitimate targets of foreign intelligence collection, thereby potentially losing insight on important national security threats. Given the challenging and complex national security picture the United States faces today, I would think that most responsible leaders and policymakers would say, "no thanks" to that option.

A second option would be to conduct the acquisition, but without FISC supervision. This would be a perverse outcome of the surveillance debate. It is also, probably, in the current environment, not possible as a practical matter, because an additional reason 702 was needed was to be able to serve lawful process, under a statutory framework, on communications service providers, in order to effectuate the collection.

In light of these options: collect less information pertaining to important foreign intelligence targets, or, collect it without statutory grounding (including Congressional oversight requirements) and judicial supervision, the collection framework established under 702 looks pretty good.

Link – transparency

Increasing transparency alerts terrorists of NSA tactics – increases the risk of cyberterrorism

De 14 - General Counsel, National Security Agency (Rajesh, “The NSA and Accountability in an Era of Big Data”, JOURNAL OF NATIONAL SECURITY LAW & POLICY, 2014,p.4//DM)

Perhaps the most alarming trend is that the digital communications infrastructure is increasingly also becoming the domain for foreign threat activity. In other words, it is no longer just a question of “collecting” or even “connecting” the dots in order to assess foreign threats amidst more and more digital noise, it is also a question of determining which of the so-called “dots” may constitute the threat itself. As President Obama has recognized, “the cyber threat to our nation is one of the most serious economic and national security challenges we face.”

Many of us read in the papers every day about cyber attacks on commercial entities. Hackers come in all shapes and sizes, from foreign government actors, to criminal syndicates, to lone individuals. But as former Secretary of Defense Leon Panetta warned a few months ago, “the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11.” And as the President warned in his recent State of the Union address, we know that our enemies are “seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems.” We also have seen a disturbing trend in the evolution of the cyber threat around the world. As General Keith Alexander, the Director of NSA, describes it, the trend is one from “exploitation” to “disruption” to “destruction.” In fundamental terms, the cyber threat has evolved far beyond simply stealing – the stealing of personal or proprietary information, for example-to include more disruptive activity, such as distributed denial of service attacks that may temporarily degrade websites; and more alarmingly, we now see an evolution toward truly destructive activity. Secretary Panetta, for example, recently discussed what he described as “probably the most destructive attack the private sector has seen to date” – a computer virus used to infect computers in the Saudi Arabian State Oil Company Aramco in mid-2012, which virtually destroyed 30,000 computers.

Within this context, big data presents opportunities and challenges for the government and the private sector. Improving our ability to gain insights from large and complex collections of data holds the promise of accelerating progress across a range of fields from health care to earth science to biomedical research. But perhaps nowhere are the challenges and opportunities of big data as stark as in the national security field, where the stakes are so high – both in terms of the threats we seek to defeat, and of the liberties we simultaneously seek to preserve. This reality is readily apparent in the evolving and dynamic cyber environment, and perhaps no more so than for an agency at the crossroads of the intelligence and the defense communities, like NSA.

Of course, NSA must necessarily operate in a manner that protects its sources and methods from public view. If a person being investigated by the FBI learns that his home phone is subject to a wiretap, common sense tells us that he will not use that telephone any longer. The same is true for

NSA. If our adversaries know what NSA is doing and how it is doing it – or even what NSA is not doing and why it is not doing it – they could well find ways to evade surveillance, to obscure themselves and their activities, or to manipulate anticipated action or inaction by the U.S. government. In sum, they could more readily use the ocean of big data to their advantage.

Link - PRISM

PRISM collects vast amount of data—prevents terrorism

Kelly et al, 2014 – Project director for Freedom on the Net, author and editor (“Freedom on the Net”, Freedom House, no date,

https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf//TT

Leaked documents indicated that the Foreign Intelligence Surveillance Court (FISA Court) had interpreted Section 215 of the PATRIOT Act to permit the FBI to obtain orders that compel the largest telephone carriers in the United States (Verizon, AT&T, Sprint, and presumably others) to provide the NSA with records of all phone calls made to, from, and within the country on an ongoing basis. These billions of call records include numbers dialed, length of call, and other “metadata.”⁸¹ Data are gathered in bulk, without any particularized suspicion about an individual, phone number, or device. Without approval from the FISA Court or any other judicial officer, NSA analysts conduct queries on this data, generating contact chains that show the web of connections emanating from a single phone number suspected of being associated with terrorism.⁸²

Leaks also revealed new details about programs authorized by Section 702 of the Foreign Intelligence Surveillance Act. Section 702 allows the NSA to conduct surveillance of people who are not U.S. citizens and who are reasonably believed to be located outside the United States in order to collect “foreign intelligence information.”⁸³ Under a program called “PRISM,” the NSA has been compelling at least nine large U.S. companies, including Google, Facebook, Microsoft and Apple, to disclose content and metadata relating to emails, web chats, videos, images, and documents.⁸⁴ Also under Section 702, the NSA taps into the internet backbone for “collection of communications on fiber cables and infrastructure as data flows past.”⁸⁵ Although these programs are targeted at persons abroad, the NSA is able to retain and use information “incidentally” collected about U.S. persons.

PRISM is Essential to U.S. Security in War Against Terrorism –DA Links!

Carafano ‘13 (James, Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow, “PRISM is Essential to U.S. Security in War Against Terrorism”, August 6th, 2013,
[http://www.heritage.org/research/commentary/2013/8/prism-is-essential-to-us-security-in-war-against-terrorism\)](http://www.heritage.org/research/commentary/2013/8/prism-is-essential-to-us-security-in-war-against-terrorism)

Our intelligence professionals must be able to find out who the terrorists are talking to, what they are saying, and what they're planning,” said the president. “The lives of countless Americans depend on our ability to monitor these communications.” He added that he would cancel his planned trip to Africa unless assured Congress would support the counterterrorism surveillance program. The president was not Barack Obama. It was George W. Bush, in 2008, pressing Congress to extend and update reforms to the Foreign Intelligence Surveillance Act (FISA). He was speaking directly to the American public, in an address broadcast live from the Oval Office. How times have changed. Back then, the President of the United States willingly led the fight for the programs he thought necessary to keep the nation safe. Now, our president sends underlings to make the case. In distancing himself from the debate over PRISM (the foreign intelligence surveillance program made famous by the world-travelling leaker Edward Snowden), President Obama followed the precedent he established in May at the National Defense University. There, he spoke disdainfully of drone strikes, the authorization to use military force against terrorists, and the detention facilities at Guantanamo Bay. All three are essential components of his counterterrorism strategy. In distancing himself from his own strategy, Obama hoped to leave the impression that he is somehow above it all. He has dealt with the Snowden

case the same way. When asked while traveling in Africa if he would take a role in going after the leaker, the president replied "I shouldn't have to." The White House's above-it-all attitude sends seriously mixed messages to the American people, who are trying to figure if the government's surveillance programs are legal and appropriate. Congress has not been much better. **The authority for PRISM is in FISA Section 702**. Congress debated these authorities in 2007 and again when the program was reauthorized in 2008. Senate Majority Leader Harry Reid, D-Nev., surely remembers the controversy. He wrote President Bush: "There is no crisis that should lead you to cancel your trip to Africa. But whether or not you cancel your trip, Democrats stand ready to negotiate a final bill, and we remain willing to extend existing law for as short a time or as long a time as is needed to complete work on such a bill." Evidently, Reid must have felt the authorities granted under Section 702 received a full and sufficient hearing. Most current members of Congress were seated under the dome during the 2008 debates. They had every opportunity not just to read the law, but to be briefed on the program by intelligence officials before voting on the bill. For them to act shocked at the scope of the program today rings about as hollow as Obama's expressed disdain for the operations he oversees. The reality is that Congress and the administration share responsibility for these programs. If they want to change or modify them, who's stopping them? If changes are made, however, they should to be made for the right reason. Leaders must never compromise our security for political expediency. **At least 60 Islamist-inspired terrorist plots have been aimed at the U.S. since the 9/11 attacks. The overwhelming majority have been thwarted thanks to timely, operational intelligence** about the threats. Congress should not go back to a pre-11 set of rules just to appeal to populist sentiment. Congress and the White House have an obligation to protect our liberties and to safeguard our security -- in equal measure. Meeting that mission is more important than winning popularity polls.

PRISM helped stop terrorism in US and 20-plus countries.

Mattise '13 (Nathan, New Orleans-based Staff Editor at Ars Technica, "PRISM helped stop terrorism in US and 20-plus countries", June 16th 2013, <http://arstechnica.com/tech-policy/2013/06/prism-helped-stop-terrorism-in-us-and-20-plus-countries-nsa-document-argues/>)

US intelligence **officials** sent Congress a new **declassified document** on Saturday, which the Senate Intelligence Committee then made public. Outlets such as CNN and the Associated Press received **the document** and **revealed** a number of interesting **statistics related to the government's use of the NSA's** controversial **PRISM program**. However, this document has not yet been published on the Senate Intelligence Committee's website (and does not seem to be easily obtained through basic Internet search). The new document is part of an intelligence official's effort to "show Americans the value of the program," according to the AP. The report's primary supporting stat? **Intelligence officials said that information** gleaned from these **NSA initiatives helped prevent terrorist plots in the US and more than 20 other countries**. Additionally, the release stated that phone metadata was searched for less than 300 times within the secretive database last year. The document also added details to the public's growing picture of the PRISM program. CNN reported that **the NSA** must delete these records after five years. The AP wrote that the **NSA** programs are reviewed every 90 days by a secret court authorized by the Foreign Intelligence Surveillance Act (FISA), and that the metadata records (which includes a call's time and length) can only be inspected for "suspected connections to terrorism." Despite all the public attention, the Obama Administration continues to insist that no privacy violations took place. According to White House Chief of Staff Denis McDonough (speaking Sunday on Face The Nation), the president plans to further clarify this "in the days ahead." On Friday, TechDirt also published a set of two documents described as "talking points about scooping up business records (i.e., all data on all phone calls) and on the Internet program known as PRISM." One of the talking points' main arguments is that Section 702 of the Foreign Intelligence Surveillance Act authorizes actions similar to those described above. This is despite the fact that no member of the public has ever been able to see the FISA court's ruling of the government's interpretation.

PRISM stopped 50 terrorist attacks, including assaults on the New York Stock Exchange and New York City subways.

Gerstein '13

(Josh, White House reporter for POLITICO, specializing in legal and national security issues, "PRISM stopped NYSE attack", June 18th 2013,

<http://www.politico.com/story/2013/06/nsa-leak-keithalexander-92971.html>)

Recently leaked communication surveillance programs have helped thwart more than 50 “potential terrorist events” around the world since the Sept. 11 attacks, National Security Agency Director Keith Alexander said Tuesday. Alexander said at least 10 of the attacks were set to take place in the United States, suggesting that most of the terrorism disrupted by the program had been set to occur abroad. The NSA also disclosed that counterterrorism officials targeted fewer than 300 phone numbers or other “identifiers” last year in the massive call-tracking database secretly assembled by the U.S. government. Alexander said the programs were subject to “extraordinary oversight.” “This isn’t some rogue operation that a group of guys up at NSA are running,” the spy agency’s chief added. The data on use of the call-tracking data came in a fact sheet released to reporters in connection with a public House Intelligence Committee hearing exploring the recently leaked telephone data mining program and another surveillance effort focused on Web traffic generated by foreigners. (POLITICO Junkies: NSA leaks cause flood of political problems) Alexander said 90 percent of the potential terrorist incidents were disrupted by the Web traffic program known as PRISM. He was less clear about how many incidents the call-tracking effort had helped to avert. Deputy FBI Director Sean Joyce said the Web traffic program had contributed to arrests averting a plot to bomb the New York Stock Exchange that resulted in criminal charges in 2008. Joyce also indicated that the PRISM program was essential to disrupting a plot to bomb the New York City subways in 2009. “Without the [Section] 702 tool, we would not have identified Najibullah Zazi,” Joyce said. However, President Barack Obama acknowledged in an interview aired Monday that it is impossible to know whether the subway plot might have been foiled by other methods. “We might have caught him some other way. We might have disrupted it because a New York cop saw he was suspicious. Maybe he turned out to be incompetent and the bomb didn’t go off. But at the margins we are increasing our chances of preventing a catastrophe like that through these programs,” Obama told Charlie Rose on PBS. At the hearing, Alexander detailed the scope and safeguards of the programs, while Deputy Attorney General James Cole laid out the legal basis for the surveillance. “This is not a program that’s off the books, that’s been hidden away,” Cole said of the call-tracking program, which was classified “top secret” prior to recent leaks. He noted that the Patriot Act provision found to authorize it has been twice reauthorized by Congress. “All of us in the national security [community] are constantly trying to balance protecting public safety with protecting people’s civil liberties,” Cole said. NSA Deputy Director Chris Inglis said a very limited number of individuals are authorized to access the call-tracking database.

Terrorism Links

Encrypted data makes it harder to catch terrorists

Raf Sanchez, September 25, 2014, Daily Telegraph, Tech giants slammed by FBI over encrypted smartphones;

Apple and Google's policy to encrypt their smartphones will make it more difficult to rescue kidnapping victims and foil terror plots, US says,

<http://www.telegraph.co.uk/news/worldnews/nor DOA: 3-21-15>

The FBI has warned that decisions by Apple and Google to encrypt their smartphones will make it more difficult to rescue kidnapping victims and foil terror plots. The two Silicon Valley giants have both decided to add new **encryption** systems in the face of privacy concerns sparked by Edward Snowden's disclosure of mass government **surveillance**. Both Apple and Google were criticised for allegedly handing over reams of customer data over to the National Security Agency (NSA). Now, the companies are offering encryption software as a default on smartphones, claiming it would make it impossible for them comply with US government searches. **"It's not technically feasible for us to respond to government warrants for the extraction of this data from devices," an Apple statement said.** The announcement has alarmed American law enforcement and on Thursday, James Comey, the director of the FBI, added his voice to the criticism. Mr Comey cited child kidnapping and terrorism cases as two examples of situations where quick access by authorities to phone data can save lives. He told reporters at FBI headquarters that US officials are in talks with the two companies and accused the companies of letting people put themselves beyond the law's reach. Law enforcement could still intercept telephone conversations if they had a wiretap warrant from a court. However, the new encryption systems would block access to call data, contacts, photos and email stored on the phone. Ronald **Hosko, a former assistant director of the FBI Criminal Investigative Division, said the encryption would "protect many thousands of criminals who seek to do us great harm, physically or financially".**

Encryption undermines snooping needed to stop terrorist attacks

New York Times, December 24, 2014, Why Democracy is Failing,

http://www.nytimes.com/2014/12/27/opinion/why-democracy-is-failing.html?_r=0 DOA: 3-21-15

Re "War on **surveillance**" (Turning Points, Dec. 6): Julian Assange's article on the Orwellian side of the Internet is provocative. But the remedy for electronic tyranny -- encryption -- fails to take into account modern terrorism. The encryption that would justifiably limit official snooping would equally frustrate the equally justifiable attempt to short-circuit terrorist plots. One could argue about the relative importance of the two imperatives, but not about the two-faced character of all aspects of Internet surveillance.

Encryption makes information needed to prevent and prosecute crimes unavailable

Bloomberg, October 2, 2014, Apple's encryption will slow not stop snooping by cops and spies, <http://www.bloomberg.com/news/articles/2014-10-02/apple-s-encryption-will-slow-not-stop-cops-and-spies> DOA: 3-20-15

The companies announced in recent weeks that their new phones will automatically scramble data so that a digital key kept by the owner is needed to unlock it, making it harder for detectives to examine the content of suspects' phones without their knowledge or cooperation. Previously, such encryption was an option that required users to endure a time-consuming process to activate. "This is going to have a very big impact on law enforcement," said Stewart Baker, a former general counsel for the NSA and now a partner at the law firm Steptoe and Johnson in Washington. "There will be crimes that people get away with because this information is not available."

Encryption decimates effective law enforcement. The impact is rampant terrorism and crime.

Glasser 14 — Ellen Glasser, President of the Society of Former Special Agents of the Federal Bureau of Investigation, Adjunct Professor in the Criminology & Criminal Justice Department at the University of North Florida, served as an FBI Agent for 24 years, 2014 ("Tech companies are making it harder for the nation's law enforcement," *The Baltimore Sun*, November 6th, Available Online at <http://www.baltimoresun.com/news/opinion/oped/bs-ed-fbi-apple-20141106-story.html>, Accessed 07-05-2015)

FBI Director Comey has been on the job for just over a year and is working to change perceptions. In addressing the myriad challenges that face our nation, he brings a positive, reasoned approach to the public discussion of privacy versus safety. While appreciating the public's concern over privacy, he has been very clear that the marketing of these new devices will seriously impede law enforcement's ability to protect Americans. Put simply, legal access to unencrypted mobile device information is needed to keep our citizens and our country safer.

Here is some FBI reality. We live in an apocalyptic, post-9/11 world, where the FBI is confronted with a dizzying array of threats from terrorist bombings to beheadings of innocent victims. Over the years, the FBI has also responded to anthrax attacks, shoe and underwear bombers, White House fence jumpers, child molesters, school shootings, human trafficking, kidnappings and massive fraud schemes. The FBI investigates these matters within the scope of the law and with great, abiding respect for the right of individuals to privacy.

Let me bring this close to home. What if your child was abducted, and the FBI developed mobile device information and had a court order, but FBI agents were unable to access the critical, time-sensitive, unencrypted information that was necessary to save your child's life? Thankfully, most people will never be in a life-or-death situation like this, but it does happen. When it does — any FBI agent can tell you from experience — people want help. Let's start by helping them now.

Public perception needs to change so the focus is on handcuffing the bad guys, not tying the hands of the good guys. Please contact your elected representatives to tell them that corrective legislation is necessary to require companies like Apple and Google to work with law enforcement and find a solution to this problem.

Law enforcement can't break strong encryption. ISIS loves this.

Wittes 15 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2015 (“Thoughts on Encryption and Going Dark: Part I,” *Lawfare*—a national security blog curated by the Brookings Institution, July 9th, Available Online at <http://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-i>, Accessed 07-13-2015)

FBI Director James Comey has been on a public offensive of late, arguing against end-to-end encryption that prevents law enforcement access to communications even when authorities have appropriate legal process to capture those communications. The offensive began with a speech at Brookings some months ago. More recently, Comey made these comments on CNN, these comments in a private conversation with me, and wrote this piece for Lawfare.

Yesterday, he was on Capitol Hill, testifying both before the Senate Judiciary Committee (video at this link, prepared statement here) and before the Senate Select Committee on Intelligence (video below):

[Video Omitted]

Comey made some news yesterday. For one thing, he stated very clearly to the Judiciary Committee—and with evident reluctance—that some of the encryption the bureau is now facing is beyond its capacity to crack:

[I]f we intercept data in motion between two encrypted devices or across an encrypted mobile messaging app and it's strongly encrypted, we can't break it.

Now, this is sometimes—I hate that I'm here saying this, but I actually think the problem is severe enough that I need to let the bad guys know that. That's the risk in what we're talking about here. The bad—I'm just confirming something for the bad guys.

Sometimes people watch TV and think, "Well, the FBI must have some way to break that strong encryption." We do not, which is why this is **such an important issue**.

At another point, he stated that while some companies have designed systems that they lack the capacity to decrypt, in other instances, some companies have simply declined to assist investigators in decrypting signal even where decryption was possible—a matter on which at least one senator fought further information. (See Comey's comments at 1:17:00 and his subsequent exchange with Senator Sheldon Whitehouse at 1:20:00 of the Judiciary Committee hearing.)

All in all, Comey's reception on the Hill was significantly warmer than I expected. The Bureau has clearly done a lot of quiet behind-the-scenes work with members to familiarize them with the problem as the FBI sees it, and many members yesterday seemed to require little persuasion.

But Comey has a very heavy lift ahead of him if he is to make progress on the "Going Dark" problem. For one thing, it's not entirely clear what constitutes progress from the Bureau's

perspective. The administration is, at this stage, not asking for legislation, after all. It's merely describing an emergent problem.

But this is a bit of a feint. The core of that emergent problem, at least as Comey's joint statement with Deputy Attorney General Sally Yates frames it, is that CALEA—which mandates that telecommunications providers retain the capacity for law enforcement to get access to signal for lawful wiretapping—does not reach internet companies. So even if Apple and Google were to voluntarily retain encryption keys, some other actor would very likely not do so. Absent a legal requirement that companies refrain from making true end-to-end encrypted services available without a CALEA-like stop-gap, some entity will see a market hole and provide those services. And it's fair to assume that ISIS and the most sophisticated bad actors will gravitate in the direction of that service provider.

In other words, I think Comey and Yates inevitably are asking for legislation, at least in the longer term. The administration has decided not to seek it now, so the conversation is taking place at a somewhat higher level of abstraction than it would if there were a specific legislative proposal on the table. But the current discussion should be understood as an effort to begin building a legislative coalition for some sort of mandate that internet platform companies retain (or build) the ability to permit, with appropriate legal process, the capture and delivery to law enforcement and intelligence authorities of decrypted versions of the signals they carry.

The plan risks catastrophic terrorism.

Weissmann 14 — Andrew Weissmann, Senior Fellow at the Center for Law and Security and the Center on the Administration of Criminal Law at New York University, former General Counsel for the Federal Bureau of Investigation, holds a J.D. from Columbia Law School, 2014 (“Apple, Boyd, and Going Dark,” *Just Security*, October 20th, Available Online at <http://justsecurity.org/16592/apple-boyd-dark/>, Accessed 07-05-2015)

To my mind – although, as in many areas of the law, there is no perfect solution — the cost of a system where we may be more at risk to illegal hacking is outweighed by the vital role lawful electronic interception plays in thwarting crime – including devastating terrorist attacks. Law enforcement and intelligence officials, including most recently FBI Director James Comey, have noted that we all – including criminals – increasingly use non-telephonic means to communicate. The ability to monitor electronic communications is decreasing with every new encryption tool on such communication systems. Law enforcement authorities in the US and overseas rightfully note how such data is critical to solving everyday crimes, such as kidnapping, fraud, child pornography and exploitation, among many others. And at least as important, preventing terrorist attacks requires such ability, as intelligence agencies note (although due to the Snowden leaks, resulting in the public perception that the intelligence community has too much, not too little, access to information, the ramifications from encryption on traditional law enforcement is likely to be relied on by the government in the public debate on this issue).

This is a judgment Congress needs to make, and soon. In weighing the interests, however, it is no answer to say that the government should revert to means other than lawful intercepts obtained through court orders based on probable cause to prevent crimes. The reality of electronic communications is here to stay and plays a vital role in how crimes are perpetrated by allowing

people to communicate with conspirators and to carry out their nefarious plans. In this regard, the government and privacy advocates both need to be consistent in their arguments: it is the latter who usually remind us that the advent of smartphones and “big data” makes traditional Fourth Amendment line-drawing obsolete. And they have a point, as the Supreme Court is starting to recognize. But by the same token, it is increasingly important to have an ability to monitor such communications, after meeting the necessary Fourth Amendment standard upon a showing to an independent Article III court.

The plan substantially increases the risk of catastrophic *crime and terrorism*.

Rubin 14 — Jennifer Rubin, Columnist and Blogger for the *Washington Post*, holds a J.D. from the University of California-Berkeley, 2014 (“Silicon Valley enables terrorists and criminals,” *Right Turn*—a *Washington Post* blog, October 19th, Available Online at <http://www.washingtonpost.com/blogs/right-turn/wp/2014/10/19/silicon-valley-enables-terrorists-and-criminals/>, Accessed 07-05-2015)

Google chairman Eric Schmidt likes to brag that his company is “on the right side of history.” He pats himself on the back for pulling out of China because of that country’s censoring practices. His company even has a slogan, “Don’t be evil,” meant to remind Google employees that they aspire to the highest ethical standards. But, to be blunt, Google is violating its own “don’t be evil” rule by insisting on encryption technology which locks out anti-terrorist and law enforcement agencies. That gives terrorists and common criminals alike huge protection and puts their fellow Americans at risk.

Benjamin Witten of the Brookings Institution explains this is not about “encryption,” as some reports characterize it. No one is talking about eliminating encryption, he explains, “Without it, you couldn’t have electronic commerce. Nobody wants to get rid of encryption.” He explains, “The only question is whether there should be government access with lawful process — or not.”

In a scantily covered speech this week, FBI Director James Comey explained:

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren’t seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple’s new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple’s announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won’t be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

That is a problem that is not solved, as Apple claims, by providing access to the cloud. "But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement," Comey said. "And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data."

In fact, the blocked phones are simply part of a marketing pitch to cater to young people who are misinformed and paranoid about what information the government has access to. Comey observed that "it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?"

Well, some terrorists will use it to plan and execute murderous schemes, organized crime will use it to hide from law enforcement and the American people will be less safe and less secure.

Maybe the president (whose party benefits from liberal high-tech donors) should call these people in for a chat and explain why they should stop this. Alternatively, Congress should hold open hearings and have these execs explain why they want to give terrorists an e-hideout. Then again, maybe concerned Americans who want to combat terrorists should simply not use these products. (Hang onto your old phone until they drop the "locked safe," for example.) What President Obama, Congress and the American people should not do is sit idly by while they put us at risk for pecuniary gain.

Comey went out of his way to be nice to these companies: "Both companies are run by good people, responding to what they perceive is a market demand." Too nice, in my mind. Instead he should have just told them flat out, "Don't be evil."

Especially true of ISIS.

AP 15 — Associated Press, 2015 ("US Officials: Encryption Hinders Monitoring Extremists," Byline Eric Tucker, June 4th, Available Online at <http://www.forensicmag.com/news/2015/06/us-officials-encryption-hinders-monitoring-extremists>, Accessed 07-06-2015)

The growing use of encrypted communications and private messaging by supporters of the Islamic State group is complicating efforts to monitor terror suspects and extremists, U.S. law enforcement officials said Wednesday.

Appearing before the House Homeland Security Committee, the officials said that even as thousands of Islamic State group followers around the world share public communications on Twitter, some are exploiting social media platforms that allow them to shield their messages from law enforcement.

"There are 200-plus social media companies. Some of these companies build their business model around end-to-end encryption," said Michael Steinbach, head of the FBI's counterterrorism division. "There is no ability currently for us to see that" communication, he said.

Encryption helps terrorists — Zazi proves.

Crovitz 14 — L. Gordon Crovitz, Columnist and Former Publisher of *The Wall Street Journal*, former Executive Vice-President of Dow Jones, 2014 (“Terrorists Get a Phone Upgrade,” *Wall Street Journal*, November 23rd, Available Online at <http://www.wsj.com/articles/gordon-crovitz-terrorists-get-a-phone-upgrade-1416780266>, Accessed 07-20-2015)

It's a good thing Najibullah Zazi didn't have access to a modern iPhone or Android device a few years ago when he plotted to blow up New York City subway stations. He was caught because his email was tapped by intelligence agencies—a practice that Silicon Valley firms recently decided the U.S. government is no longer permitted.

Apple, Google, Facebook and others are playing with fire, or in the case of Zazi with a plot to blow up subway stations under Grand Central and Times Square on Sept. 11, 2009. An Afghanistan native living in the U.S., Zazi became a suspect when he used his unencrypted Yahoo email account to double-check with his al Qaeda handler in Pakistan about the precise chemical mix to complete his bombs. Zazi and his collaborators, identified through phone records, were arrested shortly after he sent an email announcing the imminent attacks: “The marriage is ready.”

The Zazi example (he pleaded guilty to conspiracy charges and awaits sentencing) highlights the risks that Silicon Valley firms are taking with their reputations by making it impossible for intelligence agencies or law enforcement to gain access to these communications. In September, marketers from Apple bragged of changes to its operating system so that it will not comply with judicial orders in national-security or criminal investigations.

“Unlike our competitors,” Apple announced, “it’s not technically feasible for us to respond to government warrants.” This encryption was quickly matched by Google and the WhatsApp messaging service owned by Facebook.

In a private meeting last month, Deputy Attorney General James Cole asked the general counsel of Apple why the company would want to market to criminals. As the Journal reported last week, Mr. Cole gave the hypothetical of the police announcing that they would have been able to rescue a murdered child if only they could have had access to the killer’s mobile device. Apple’s response was that the U.S. can always pass a law requiring companies to provide a way to gain access to communications under court orders.

Since then, U.S. and British officials have made numerous trips to Silicon Valley to explain the dangers. FBI Director James Comey gave a speech citing the case of a sex offender who lured a 12-year-old boy in Louisiana in 2010 using text messages, which were later obtained to get a murder conviction. “There should be no one in the U.S. above the law,” Mr. Comey said, “and also no places within the U.S. that are beyond the law.”

Robert Hannigan, the head of Britain’s electronic-intelligence agency, Government Communications Headquarters, warned in a Financial Times op-ed earlier this month: “However much they may dislike it,” Silicon Valley firms “have become the command-and-control networks of choice for terrorists and criminals.”

Even without terrorism attacks that could have been prevented, Mr. Hannigan said, he thought Internet users may be “ahead” of Silicon Valley: “They do not want the media platforms they use with their friends and families to facilitate murder or child abuse.”

It looks like Silicon Valley has misread public opinion. The initial media frenzy caused by the Edward Snowden leaks has been replaced by recognition that the National Security Agency is among the most lawyered agencies in the government. Contrary to initial media reports, the NSA does not listen willy-nilly to phone and email communications.

Last week, the Senate killed a bill once considered a sure thing. The bill would have created new barriers to the NSA obtaining phone metadata to connect the dots to identify terrorists and prevent their attacks. Phone companies, not the NSA, would have retained these records. There would have been greater risks of leaks of individual records. An unconstitutional privacy advocate would have been inserted into Foreign Intelligence Surveillance Court proceedings.

The lesson of the Snowden accusations is that citizens in a democracy make reasonable trade-offs between privacy and security once they have all the facts. As people realized that the rules-bound NSA poses little to no risk to their privacy, there was no reason to hamstring its operations.
Likewise, law-abiding people know that there is little to no risk to their privacy when communications companies comply with U.S. court orders.

Finding no willingness by Silicon Valley to rethink its approach without being required by law, FBI Director Comey recently asked Congress to update the Communications Assistance for Law Enforcement Act of 1994. This requires traditional phone companies to comply with court orders to provide access to records. He wants the law updated to cover Apple, Google and other digital companies.

Silicon Valley firms should find ways to comply with U.S. court orders or expect Congress to order them to do so. They also shouldn't be surprised if their customers think less of companies that go out of their way to market technical solutions to terrorists and criminals.

Strong encryption greatly increases chance of successful terror attack

RT 15 (RT, “Apple, Google helping terrorists with encryption- Manhattan DA” 04/21/15, <http://www.rt.com/usa/251469-apple-google-encryption-terrorists/>)

Allowing users to take advantage of advanced encryption in order to keep their messages and mobile communication out of the government's hands will only help terrorists plot future attacks, a top New York law enforcement official said. The new encryption services offered by Apple and Google will make it harder to protect New Yorkers, Manhattan District Attorney Cyrus Vance Jr. told local AM970 radio host John Cats. He mentioned built-in encryption – which Apple claims its own engineers cannot break – means that federal and local law enforcement bodies won't be able to intercept communications between potential criminals and terrorists, even if they acquire a warrant. When Cats suggested, “terrorists are running out to buy iPhones,” Vance responded by saying, he was “absolutely right.” If individuals who are seeking to do serious harm to our citizenry know they have a device that they can use with impunity and that the contents of their messages and images on their phones cannot be accessed by law enforcement that's going to be the terrorists' community device of choice. he added, according to the Daily Dot. In addition to Apple, Google is also incorporating encryption into its mobile devices. The two tech giants’ smartphones comprise 96 percent of the global market, the New York Post mentions. Apple has created a phone that is dark, that cannot be accessed by law enforcement even when a court has authorized us to look at its contents,” Vance said. In response, Vance wants police departments around the country to register their opposition with politicians and for hearings on the issue to take place. On its website, Apple says that encryption is enabled “end-to-end” on its devices and that it has “no way to decrypt iMessage and FaceTime data when it's in transit between devices.” Additionally, the company states, We wouldn't be able to comply with a wiretap order even if we wanted to. Other features such as iCloud and Mail also offer some encryption protections. READ MORE: FBI director lashes out at Apple, Google for encrypting smartphones Vance isn't the only law enforcement official to come out against widespread encryption. In October, New York Police Department Commissioner Bill Bratton heavily criticized Apple and Google for

the move, and FBI Director James Comey also blasted the development. "There will come a day -- well it comes every day in this business -- when it will matter a great, great deal to the lives of people of all kinds that we be able to with judicial authorization gain access to a kidnapper's or a terrorist or a criminal's device," Comey said. "I just want to make sure we have a good conversation in this country before that day comes." In a blog post at the Wall Street Journal, Amy Hess of the FBI clarified the bureau's position on the issue, which has seen a surge in support since former government contractor Edward Snowden revealed a massive domestic and international surveillance operation. She said law enforcement officials will need "some degree of access" to encrypted messages in order to stop criminal and violent plots in the future. "No one in this country should be beyond the law," she wrote. "The notion that electronic devices and communications could never be unlocked or unencrypted – even when a judge has decided that the public interest requires accessing this data to find evidence — is troubling. It may be time to ask: Is that a cost we, as a society, are prepared to pay?"

Encryption decks counter-terror effectiveness

Hess 15 (Amy Hess, Executive Assistant Director Federal Bureau of Investigation, Before the Subcommittee on Information Technology Oversight and Government Reform U.S. House of Representatives Concerning Encryption and Cybersecurity for Mobile Electronic Communication Devices, page 6-7, April 29, 2015.)\\mwang

Examples

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that evidence that was once found in filing cabinets, letters, and photo albums will now be available only in electronic storage. We have seen case after case – from **homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation** – where critical evidence came from smart phones, computers, and online communications. Each of the following examples demonstrates how important information stored on electronic devices can be to prosecuting criminals and stopping crime. As encryption solutions become increasingly inaccessible for law enforcement, it is cases like these that could go unsolved, and criminals like these that could go free. Another investigation in Clark County, Nevada, centered on allegations that a woman and her boyfriend conspired together to kill the woman's father who died after being stabbed approximately 30 times. Text messages which had been deleted from the phone and recovered by investigators revealed the couple's plans in detail, clearly showing premeditation. Additionally, the communications around the time of the killing proved that both of them were involved throughout the process and during the entire event, resulting in both being charged with murder and conspiracy to commit murder. Following a joint investigation conducted by the FBI and Indiana State Police, a pastor pleaded guilty in Federal court to transporting a minor across state lines with intent to engage in illicit sexual conduct in connection with his sexual relationship with an underage girl who was a student at the church's high school. During this investigation, information recovered from the pastor's smart phone proved to be crucial in showing the actions taken by the pastor in the commission of his crimes. Using forensic software, investigators identified Wi-Fi locations, dates, and times when the pastor traveled out of state to be with the victim. The analysis uncovered Internet searches including, "What is the legal age of consent in Indiana", "What is the legal age of consent in Michigan", and "Penalty for sexting Indiana." In addition, image files were located which depicted him in compromising positions with the victim. These are examples of how important evidence that resides on smart phones and other devices can be to law enforcement – evidence that might not have been available to us had strong encryption been in place on those devices and the user's consent not granted. The above examples serve to show how critical electronic evidence has become in the course of our investigations and how timely, reliable access to it is imperative to ensuring public safety. Today's encryption methods are increasingly more

sophisticated, and pose an even greater challenge to law enforcement. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop – evidence that may be the difference between an offender being convicted or acquitted – **but we cannot access it.** Previously, a company that manufactured a communications device could assist law enforcement in unlocking the device. Today, however, upon receipt of a lawful court order, the company might only be able to provide information that was backed up in the cloud – **and there is no guarantee such a backup exists, that the data is current, or that it would be relevant to the investigation.** **If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.**

Encryption is getting stronger—cloaks terrorists.

Hess 15 (Amy Hess, Executive Assistant Director Federal Bureau of Investigation, Before the Subcommittee on Information Technology Oversight and Government Reform U.S. House of Representatives Concerning Encryption and Cybersecurity for Mobile Electronic Communication Devices, page 4-5, April 29, 2015.)\mwang

Court-Ordered Access to Stored Encrypted Data Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks. In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default – without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice. Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection. Additional Considerations Some assert that although more and more devices are encrypted, users back-up and store much of their data in “the cloud,” and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many companies impose fees to store information there – fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves – devices which are increasingly encrypted.

Strong encryption facilitates terrorist recruitments and plots

Ybarra 15 (Maggie Ybarra, military affairs and Pentagon correspondent for the Washington Times, Washington Times, “FBI director James Comey flags dangers of encryption services, 07/7/15, <http://www.washingtontimes.com/news/2015/jul/7/fbi-encryption-fosters-furtive-terrorism/>)

FBI Director James B. Comey will be arguing for a robust debate on message-encryption technology to lawmakers Wednesday, as he takes to Capitol Hill to plead his case that terrorist groups such as the Islamic State could take advantage of such technology to recruit Americans into their organization. The technology, commonly referred to as “going dark” allows people to send messages to one another that cannot be traced by the government. Google has reported about 80 percent of its Gmail messages to other addresses in the last month were encrypted, and Apple has said it uses encryption on its iMessage and FaceTime tools which is so secure that even the company can’t read or decode the communications. But for all the good encryption services provide — protecting innovation, private thoughts and other things of value — the technology can also be used for nefarious purposes, Mr. Comey wrote in a blog posting Monday. “There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption,” Mr. Comey wrote. The Senate Judiciary Committee is prepared to hear Mr. Comey’s testimony about the technology, along with the testimony of Sally Quillian Yates, the deputy attorney general at the Department of Justice. “Today’s hearing is intended to start a conversation in the Senate about whether recent technological changes have upset the balance between public safety and privacy.” Sen. Chuck Grassley, Iowa Republican and the panel, said in prepared remarks. “In particular, Director Comey has talked about the challenges this issue presents the FBI in the national security context. According to the Director, ISIS is recruiting Americans on-line and then directing them to encrypted communication platforms that are beyond the FBI’s ability to monitor, even with a court order. If this is accurate, it obviously represents a dangerous state of affairs.” Despite the danger, a group of computer scientists and security experts are trying to counter Mr. Comey’s message by defending the need for encrypted technology. The same day that FBI director made a rare social media effort to flag the dangers of “going dark,” the Computer Science and Artificial Intelligence Laboratory released a 34-page technical report that advocates against providing federal authorities access to encrypted conversations. “We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago,” the report states. “In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution.” President Obama has been trying to ease the concerns of Mr. Comey and the other heads of U.S. government intelligence agencies by searching for a middle ground solution that protects the privacy of U.S. citizens while providing federal agencies with the tools they need to track down and halt potential terrorist threats. Mr. Obama said during a joint January press conference with British Prime Minister David Cameron that his administration has been communicating with companies about how to provide agencies with legal access to conversations that might be taking place via technologies that are constantly evolving. “If we get into a situation in which the technologies do not allow us at all to track somebody that we’re confident is a terrorist, if we … have specific information, we are confident that this individual or this network is about to activate a plot and, despite knowing that information, despite having a phone number or despite having a social media address or a e-mail address, that we can’t penetrate that, that’s a problem,” he said. The solution to that problem will likely be complicated and involve consideration of legislation, regulation, cooperation among lawmakers and with private companies, Mr. Comey said during a June 18 press conference at the Department of Justice. “The companies that are providing communication services don’t want folks killed by people using their platforms,” he said. “So we’re having good conversations with them. I’m sure a big part of it’s going to be international cooperation.”

Backdoor searches protect privacy and are key to law enforcement

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.2-3, <http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy> //wx

As you know, the Fourth Amendment of the United States Constitution authorizes reasonable searches and seizures, providing law enforcement agencies access to places where criminals hide evidence of their crimes – from car trunks, to storage facilities, to computers, mobile devices, and digital networks. In order to safeguard Fourth Amendment rights, these searches are conducted pursuant to judicial warrants, issued upon a neutral judge's finding of probable cause. The probable cause standard represents a balance between privacy and public safety carefully calibrated by centuries of jurisprudence, and it guides individuals and companies in developing their expectations of privacy. Through this judicial process, my Office obtains smartphone evidence to support all types of cases – homicides, sex crimes, child abuse, fraud, assaults, robberies, cybercrime, and identity theft. Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on computers and smartphones. Between October 2014 and June 2015, 35 percent of the data extracted from all phones by my Office was collected from Apple devices; 36 percent was collected from Android devices.² That means that when smartphone encryption is fully deployed by Apple and Google, 71 percent of all mobile devices examined – at least by my Office's lab – may be outside the reach of a search warrant. I want to emphasize I am testifying from a state and local perspective. I am not advocating bulk data collection or unauthorized surveillance. Instead, I am concerned about protecting local law enforcement's ability to conduct targeted requests for information, scrutinized by an impartial judge for his or her evaluation as to whether probable cause has been established. Importantly, and by Apple's own admission, governmental request for information have affected only .00571 percent of Apple's customers.

Strong encryption decks law enforcement abilities – can't obtain any data

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.3-5, <http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf>>//wx

Last fall, Apple and Google, whose operating systems run 96 percent of smartphones worldwide, announced with some fanfare, but without notice to my Office or other law enforcement offices I have spoken to, that they had engineered their new mobile operating systems such that they can no longer assist law enforcement with search warrants written for passcode- protected smartphones. According to Apple's website: On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode... Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess. [Emphasis added.]⁵ Apple's announcement led to an immediate response by law enforcement officials who pointed out that allowing a phone or tablet to be locked such that it would be beyond the reach of lawful searches and seizures was unprecedented and posed a threat to law enforcement efforts – in effect, a boon to criminals. Unless law enforcement officials can obtain the passcode from the user, which will be difficult or impossible in many cases, or can use “brute force” to obtain the passcode (again, difficult or impossible, and attempts to do this would likely lead to the destruction of evidence on the iPhone), the search warrant would be of no consequence, because no one will be able to unlock the phone, notwithstanding the court order. Law enforcement's warnings are hardly idle. Recently, a father of six was murdered in Evanston, Illinois. City of Evanston Police believe that prior to his murder, the victim was robbed of a large sum of money. There were no eyewitnesses to or surveillance footage of the killing. Found alongside the body of the deceased were an iPhone 6 and a Samsung Galaxy S6 Edge running Google Android. Cook County prosecutors served Apple and Google with judicial warrants to unlock the phones, believing that relevant evidence might be stored on them. Apple and Google replied, in substance, that they could not, because they did not know the user's passcode. Information that might be crucial to solving the murder, therefore, had effectively died with the victim. His homicide remains unsolved. His killer remains at large. It is not hyperbole to say that beginning in September 2014, Americans conceded a measure of their protection against everyday crimes to Apple and Google's new encryption policies. Yet, I would note that, before the changes, neither company, to our knowledge, ever

suggested that their encryption keys, held by the companies, were vulnerable to hacking or theft. Fully one-quarter of our felony cases now involve cybercrime or identity theft, so I am keenly aware of the dangers and impact of these crimes on our community (which happens to be situated in a world financial center and is the number one target for terrorism in the world). Because of this, my Office has invested heavily in becoming highly proficient and active in the prosecution of these crimes, and in the promotion of best cybersecurity practices for New York consumers and companies. From my vantage point, and in my opinion, for reasons set forth later in my testimony, Apple and Google's new encryption policies seem to increase protection for consumers from hackers only minimally, if at all. But those policies create serious new risks for my constituents and the millions of visitors and workers passing through Manhattan every day.

Access to smartphone data is key to law enforcement – numerous cases prove

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy", p.3-5, <http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf>>//wx

The Cost of Evidence Made Inaccessible Through Apple's Encryption Although encryption has been often discussed in the context of international terrorism, the NSA, and the CIA, the greatest cost of these new encryption policies may well be borne by local law enforcement. Smartphones are ubiquitous, and there is almost no kind of case in which prosecutors have not used evidence from smartphones. My Office (and, I expect, every other local prosecutor's office) has used evidence from cellphones in homicides, rape cases, human trafficking, assaults, domestic violence cases, narcotics cases, kidnappings, larcenies, frauds, identity theft, cybercrime, and robberies. Indeed, it is the rare case in which information from a smartphone is not useful. The following list of recent cases is representative: • Homicide: People v. Hayes, Indictment Number 4451/12: The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life. • Sex Trafficking: People v. Brown, Indictment Numbers 865/12, 3908/12, and 3338/13: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices lawfully seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's cellular phones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his 14 nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison. • Cybercrime and Identity Theft: People v. Jacas et al., Indictment Number 42/12 and People v. Brahms et al., Indictment Number 5151/11: This case involved the successful prosecution of a 29-member identity theft ring, which was able to be investigated and prosecuted, in large part, because of evidence obtained early in the investigation from an iPhone, pursuant to a search warrant. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was lawfully searched, law enforcement officials discovered text messages between members of the group regarding the ring's crimes. Investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole property worth over \$1,000,000. All of the defendants pleaded guilty, and more than \$1,000,000 in cash and merchandise were seized and forfeited. • Sex Offenses: United States v. Juarez, Case No. 12-CR-59: The defendant was arrested for unlawful surveillance by an NYPD officer after the officer observed the defendant using a cell phone to film up women's skirts. My Office obtained a search warrant for the phone. During the subsequent search of the phone's micro SD card, forensic analysts discovered a series of images, taken by the defendant, showing a seven-year-old girl lying down on a bed and an adult man pushing aside her underwear, revealing her genitals. The case was referred to the United States Attorney's Office for the Eastern District of New York, which charged the defendant with producing child pornography. • Physical and Sexual Abuse of a Child: U.S. v. Patricia and Matthew Ayers, Case No. 5:14 CR 0117 LSC SGC: In case after case, law enforcement has been able to discover and prosecute child abuse by using video or photographic evidence taken by the abuser. This case is illustrative: From 2010 to 2013, the defendants abused and exploited a young child in their care who, during that period, was six to nine years old. The couple took photographs of the child in lewd poses, as well as of each other engaged in sexual acts with the child. The defendants recorded the abuse with their smartphones and downloaded the images to a computer. In at least one instance, one of the defendants transmitted images to another individual, indicating that she would travel interstate with the child

to the individual's home so the individual could also have sexual relations with the child. The federal judge overseeing the case described it as the worst case he has personally dealt with, including murders, in his 16 years on the bench. The defendants were ultimately convicted of producing child pornography, in violation of 18 U.S.C. § 2251(a), and were sentenced to 1,590 and 750 years, respectively, in federal prison. There are many other cases—almost too many to count—that I might have selected, but the point is clear: We would risk losing crucial evidence in all of these cases if the contents of passcode-protected smartphones were unavailable to us, even with a warrant. 16 The enormity of the loss is fully appreciated by wrongdoers who use smartphones. Recently, a defendant in a serious felony case told another individual on recorded jailhouse call that “Apple and Google came out with these softwares that can no longer be encrypted [sic: decrypted] by the police. . . If our phones is running on the iO[S]8 software, they can’t open my phone. That might be another gift from God.” This defendant’s appreciation of the safety that the iOS 8 operating system afforded him, is surely shared by criminal defendants in every jurisdiction in America charged with all manner of crimes, including rape, kidnapping, robbery, promotion of child pornography, larceny, and presumably by those interested in committing acts of terrorism. Criminal defendants across the nation are the principal beneficiaries of iOS 8, and the safety of all American communities is imperiled by it.

Data on encrypted devices is crucial to law enforcement and counterterrorism

Yates and Comey 7/8 <Sally Quillian Yates, Deputy Attorney General, and James B. Comey, Director of the FBI, 7/8/2015, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.3-4, <http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf>>//wx

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications. When changes in technology hinder law enforcement’s ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence. These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole. Of course, encryption is not the only technology terrorists and criminals use to further their ends.

Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from State to State and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that - 4 - phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker. In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully-authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other

types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders. Legal Framework

Encryption blocks successful investigation – Investigators locked out

Ellen Nakashima and Barton Gellman '15 (Ellen Nakashima is a national security reporter for The Washington Post. Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post. He is a senior fellow at the Century Foundation and visiting lecturer at Princeton's Woodrow Wilson School.

https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html)CK

Bitkower cited a case in Miami in December in which a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from state to state and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. His defense, Bitkower said, was that she engaged in consensual sex. As it turned out, the trucker had video-recorded his assault, and the phone did not have device encryption enabled. Law enforcement agents were able to get a warrant and retrieve the video. It "revealed in quite disturbing fashion that this was not consensual," Bitkower said. The jury convicted the trucker. Officials and former agents say there will be cases in which crimes will go unsolved because the data was unattainable because only the phone owner held the key. "I just look at the number of cases I had where, if the bad guy was using one of these [locked] devices, we never would have caught him," said Timothy P. Ryan, a former FBI supervisory special agent who now leads Kroll Associates' cyber-investigations practice.

Encryption decks efforts to combat ISIS- online recruiting

Clare Hopping 7/8/15--Freelance editor and journalist as well as editorial editor for Longneck and Thunderfoot. Cites FBI. (Hopping, "FBI director complains encryption makes his job harder", ITpro. <http://www.itpro.co.uk/security/24943/fbi-encryption-helps-isis-recruit-new-members.//ET>)

Universal encryption will help terrorists spread their creeds through secure messaging services, according to the FBI. James Comey, director of the agency, claimed in a blog post that worldwide encryption will help groups like ISIS ahead of his appearance at the Senate Intelligence Committee. He wrote that secure messaging services and social media will help ISIS recruit new members online. "When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public safety." he wrote on pro surveillance website Lawfare. "That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment."

Backdoors would allow criminals to bypass encryption

Phys.org 15 ("Security experts warn against encryption 'backdoors'", 7/7/15, <http://phys.org/news/2015-07-experts-encryption-backdoors.html>)

A group of computer code experts said Tuesday that law enforcement cannot be given special access to encrypted communications without opening the door to "malicious" actors. A research report published by the Massachusetts Institute of Technology challenges claims from US and British authorities that such access is the policy response needed to fight crime and terrorism. Providing this kind of access "will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend," said the report by 13 scientists. The paper was released a day after FBI Director James Comey called for public debate on the use of encrypted communications, saying Americans may not realize how radical groups and criminals are using the technology. Comey argued in a blog post that Islamic State militants are among those using encryption to avoid detection. The New York Times, which reported earlier on the study, said Comey was expected to renew a call at a congressional hearing for better access to encrypted communications to avoid "going dark." The computer scientists said, however, that any effort to build in access for law enforcement could be exceedingly complex and lead to "unintended consequences," such as stifling innovation and creating hostility toward new tech products. "The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict," the report said. "The costs to developed countries' soft power and to our moral authority would also be considerable." In the 1990s, there was a similar debate on the "clipper chip" proposal to allow "a trusted third party" to have access to encrypted messages that could be granted under a legal process. The clipper chip idea was abandoned, but the authors said that if it had been widely adopted, "it is doubtful that companies like Facebook and Twitter would even exist." The computer scientists said the idea of special access would create numerous technical and legal challenges, leaving unclear who would have access and who would set standards.

NSA decryption is vital to counterterrorism – international consensus

Robertson 13 (Adi Robertson, tech policy correspondent for The Verge, "Intelligence chief says the US attacks encryption because the bad guys use it", 10/4/13, <http://www.theverge.com/2013/10/4/4803646/james-clapper-justifies-tor-breaking-as-necessary-to-fight-terrorists>) -LL

Director of National Intelligence James Clapper has responded to leaks showing how the NSA tried (and largely failed) to break through Tor's encryption network. While his statement doesn't shed much new light on the situation, it encapsulates the intelligence community's general response to criticism since the first leaks were published: that the threat of terrorism or other threats to national security makes any arguably legal tactic not only ethical, but vital. Recently published news articles discuss the intelligence community's interest in tools used to facilitate anonymous online communication. The articles accurately point out that the intelligence community seeks to understand how these tools work and the kind of information being concealed. However, the articles fail to make clear that the intelligence community's interest in online anonymity services and other online communication and networking tools is based on the undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies. Clapper accuses the articles' authors (unnamed, but likely journalist Glenn Greenwald and security expert Bruce Schneier) of painting an "inaccurate and misleading picture of the intelligence community. "The reality is that the men and women at the National Security Agency and across the intelligence community are abiding by the law, respecting the rights of citizens and doing everything they can to help keep our nation safe," he says. To do this, they must "use every intelligence tool available to understand the intent of our foreign adversaries." In the modern telecommunications era, our adversaries have the ability to hide their messages and discussions among those of innocent people around the world. They use the very same social networking sites, encryption tools and other security features that protect our

daily online activities. These are promises and warnings we've heard many times, and they're all valid defenses of the overall surveillance apparatus. What they don't do, unfortunately, is address the implicit questions that Greenwald and Schneier have posed: should one wing of the US government attempt to undermine the very tools that other branches have helped create? And is it valuable to be able to keep some communications almost completely private, even if terrorists can also exercise this privacy? If the dismissive GCHQ comments of "pseudo-legitimate" Tor uses are any indication, the international intelligence community's answer may be a resounding "No."

Decryption Methods Prevent Terrorism

Peterson 6/4-15(Andrea Reporter for Washington Post, "FBI official: Companies should help us 'prevent encryption above all else'", Washington Post, "<http://www.washingtonpost.com/blogs/the-switch/wp/2015/06/04/fbi-official-companies-should-help-us-prevent-encryption-above-all-else/>")

The debate over encryption erupted on Capitol Hill again Wednesday, with an FBI official testifying that law enforcement's challenge is working with tech companies "to build technological solutions to prevent encryption above all else." At first glance the comment from Michael B. Steinbach, assistant director in the FBI's Counterterrorism Division, might appear to go further than FBI Director James B. Comey. Encryption, a technology widely used to secure digital information by scrambling data so only authorized users can decode it, is "a good thing," Comey has said, even if he wants the government to have the ability get around it. [Special report: The Internet's founders saw its promise but didn't foresee users attacking one another] But Steinbach's testimony also suggests he meant that companies shouldn't put their customers' access to encryption ahead of national security concerns -- rather than saying the government's top priority should be preventing the use of the technology that secures basically everything people do online. **"Privacy, above all other things, including safety and freedom from terrorism, is not where we want to go,"** Steinbach said. He also disputed the "back door" term used by experts to describe such built-in access points. **"We're not looking at going through a back door or being nefarious,"** he argued, saying that the agency wants to be able to access content after going through a judicial process.

Decryption is effective for counter-terrorism

Ataide 2/7/-13(Rui As a security conscious individual, I've learned to educate people on the advantages of encryption, "The Man in the Middle: Advantages of SSL Decryption ", RSA "<https://blogs.rsa.com/author/rui-ataide/>")

I'm currently involved on a lot of security analytics, security response, and other defensive activities. While encryption provides a level of protection when it comes to defense, it also causes a lack of visibility when analyzing network traffic. More and more, even the "bad guys" are using encryption to cover their tracks and avoid detection. It's therefore no surprise that more and more organizations are using SSL inspection devices to monitor their traffic and infrastructure. I actually find myself recommending that they do use the technology and how to best implement it. SSL inspection devices are nothing more than a well designed man-in-the-middle attack that breaks the encryption into two separate encrypted streams. Therefore, they still provide an adequate level of protection to end-users while allowing security analysts and devices to properly monitor and alert when malicious or unwanted activity takes place. This could be something as simple as a user uploading a confidential document to his/her personal webmail account or more elaborate as someone using an SSL VPN to connect back to a host using a Dynamic DNS name service (a technique commonly used by current malware and advanced attackers).

Decryption is crucial to fighting cyberattacks

Butler 13 (J. Michael Butler, Associate Professor of Humanities at Flagler College, “Finding Hidden Threats by Decrypting SSL”, November 2013, <http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840>)

SSL encryption is crucial to protecting data in transit during web transactions, email communications and the use of mobile apps. Data encrypted with this common method can sometimes pass uninspected through almost all the components of your security framework, both inbound and outbound. As such, SSL encryption has become a ubiquitous tool for the enemy to hide sensitive data transfers and to obfuscate their command and control communications. For example, suppose a user has succumbed to one of the many phishing emails she receives every day, has followed a bad URL link and inadvertently downloaded encrypted Zeus malware to the financial officer’s computer used for ACH bank transfers. Under the cover of encryption, Zeus sends that password information and other sensitive data to an external user, making it possible for the remote attacker to capture a login session, use the transmitted password and deposit the organization’s money in an offshore account. With all commands and traffic transmitted into and out of the network via SSL, the company’s security tools were blind to these activities. Now companies are accepting even more encrypted traffic as they shift toward greater use of cloud services. This means malware will find more innovative ways to take advantage of this common form of transport encryption. For example, attackers can use cloud services to bypass the firewall and synchronize malware from one computer to another, as described in an August 2013 article in “Technology Review News.” ¹ With the good guys and bad guys both using encryption, making malicious traffic visible through decryption—and inspecting it—becomes essential. The decryption must be conducted in a way that doesn’t interfere with legitimate network traffic, while working with other security systems for optimum accuracy and performance. Then, the traffic must be re-encrypted before sending it on to its destination to protect sensitive information that might be caught up in the packets being decrypted. This whitepaper describes the role of SSL, the role SSL decryption/inspection tools play in security, options for deploying inspection tools, and how the information generated by such inspection can be shared with other security monitoring systems.

NSA decryption Program Works

Insider Surveillance 12/30/-14(“NSA Decryption: New Snowden Leak is Ancient History “,Insider surveillance”[https://insidersurveillance.com/nsa-decryption-new-snowden-leak-is-ancient-history/”](https://insidersurveillance.com/nsa-decryption-new-snowden-leak-is-ancient-history/))

Well-known for many months now is that the NSA views encryption as a threat to national security, and classifies five types of network communications challenges ranging from “trivial,” “minor” and “moderate” on the low end to the most serious, “major” and “catastrophic.” Small time stuff for NSA Decryption experts: Peer-to-Peer. Skype, still touted as a “secure” form of voice & video communication by owner Microsoft, has been an open book to NSA analysts since at least 2011. Secure Socket Layer — Not so Much. Web connections via https — with the “s” standing for secure, and using secure socket layer (SSL) for encryption, are a snap to break into. NSA routinely captures untold number of SSL handshakes, then analyzes metadata about the connections and metadata from the encryption protocols to break the keys and decrypt any traffic on the Internet via man-in-the-middle attacks. Virtual Private Networks. Long considered highly

secure, and still used to connect mediation devices/routers with law enforcement end points, VPNs have for quite some time been readily opened and their contents reviewed by NSA analysts. "Major" encryption challenges deemed difficult but not impossible: Zoho and Tor. As of 2012 the NSA had problems cracking messages sent through encrypted email service providers Zoho. Monitoring users of the Tor network was also a challenge. Truecrypt. The leaked files point to Truecrypt, a program for "on the fly encryption," as a major headache for the NSA several years ago. Truecrypt was discontinued in May 2014 and developers urged site visitors to find another source for encryption. Read: The NSA figured it out. Off-the-Record (OTR). OTR is an open source protocol for encrypting instant messaging in an end-to-end encryption process. OTR once proved a formidable challenge by combining AES symmetric key algorithm, the Diffie-Hellman method of securely exchanging cryptographic keys over a public channel, and SHA-1 (secure hash algorithm) cryptographic hash function developed by the NSA itself in the mid-1990s. Any combination of encryption modes raises the bar for network penetration. In addition, open source software is harder to attach back doors to without the public noticing. Back in 2011 – 2012, released documents showed that OTR occasionally created problems for NSA. One internal comment reads, "No decrypt available for this OTR encrypted message." However, tech moves on. The NSA — being a significant user of encryption itself — is often directly behind new developments in the field like SHA-1. Like all honest brokers in the field, NSA likes to crack its own work, find the weak spots, fix them and move on. New and improved versions of the hash function include SHA-2 and SHA-3. Companies are following NSA's lead. Microsoft announced in Nov 2013 its "depracation" policy for discontinuing use of SHA-1. Google followed suit for Chrome in Sept 2014. Does this mean that the SHA-1 component of OTR is no longer a head-scratcher for NSA? Yep. What earns the moniker "catastrophic" at NSA? At the head of the list, at least in 2012, was the challenge of users combining Tor with other anonymizing services such as ZRTP, which encrypts VoIP voice and text chats on mobile phones. The "Z" stands for its author, Phil Zimmerman, and the "RTP" for Real-Time Transport Protocol." ZRTP uses Diffie-Hellman secure key cryptography, and auto-senses for other VoIP clients that support ZRTP. It is common to open source programs such as Signal and Redphone. While Tor and ZRTP penetration may have seemed insurmountable several years, the UK's NSA equivalent — GCHQ — has proposed methods for breaking into Tor and defeating other encryption methods.

Targeting terrorist use of encryption is key

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, ES)

As law enforcement and security services' interception of terrorists' messages in some countries has grown, 92 operatives have increasingly utilized encryption technologies to communicate online via e-mail. 93 As the Washington Post reported, "Al Qaeda members have taught individuals ... how to use the Internet to send messages and how to encrypt those communications to avoid detection." 94 For example, Wadih El-Hage, Osama bin Laden's former personal secretary and a senior planner of the 1998 Al Qaeda bombings of U.S. Embassies in Kenya and Tanzania, "sent en- crypted e-mails under various names to associates in Al Qaeda." 95 In addition, "Khalik Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bombings in Jordan at the turn of the millennium." 96 The convicted planner of the

1993 World Trade Center bombing, Ramzi Yousef, "used encrypted files to hide details of a plot to destroy eleven U.S. airliners over the Pacific Ocean. 97

Targeting encrypted data key to countering terrorist backdoors

Barfield 6/9/15 [Claude Barfield, a former consultant to the office of the U.S. Trade Representative, researches international trade policy (including trade policy in China and East Asia), the World Trade Organization (WTO), intellectual property, and science and technology policy. “Encryption: The next battle between security and privacy”, American Enterprise Institute, <https://www.aei.org/publication/encryption-the-next-battle-between-security-and-privacy/>] Schuler 20

Over the past several weeks, we have witnessed an intense debate over cybersecurity and privacy, revolving around the USA Freedom Act. A badly divided Congress, finally—in a rebuke to Senate Majority Leader Mitch McConnell (R-KY) and other defenders of the status quo—mandated the end of the so-called NSA metadata (bulk collection) program that swept up data on the dates, times and location of phone calls. The battle over the NSA metadata program, however, is only the first of what are likely to be a series of clashes over the balance between security and privacy. Looming as the next faceoff is the conflict over encryption and the moves by a number of US technology companies to protect their customers against hackers, whether private or public. In the US, the current skirmish was precipitated by announcements from Apple and Google that they were installing encryption protection in their cellphones that would allow only users—and no outside individual or public official—to unblock the devices. Text messaging services such as WhatsApp and iMessage have followed suit. FBI Director James Comey has taken the lead in strenuous opposition to the encryption moves, denouncing “companies that are marketing something expressly to allow people to place themselves beyond the law.” Following up, last week FBI Assistant Director Michael Steinbach warned a congressional committee that crime groups and terrorists organizations such as ISIS were “going dark” with encryption, heightening the chance that future attacks would go unmasked. House Homeland Security Committee Chairman Michael McCaul (R-TX) responded by labeling the use of encryption a “threat to the homeland.” Thus far, US tech companies are defiant and determined to increase encryption applications to their technologies. Google’s Eric Schmidt argued that the security agencies had only themselves to blame: “The people who criticized this are the ones who should have expected this.” And Apple CEO Tom Cook recently delivered an impassioned defense of encryption, labeling attempts to undermine encryption “incredibly dangerous.” The companies make two arguments. First, technologically, there is no way to introduce “backdoors” for the government without allowing criminals or terrorists to exploit the same flaws. Second, they argue that the government has a number of alternatives: much cellphone data is now stored in the providers’ cloud services and can be retrieved; legal wiretaps of smartphones are not affected; and finally, officials can still retrieve real-time phone records and logs of text messages. There is also an international dimension to the conflict. British Prime Minister David Cameron, new re-elected, has vowed to push through legislation that would force tech companies doing business in Great Britain to provide encryption to police and security officials or risk being banned from that country. In France, in the wake of the Hebdo massacre, new security legislation gives sweeping powers to the government to undertake a host of new tactics against future terrorist attacks. And the loose language may allow similar action against encrypted devices. Back in the United States, the resolution of the standoff is unclear. Chairman McCaul and others have yet to push hard for legislation. And the position of the Obama administration remains indeterminate. President Obama has been equivocal. When queried insistently by the press, he responded that he

sympathized with the tech companies: "They're patriots." But the president went on to note: "If we find evidence of a terrorist plot...and despite having a phone number, despite having a social media address or e-mail address, we can't penetrate that, that's a problem." If the syntax was garbled, so was the message.

Encryption cracking necessary to prevent terrorism

Network World, September 19, 2013, NSA wants even closer partnership with tech industry;

NSA's Debora Plunkett says NSA's now is real-time automated information sharing on a large scale, <http://www.networkworld.com/news/2013/091913-nsa-tech-industry-274011.html> DOA: 2-1-15

The National Security Agency's director of information assurance today said **the "way to achieve confidence in cyberspace" is to increase collaboration between the government and the high-tech industry** -- remarks that rang ironic given former NSA contractor Edward Snowden's revelations about how NSA works with industry. NSA documents leaked by Snowden showed that **the NSA's goal is to build backdoors into commercial products and weaken encryption to make it easier for surveillance**, allegations that the U.S. government has not even tried to refute. When asked about that today, NSA director of information assurance Debora Plunkett, who gave the keynote address at the New York Institute of Technology Cyber Security Conference here, flatly refused to discuss the topic. But her keynote address was intended to get hardware and software vendors to work in ever-closer partnership with the NSA. **Cyberattacks that could take electricity grids offline and disrupt transportation systems are possible.** Plunkett said in her keynote, pointing out the destructive attack that hit Saudi Aramco last year and impacted data systems there. [RELATED: Reported NSA actions raise serious questions about tech industry partnerships MORE: Black Hat: Top 20 hack-attack tools] It's a simple matter to hire hacking services to carry out attacks such as denial-of-service, she said, and the fear now is of "integrity attacks" that would destroy or alter critical data. These are all "cyber security challenges," she noted, and the government today is largely dependent on commercial hardware and software for which the NSA itself cannot "provide indemnification." NSA's needs industry's help, she said. Plunkett said "we have to have a community come together" to collaborate on security in mobility and the cloud especially. **The NSA expects that the future of network security lies in "more automated cyber defense" based on "large-scale automation" that would reduce the need for manpower where there would be more real-time sharing of findings.** She said there's a need for collaboration with ISPs and hardware companies to achieve all of this. "We have to build a close partnership," she said, adding, there can be "confidence in cyberspace" if "we stay the course." Plunkett is a 29-year veteran of the NSA who worked her way up through the ranks to have a hand in guiding strategic direction for the agency, which carries out surveillance to help defend the country against cyberthreats. But NSA documents recently leaked by Snowden show that the NSA views its partnership with industry in part as a way to subvert security in commercial products and services to make cyber-spying easier. This revelation casts NSA's call for industry partnership and its insistence that there can be "confidence in cyberspace" in a questionable light.

The Bullrun program is key to decrypting internet communications and data relevant to international terrorism

Larson, Perlroth, and Shane, 9/5/13 (Jeff, Data Editor at ProPublica; Nicole, The New York Times; Scott, The New York Times; ProPublica, the organization that Snowden gave his leaks, "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security"
<http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>, accessed 7/14/15)

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor. Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own "back door" in all encryption, it set out to accomplish the same goal by stealth. The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated. The N.S.A. hacked into target computers to snare messages before they were encrypted. And the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world. "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable." When the British analysts, who often work side by side with N.S.A. officers, were first told about the program, another memo said, "those not already briefed were gobsmacked!" An intelligence budget document makes clear that the effort is still going strong. "We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet traffic," the director of national intelligence, James R. Clapper Jr., wrote in his budget request for the current year. In recent months, the documents disclosed by Mr. Snowden have described the N.S.A.'s broad reach in scooping up vast amounts of communications around the world. The encryption documents now show, in striking detail, how the agency works to ensure that it is actually able to read the information it collects. The agency's success in defeating many of the privacy protections offered by encryption does not change the rules that prohibit the deliberate targeting of Americans' e-mails or phone calls without a warrant. But it shows that the agency, which was sharply rebuked by a federal judge in 2011 for violating the rules and misleading the Foreign Intelligence Surveillance Court, cannot necessarily be restrained by privacy technology. N.S.A. rules permit the agency to store any encrypted communication, domestic or foreign, for as long as the agency is trying to decrypt it or analyze its technical features. The N.S.A., which has specialized in code-breaking since its creation in 1952, sees that task as essential to its mission. If it cannot decipher the messages of terrorists, foreign spies and other adversaries, the United States will be at serious risk, agency officials say. Just in recent weeks, the Obama administration has called on the intelligence agencies for details of communications by Qaeda leaders about a terrorist plot and of Syrian officials' messages about the chemical weapons attack outside Damascus. If such communications can be hidden by unbreakable encryption, N.S.A. officials say, the agency cannot do its work.

Without access to backdoors, law enforcement won't have the capacity to collect intelligence data because of increasingly complex encryption

AP 7/8 (Eric Tucker, "FBI, JUSTICE DEPT. TAKE ENCRYPTION CONCERNS TO CONGRESS" Associated Press,
[http://hosted.ap.org/dynamic/stories/U/US_FBI_ENCRYPTION?SITE=AP&SECTIO
N=HOME&TEMPLATE=DEFAULT&CTIME=2015-07-08-06-22-03\)](http://hosted.ap.org/dynamic/stories/U/US_FBI_ENCRYPTION?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2015-07-08-06-22-03)

WASHINGTON (AP) -- Federal law enforcement officials warned Wednesday that data encryption is making it harder to hunt for pedophiles and terror suspects, telling senators that consumers' right to privacy is not absolute and must be weighed against public-safety interests. The testimony before the Senate Judiciary Committee marked the latest front in a high-stakes dispute between the Obama administration and some of the world's most influential tech companies, placing squarely before Congress an ongoing discussion that shows no signs of an easy resolution. Senators, too, offered divided opinions.FBI and Justice Department officials have repeatedly asserted that encryption technology built into smartphones makes it harder for them to monitor and intercept messages from criminal suspects, such as Islamic State sympathizers who communicate online and child predators who conceal pornographic images. They say it's critical that they be able to access encrypted communications during investigations, with companies maintaining the key to unlock such data.¶ But they face fierce opposition from Silicon Valley companies who say encryption safeguards customers' privacy rights and offers protections from hackers, corporate spies and other breaches. The companies in recent months have written to the Obama administration and used public speeches to argue for the value of strong encryption.¶ FBI Director James Comey, who has pressed his case repeatedly over the last year before think tanks and in other settings, sought Wednesday to defuse some of the tension surrounding the dispute. He told senators that he believed technology companies were fundamentally on the same page as law enforcement, adding, "I am not here to fight a war."¶ "Encryption is a great thing. It keeps us all safe. It protects innovation," Comey said. "It protects my children. It protects my health care. It is a great thing."¶ But he warned that criminals were using encryption to create a safe zone from law enforcement. He said that concern was especially acute at a time when the Islamic State has been recruiting sympathizers through social media and then directing them to encrypted platforms that federal agents cannot access.¶ "Our job is to look at a haystack the size of this country for needles that are increasingly invisible to us because of end-to-end encryption," he said.¶

Deterrence

Independently, the perception of widespread surveillance is crucial to deter effective terrorist communication --- the plan emboldens effective regrouping
Rascoff 14 [Samuel J. Rascoff, Associate Professor of Law, Faculty Director, Center on Law and Security, New York University School of Law, "COUNTERTERRORISM AND NEW DETERRENCE," 2014]

An open question - an answer to which requires more empirical data - is whether the government's prosecution of relatively amateur would-be terrorists based on stings is likely to be effective in deterring better-trained terrorists. n109 But it bears remembering that the viability [*855] of the deterrence-based account of stings does not depend on who is prosecuted. The mere fact of prosecution can alter terrorists' perceptions of future success by implying a **pervasive surveillance network** n110 facilitated by technology. n111 As Alex Wilner observed of Canadian counterterrorism, the fact that the country's "intelligence community clearly has the **means and the tools to uncover plots expeditiously"** creates an "overwhelming perception ... that terrorists are unlikely to evade Canada's watchful eye." n112 In sum, the meaning of a sting operation and subsequent trial must include the strategic benefits of revealing the fact of undercover surveillance as well as the normative costs implied by widespread surveillance. n113 This in turn illustrates the [*856] complicated relationship between transparency and secrecy entailed by new deterrence. C. Psychology and Strikes New deterrence also enriches understanding of the role of fear and emotion in counterterrorism. Terrorism aims at communicating vulnerability and sowing distrust; violent attacks are, in a sense, means to bring about these more intangible objectives. n114 (Thus, building sufficient social resiliency to withstand terrorist attacks, as new deterrence counsels, deprives terrorists of an important goal, even when an attack succeeds. n115) But fear n116 and distrust are also part of the counterterrorism repertoire. n117 Inevitably this fact raises serious [*857] normative issues. First is the foundational question of what it means for the state to manage terrorist risk through the potentially widespread, deliberate employment of fear. n118 Rich sociological and historical literature attest to the emotional costs of aggressive national security tactics. n119 Second is a concern about the distribution of fear and whether the government considers race and religion when employing it. n120 My central point here, however, is not normative so much as conceptual: Whereas policymakers, lawyers, and the general public often define counterterrorism as the sum of so many violent interventions, new deterrence reminds us that counterterrorism also operates in a psychological register. Unlike traditional deterrence, which conveys its message through fear of being caught and punished, new deterrence relies on a wider and subtler range of official modalities that go to the likelihood of terrorist success. For example, the government may aim to demoralize an adversary by telegraphing the state's overwhelming might. The state might do so by "spreading false or exaggerated rumors of the [*858] existence of sting operations," n121 sowing a sense of distrust within a cell by implying that one among them is on an official payroll, or even conveying an image of officials as irrational and prone to unmeasured violence.

Every Piece Matters

Successful counterterrorism requires a *broad, multi-faceted strategy* – removing even a small part of the mandate weakens the entire mission

White House '11

[White House Brief on Federal/Local Partnerships to Combat Extremism. “Empowering Local Partners to Combat Violent Extremism” August 2011

https://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf]

We are fortunate that our experience with community-based problem solving, local partnerships, and community-oriented policing provides a basis for addressing violent extremism as part of a broader mandate of community safety. We therefore are building our efforts to counter radicalization that leads to violence in the United States from existing structures, while creating capacity to fill gaps as we implement programs and initiatives. Rather than creating a new architecture of institutions and funding, we are utilizing successful models, increasing their scope and scale where appropriate.¶ While communities must often lead this effort, the Federal Government has a significant responsibility. Our research and consultations with local stakeholders, communities, and foreign partners have underscored that the Federal Government's most effective role in strengthening community partnerships and preventing violent extremism is as a facilitator, convener, and source of information. The Federal Government will often be ill-suited to intervene in the niches of society where radicalization to violence takes place, but it can foster partnerships to support communities through its connections to local government, law enforcement, Mayor's offices, the private sector, local service providers, academia, and many others who can help prevent violent extremism. Federal departments and agencies have begun expanding support to local stakeholders and practitioners who are on the ground and positioned to develop grassroots partnerships with the communities they serve. Our central goal in this effort is to prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence. The U.S. Government will work tirelessly to counter support for violent extremism and to ensure that, as new violent groups and ideologies emerge, they fail to gain a foothold in our country. Achieving this aim requires that we all work together—government, communities, the private sector, the general public, and others—to develop effective programs and initiatives.

Every facet of domestic surveillance is critical because successfully preventing attacks requires successful coordination of diffuse priorities

White House '11

[“Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States” December 2011 <https://www.whitehouse.gov/sites/default/files/sip-final.pdf>]

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include:

(1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.¶ 1. Whole-of-Government Coordination¶ Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ,

and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, “including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence.” To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.[¶] This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

National Security Letters

Our dead drops link:

Terrorists coordinate attacks using email dead drops

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, “ENDING THE CYBER JIHAD:

COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE” 2006, HeinOnline, p. 138-9)

E-mail dead drops are another simple but effective tactic used by terrorist conspirators. E-mail dead drops involve the distribution of a user name and password for an e-mail account to members of a terrorist cell who can then enter the account and save an unsent message in the draft folder for the other account users.¹ ° Because the message is never sent from the account, there is no identifying information to assist law enforcement officials in tracing the IP address or location of the message creator.¹ Khalid Sheik Mohammed, a key planner of the September 11 th attacks arrested in Pakistan in March 2003,¹² "used the e-mail dead drop technique to avoid having his e-mails intercepted by eavesdroppers in the United States or allied governments."¹³ Mohammed or his operatives would open an account on a free, public e-mail service such as Hotmail, write a message in draft form, save it as a draft, then transmit the e-mail account name and password during chatter on a relatively secure message board The intended recipient could then open the e-mail account and read the draft¹⁴ Because no e-mail message was sent, there was a reduced risk of interception by authorities.

NSL's are key to stop those because they require ISPs to grant access

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, “ENDING THE CYBER JIHAD:

COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE” 2006, HeinOnline, p. 151-3)

In the weeks following the September 11th attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"),² which was designed to address inadequacies in our nation's homeland security and to provide the necessary tools to address these problems.⁰ In the area of cyber terrorism, however, the Act narrowly focuses on stiffer penalties for individuals who carry out offensive cyber attacks resulting in physical injury to American citizens, damage to U.S. facilities, or threaten public health or safety.² The legislation also authorizes additional funding for forensic laboratories to investigate cyber crimes.²⁷ However, the law does not include penalties for using the Internet to promote or communicate terrorism-related activities unrelated to cyber attacks. Instead, Congress appears content to allow terrorism-related activity on the Internet to be governed by anti-terrorism statutes.²⁰ The Bush administration has emphasized that the PATRIOT Act encourages ISPs and e-mail providers to act as cyber watchdogs and report suspicious online activities.²⁰⁹ In a July 2005 speech, President Bush argued that the PATRIOT Act enhances the security of the Internet by protecting ISPs from civil lawsuits "when they give information to law enforcement when it would help law enforcement prevent a threat of death or serious injury."²¹⁰ The statutory provision, however, encourages rather than requires ISPs to report threatening information on their sites.²¹¹ To date, there is no available evidence to suggest that ISPs, Web hosts, or e-mail providers have increased their monitoring or reporting of

suspected terrorism-related emails since September 11th.²¹² Furthermore, the voluntary nature of this measure limits the likelihood that an ISP would shut down a Web site at the request of the government out of a fear that such action will raise civil liberties and prior restraint concerns.²¹³

General Surveillance Restriction Links

Surveillance key to stop lone wolf domestic terrorism – recent cases prove

David **Inserra** specializes in cyber and homeland security policy, including protection of critical infrastructure, as research assistant in The Heritage Foundation's Allison Center for Foreign Policy Studies; **7-5**-15 ("How to turn the tide on terrorism," Omaha, http://www.omaha.com/opinion/david-inserra-how-to-turn-the-tide-on-terrorism/article_583ccd2b-3b3d-509d-b3a4-d18619f36ca2.html, ME)

Most of us are familiar with Dzhokhar Tsarnaev, thanks to media coverage of **the Boston Marathon bombing** case. But very few have heard of Munther **Omar Saleh**. There's a good reason for that, though. Both shared a desire to commit acts of terrorism, but Saleh's plans, unlike Tsarnaev's, were disrupted before they could be carried out. He and two co-conspirators considered numerous sites in New York City for their attack before being arrested on June 13 — **the 70th publicly known terror plot on the U.S. since 9/11**. So how was Saleh's attack foiled? And how can we address the current spike in terrorist activity? Let's consider these important questions in turn. Late last year, **Saleh began making radical statements through social media**. He called al-Qaida "too moderate" and expressed support for the caliphate that **the Islamic State** claims to have established in parts of Iraq and Syria. He expressed support for the attack on the Mohammed cartoon contest in Texas and began to translate Islamic State and other radical videos and material into English. **The FBI began watching Saleh and his computer activity through judicially authorized surveillance**, and in March twice found him examining the George Washington Bridge between New York and New Jersey. They interviewed Saleh. He denied supporting Islamic State or holding any radical, violent beliefs, but he provided access to his computer. He then denied reading or translating the radical material they found on it. In May, **Saleh began to research weapons, training and equipment that could be used to carry out violent attacks and bombings**. He downloaded instructions for building a pressure-cooker bomb; researched various weapons, as well as surveillance and disguise equipment and electronics; and continued to look at various New York landmarks. During this time, **Saleh was also enrolled in an electrical engineering course that would teach him skills useful for building a bomb**. When approached by a confidential informant, Saleh said he was "in NY and trying to do an op," a reference to his terrorist operations and plotting. He would not communicate further with the informant, however, because he was ordered by officials he believed to be part of Islamic State not to communicate with others. On June 13, Saleh and another co-conspirator were picked up by Fareed Mumuni and began to perform anti-surveillance measures — driving without lights, not stopping at stop signs, and erratically pulling over and speeding up. At around 4 a.m., they stopped at a red light, and Saleh (with knife in hand) and one other individual got out of the car and charged a law enforcement vehicle tracking them. Their surveillance operation blown, the police moved in and arrested Saleh and the other conspirator who ran at the police vehicle. **After questioning Saleh, the FBI learned that the group had planned to use a bomb, run over law enforcement that responded with a car, and then take their weapons to attack others. Saleh pledged full allegiance to the Islamic State and claimed that his co-conspirators had also.** When the FBI went to arrest Mumuni on June 17, he stabbed an FBI agent multiple times, but the agent's vest prevented the knife from doing serious injury. **The Saleh case, one of three foiled attacks in June alone, shows why law enforcement and intelligence officials need more tools to stop terrorists before they strike — not fewer, as some lawmakers have suggested. Legitimate government surveillance programs, for example, are a vital component of our national security and should be allowed to continue.** Greater cyber-investigation capabilities in the higher-risk urban areas are also essential. **With so much terrorism-related activity occurring on the Internet, local law enforcement should be able to monitor and track violent extremist activity on the Web** when reasonable suspicion exists to do so. Greater intelligence and law enforcement cooperation is also needed to uncover and neutralize terrorist plots, curtail the flow of foreign fighters to Syria, and monitor the activities of foreign fighters who have returned to the U.S. and other countries. This doesn't mean we allow anything in the name of national security. Far from it. The government has an obligation to follow the law and respect individual privacy and liberty. But within those necessary strictures, **we should give our law enforcement and**

intelligence officials all the tools they need — to ensure that any future aspiring terrorists remain as unknown as Munther Omar Saleh.

Communication surveillance essential to prevent terrorism

Lewis 14 (senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies)

(James Andrew, Underestimating Risk in the Surveillance Debate, http://csis.org/files/publication/141209_-Lewis_UnderestimatingRisk_Web.pdf)

There is general agreement that **as terrorists splinter** into regional groups, **the risk of attack increases**.

Certainly, the threat to Europe from militants returning from Syria points to increased risk for U.S. allies. The messy U.S. withdrawal from Iraq and (soon) Afghanistan contributes to an increase in risk.²⁴ European authorities have increased surveillances and arrests of suspected militants as the Syrian conflict lures hundreds of Europeans. Spanish counterterrorism police say they have broken up more terrorist cells than in any other European country in the last three years.²⁵ The chairman of the House Select Committee on Intelligence, who is better placed than most members of Congress to assess risk, said in June 2014 that the level of terrorist activity was higher than he had ever seen it.²⁶ If the United States overreacted in response to September 11, it now risks overreacting to the leaks with potentially fatal consequences.

A simple assessment of the risk of attack by jihadis would take into account a resurgent Taliban, the power of Islamist groups in North Africa, the continued existence of Shabaab in Somalia, and the appearance of a powerful new force, the Islamic State in Iraq and Syria (ISIS).

Al Qaeda, previously the leading threat, has splintered into independent groups that make it a less coordinated force but more difficult target. On the positive side, the United States, working with allies and friends, appears to have contained or eliminated jihadi groups in Southeast Asia. Many of these groups seek to use adherents in Europe and the United States for manpower and funding. A Florida teenager was a suicide bomber in Syria and Al Shabaab has in the past drawn upon the Somalipopulation in the United States. Hamas and Hezbollah have achieved quasi-statehood status, and Hamas has supporters in the United States. Iran, which supports the two groups, has advanced capabilities to launch attacks and routinely attacked U.S. forces in Iraq. The United Kingdom faces problems from several hundred potential terrorists within its large Pakistani population, and there are potential attackers in other Western European nations, including Germany, Spain and the Scandinavian countries. France, with its large Muslim population faces the most serious challenge and is experiencing a wave of troubling anti-Semitic attacks that suggest both popular support for extremism and a decline in control by security forces. The chief difference between now and the situation before 9/11 is that all of these countries have put in place much more robust surveillance systems, nationally and in cooperation with others, including the United States, to detect and prevent potential attacks. Another difference is that the failure of U.S. efforts in Iraq and Afghanistan and the opportunities created by the Arab Spring have

opened a new "front" for jihadi groups that makes their primary focus regional. **Western targets still remain of interest, but are more likely to face attacks from domestic sympathizers. This could change if the well-resourced ISIS is frustrated in its efforts to establish a new Caliphate and turns its focus to the West.** In addition, the al Qaeda affiliate in Yemen (al Qaeda in the Arabian Peninsula) continues to regularly plan attacks against U.S. targets.

The incidence of attacks in the United States or Europe is very low, but **we do not have good data on the number of planned attacks that did not come to fruition. This includes not just attacks that were detected and stopped, but also attacks where the jihadis were discouraged and did not initiate an operation or press an attack to its conclusion because of operational difficulties. These attacks are the threat that mass surveillance was created to prevent. The needed reduction in public anti-terror measures without increasing the chances of successful attack is contingent upon maintaining the capability provided by communications surveillance** to detect, predict, and prevent attacks. Our opponents have not given up; neither should we.

Communication surveillance the best way to reduce terrorism

Lewis 14 (senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies)

(James Andrew, Underestimating Risk in the Surveillance Debate, http://csis.org/files/publication/141209_-Lewis_UnderestimatingRisk_Web.pdf)

The echoes of September 11 have faded and the fear of attack has diminished. We are reluctant to accept terrorism as a facet of our daily lives, but major attacks—roughly one a year in the last five years—are regularly planned against U.S. targets, particularly passenger aircraft and cities. **America's failures in the Middle East have spawned new, aggressive terrorist groups.**

These groups include radicalized recruits from the West—one estimate puts the number at over 3,000—who will return home embittered and hardened by combat. Particularly in Europe, the next few years will see an influx of jihadis joining the existing population of homegrown radicals, but the United States itself remains a target.

America's size and population make it is easy to disappear into the seams of this sprawling society. Government surveillance is, with one exception and contrary to cinematic fantasy, limited and disconnected. That exception is communications surveillance, which provides the best and perhaps the only national-level solution to find and prevent attacks against Americans and their allies. Some of the suggestions for alternative approaches to surveillance, such as the recommendation that NSA only track “known or suspected terrorists,” reflect both deep ignorance and wishful thinking. It is the unknown terrorist who will inflict the greatest harm. This administration could reasonably argue that everything it has done is legal and meets existing requirements for oversight, but this defense is universally perceived as legalistic hairsplitting. If the government can be faulted, it is for obsessive secrecy. The public debate over NSA's surveillance programs routinely exaggerates risks and errors, but in the absence of a compelling official narrative, the space was filled with conjecture and distortion. This has not helped a crucial debate where a wrong answer could mean more bombings.

Surveillance of communication info is key to check terror risks

Clarke '13

(et al; This is the Final Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. President Obama ordered a blue-ribbon task force to review domestic surveillance. This report releases the findings of that group. The report was headed by five experts – including Richard Alan Clarke, who is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. Other expert contributors include Michael Joseph Morell, who was the deputy director of the Central Intelligence Agency and served as acting director twice in 2011 and from 2012 to 2013 and Cass Robert Sunstein, who was the Administrator of the White House Office of Information and Regulatory Affairs in the Obama administration and is currently a Professor of Law at Harvard Law School. “LIBERTY AND SECURITY IN A CHANGING WORLD” – December 12th, 2013 – Easily obtained via a google search.
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=https%3A%2F2Fwww.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fdocs%2F2013-12-12_rg_final_report.pdf&ei=Db0yVdDjKIKdNtTXgZgE&usg=AFQjCNH0S_Fo9dckL9bRarVpi4M6pq6MQ&bvm=bv.91071109,d.eXY

The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare. A robust foreign intelligence collection capability is essential if we are to protect ourselves against such threats. Because our adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

Expansive Domestic Communication Surveillance is key to check terror risks.

Small '8

MATTHEW L. SMALL. Small wrote this paper as part of studies at the United States Air Force Academy. This paper was completed with guidance from Dr. Damon Coletta – a professor at the US Air Force Academy. He holds a Ph.D. in Political Science from Duke and a Masters in Public Policy from Harvard. This paper was also completed with guidance from Dr. Gary Donato – who is a Lecturer of Global Studies at Bentley University. – “His Eyes are Watching You: Domestic Surveillance, Civil Liberties and Executive Power during Times of National Crisis” – 2008 – available at: <http://cspc.nonprofitsoapbox.com/storage/documents/Fellows2008/Small.pdf>

Very soon after the terrorist attack of September 11th, 2001, President Bush authorized the NSA to conduct warrantless wiretaps on the communications of American citizens. The agency monitored communications from phone numbers of suspected al Qaeda affiliates (Risen and Lichtblau 2005). The calls that the NSA monitored originated in the United States and ended overseas but still involved American citizens. Bush asserted that it was necessary to move quickly to gain information on other suspected terrorist and/or terrorist activities (Risen and Lichtblau 2005). Officials close to the president claimed these actions successful in averting terrorist attacks as in the case of Iyman Faris, an Ohio trucker and naturalized citizen who intended to bring down the Brooklyn Bridge (Risen and Lichtblau 2005). Similar to the warrantless wiretaps, President Bush authorized the collection of phone records of millions of Americans from major phone companies such as AT&T and Verizon (USA Today [Washington], 11 May 2006). The records contain the communications of suspected terrorists or terrorist affiliates within the US. Even though these appear to be the under the same issue concerning the right to privacy, each act must be approached separately. In light of historical precedence, legislation enacted at the time, and the nature of the threat the US faces, President Bush's actions are more than justified. From Washington on, presidents have invaded citizens' privacy by authorizing surveillance of communications. Washington did not provide detailed accounts of his domestic surveillance to the Continental Congress, nor did Lincoln ask the permission of Congress to intercept wire communications within the US. Instead, each president assumed it as part of their powers as Commander-in-Chief and protectors of the rule of law. In comparison, Bush's actions are actually restrained. At the least he is recognizing the existence of legislation restraining the use of wiretaps and attempting to fit the urgent need for information within its confines.¹⁴ In Woodrow Wilson's case, Congress actually gave him the power to essentially search and seize international communication. Presidents from Harry S. Truman to Lyndon B. Johnson authorized the warrantless monitoring of communications by the NSA and FBI to combat dissension and subversion by Communist sympathizers. Although illegal, presidents even used the CIA to carry out many of these same activities. President Bush simply followed the same course of action as his predecessors, a logical course considering the nature of the threat. Terrorists can come in all forms and can easily manifest within the United States. Intercepting communications serves as one of the best and only ways to prevent these attacks from occurring. Herein lays the justification for legislative expansion of executive power.

We must keep all intelligence tools to fight terror

John McLaughlin teaches at the Johns Hopkins School of Advanced International Studies. He was deputy director and acting director of the CIA from 2000 to 2004, January 2, 2014, Washington Post, “NSA Intelligence-Gathering Programs Keep us Safe,” http://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html

As our debate continues, the terrorist threat is not receding but transforming. The core leadership of al-Qaeda has been degraded and remains under pressure, but robust al-Qaeda affiliates have multiplied. With the decline of central government authority in the Middle East and North Africa in the wake of the Arab Spring and the war in Syria, terrorists have the largest havens and areas for operational planning in a decade. If anything, the atomization of the movement has made the job of intelligence more labor-intensive, more detail-oriented and more demanding. Now is not the time to give up any tool in the counterterrorism arsenal.

Surveillance is a critical tool needed to defeat terrorism

Alan Dershowitz, Harvard Law School, May 5, 2014, The Atlantic, “No one opposes all surveillance; false equivalence on the NSA,” <http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-dershowitz/361694/> DOA: 2-22-15

Our enemies, especially those who target civilians, have one major advantage over us. They are not constrained by morality or legality. We have an advantage over them. In addition to operating under the rule of law, we have developed through hard work and extensive research technological tools that allow us to monitor and prevent their unlawful and lethal actions. Such technological tools helped us break the German and the Japanese code during the Second World War. They helped us defeat fascism. They helped us in the Cold War. And they are helping us now in the hot war against terrorists who would bomb this theater if they had the capacity to do so. You're going to hear again that there are only excuses that are being offered, that terrorism is really not a serious problem, or that American policy is as terroristic as the policy of al-Qaeda. I don't think you're going to accept that argument. We must not surrender our technological advantage.

Surveillance needed to defeat terrorism

Glenn Sulmasy, 2013, CNN, "Feds start building case against NSA leaker,"
<http://www.cnn.com/2013/06/10/opinion/sulmasy-nsa-snowden/> DOA: 4-1-15

The current threat by al Qaeda and jihadists is one that requires aggressive intelligence collection and efforts. One has to look no further than the disruption of the New York City subway bombers (the one being touted by DNI Clapper) or the Boston Marathon bombers to know that the war on al Qaeda is coming home to us, to our citizens, to our students, to our streets and our subways. This 21st century war is different and requires new ways and methods of gathering information. As technology has increased, so has our ability to gather valuable, often actionable, intelligence. However, the move toward "home-grown" terror will necessarily require, by accident or purposefully, collections of U.S. citizens' conversations with potential overseas persons of interest. An open society, such as the United States, ironically needs to use this technology to protect itself. This truth is naturally uncomfortable for a country with a Constitution that prevents the federal government from conducting "unreasonable searches and seizures." American historical resistance towards such activities is a bedrock of our laws, policies and police procedures. But what might have been reasonable 10 years ago is not the same any longer. The constant armed struggle against the jihadists has adjusted our beliefs on what we think our government can, and must, do in order to protect its citizens. However, when we hear of programs such PRISM, or the Department of Justice getting phone records of scores of citizens without any signs of suspicious activities nor indications of probable cause that they might be involved in terrorist related activities, the American demand for privacy naturally emerges to challenge such "trolling" measures or data-mining. The executive branch, although particularly powerful in this arena, must ensure the Congress is kept abreast of activities such as these surveillance programs. The need for enhanced intelligence activities is a necessary part of the war on al Qaeda, but abuse can occur without ensuring the legislative branch has awareness of aggressive tactics such as these. Our Founding Fathers, aware of the need to have an energetic, vibrant executive branch in foreign affairs, still anticipated checks upon the presidency by the legislature. Working together, the two branches can ensure that both legally, and by policy, this is what the citizens desire of their government -- and that leaks such as Snowden's won't have the impact and damage that his leaks are likely to cause.

Surveillance critical to the war on terror

Jessica Zuckerman et al, 2013, 60 Terrorist Plots Since 9-11: Continued Lessons in Domestic Counterterrorism, <http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism> DOA: 5-24-15 Zuckerman is a Policy Analyst @ Heritage, Steven Bucci Phd, Director, Douglas and Sarah Allison Center for Foreign and National Security Policy, James Carafano, Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow

Three months after the attack at the Boston Marathon, the pendulum of awareness of the terrorist threat has already begun to swing back, just as it did after 9/11. Due to the resilience of the nation and its people, for most, life has returned to business as usual. The threat of terrorism against the United States, however, remains.

Expecting to stop each and every threat that reaches a country's borders is unreasonable, particularly in a free society committed to individual liberty. Nevertheless, there are important steps that America's leaders can take to strengthen the U.S. domestic counterterrorism enterprise and continue to make the U.S. a harder target. Congress and the Administration should:

Ensure a proactive approach to preventing terrorist attacks. Despite the persistent threat of terrorism, the Obama Administration continues to focus on reactive policies and prosecuting terrorists rather than on proactive efforts to enhance intelligence tools and thwart terrorist attempts. This strategy fails to recognize the pervasive nature of the threat posed by terrorist groups such as al-Qaeda and homegrown extremism. The Administration, and the nation as a whole, should continue to keep in place a robust, enduring, and proactive counterterrorism framework in order to identify and thwart terrorist threats long before the public is in danger.

Maintain essential counterterrorism tools. Support for important investigative tools such as the PATRIOT Act is essential to maintaining the security of the U.S. and combating terrorist threats. Key provisions within the act, such as the roving surveillance authority and business records provision, have proved essential for thwarting terror plots, yet they require frequent reauthorization. In order to ensure that law enforcement and intelligence authorities have the essential counterterrorism tools they need, Congress should seek permanent authorization of the three sun setting provisions within the PATRIOT Act.^[208] Furthermore, legitimate government surveillance programs are also a vital component of U.S. national security, and should be allowed to continue. Indeed, in testimony before the house, General Keith Alexander, the director of the National Security Agency (NSA), revealed that more than 50 incidents of potential terrorism at home and abroad were stopped by the set of NSA surveillance programs that have recently come under scrutiny. That said, the need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well. Break down the silos of information. Washington should emphasize continued cooperation and information sharing among federal, state, and local law enforcement agencies to prevent terrorists from slipping through the cracks between the various jurisdictions. In particular, the FBI should make a more concerted effort to share information

more broadly with state and local law enforcement. State and local law enforcement agencies are the front lines of the U.S. national security strategy. As a result, local authorities are able to recognize potential danger and identify patterns that the federal authorities may miss. They also take the lead in community outreach, which is crucial to identifying and stopping “lone wolf” actors and other homegrown extremists. Federal law enforcement, on the other hand, is not designed to fight against this kind of threat; it is built to battle cells, groups, and organizations, not individuals.

Britain **Eakin**, June 19, 2013, Al Arabia, “NSA: Secret Surveillance Helped Prevent 50-plus terror attacks,” <http://english.alarabiya.net/en/News/world/2013/06/19/NSA-Secret-U-S-surveillance-helped-prevent-50-plus-terror-attacks.html> DOA: 4-25-15

Secret surveillance programs helped prevent more than 50 potential terror attacks worldwide, including plots to target the New York Stock Exchange and the city's subway, the director of the National Security Agency testified on Tuesday. **Ten of the 50 potential threats were domestic,** said Army General Keith B. Alexander. A hearing before the House Intelligence Committee sought to calm fears among the American public that the U.S. government spies on them unconstitutionally, and repeated assurances that none of the NSA surveillance programs can target U.S. citizens at home or abroad without a court order. “These programs are limited, focused and subject to rigorous oversight,” Alexander said.

Because of that, the civil liberties and privacy of Americans are not at stake, he added.

However, Bruce Fein, a specialist in constitutional law, said the NSA surveillance programs are unconstitutional because there is no demonstration of individualized suspicion, as required by the Fourth Amendment.

“The government has a burden to show some reasonable suspicion that someone being spied on is engaged in some wrongdoing before privacy can be invaded,” said Fein.

Nonetheless, the witnesses defended the NSA programs as legal and necessary because of the nature of the threat of terrorism.

“If you’re looking for a needle in a haystack, you have to get the haystack first,” testified Deputy Attorney General James Cole.

Alexander and other senior U.S. intelligence officials testified in response to details leaked by former NSA contractor Edward Snowden about how the agency gathers data.

The hearing reviewed NSA surveillance programs 215 and 702. Testimony said program 215 gathers data in bulk from various providers, such as Verizon, but does not look at content or names, while program 702 applies only to foreign citizens.

The leak has sparked a debate among the American public over what information the government should be able to collect to safeguard national security, and how it should be allowed to gather it.

A recent Pew poll shows that a slight majority of Americans think the NSA surveillance programs are acceptable.

Meanwhile, U.S. President Barack Obama's approval ratings have dropped over the past month.

Alexander linked the relative safety Americans have enjoyed since the 9/11 attacks directly to the NSA surveillance programs, but Fein said people's fears are being exploited.^[SEP] "Most people are risk-averse. They're easily frightened, and told they need to surrender their liberties in order to be safe, even if it's not true," Fein said.

The government has not provided any evidence that these programs are effective, he added. "It's just their say-so."

When questioned about whether the NSA surveillance programs previously collected any other information, Alexander said what they have and have not collected remains classified and cannot be discussed.

However, some **details about how the programs have stopped potential terror attacks would be presented** as early as Wednesday to U.S. lawmakers, he said.

The largely docile Congress expressed overall support for the NSA programs, with Rep. Michele Bachmann framing Snowden as a traitor.

"It seems to me that the problem here is that of an individual who worked within the system, who broke laws and who chose to declassify highly sensitive classified information," Bachmann said.

Alexander said they are investigating where security broke down, and how to provide better oversight for nearly 1,000 system administrators that can access classified information.

The leaks were viewed across the board as a threat to national security.

"These are egregious leaks... and now here we are talking about this in front of the world, so I think those leaks affect us," said Sean Joyce, deputy director of the FBI.

Only one member of the House Committee, Rep. Jim Himes, said he was troubled by what he called the historically unprecedented revelations revealed in the leaks.

"We know that when a capability exists, there's a potential for abuse... From time to time, it'll be abused."

Intelligence collection key to defeating Al Qaeda

Benjamin Wittenberg, Brookings, 2014, Senior Fellow in Governance Studies at the Brookings Institution. I co-founded and am Editor in Chief of *Lawfare*, a website devoted to sober and serious discussion of "Hard National Security Choices." I am the author or editor of several books on subjects related to law and national security: *Detention and Denial: The Case for Candor After Guantánamo* (2011), *Law and the Long War: The Future of Justice in the Age of Terror* (2008), and *Legislating the War on Terror: An Agenda for Reform* (2009). I have written extensively both on the AUMF and on NSA collection under various provisions of the Foreign Intelligence Surveillance Act (FISA).³ The views I am expressing here are my own, April 8, Prepared Statement, Is Al Qaeda Winning the Administration's

Counterterrorism Policy,"

<http://docs.house.gov/meetings/FA/FA18/20140408/102109/HHRG-113-FA18-Wstate-WittesB-20140408.pdf> DOA: 5-1-15

Yet in considering the question of the state of the U.S. confrontation with Al Qaeda, there is something to be said for considering these questions in conjunction with one another. These are, after all, two of the most important legal instruments in the struggle this committee is endeavoring to assess. One is the key legal authority for virtually every military action the United States undertakes in its military battle against Al Qaeda, its offshoots, and its affiliates. The other is the single most important legal authority the intelligence community has for collecting intelligence against the Al Qaeda target—not to mention other foreign targets of great national security significance. This intelligence is key to arrests and the thwarting of terrorist plots against the United States and its allies. It is also key to accurate and precise targeting judgments in lethal force operations.

Surveillance is one piece of the puzzle used to catch terrorists

General Keith Alexander, retired after 8 years as director of the NSA, May 15, 2014, New Yorker, <http://www.newyorker.com/online/blogs/newsdesk/2014/05/were-at-greater-risk-q-a-with-general-keith-alexander.html> DOA: 2-20-15

In January, President Obama claimed that the N.S.A. bulk-metadata program has disrupted fifty-four terrorist plots. Senator Patrick Leahy said the real number is zero. There's a big difference between fifty-four and zero. Those [fifty-four events] were plots, funding, and giving money—like the Basaaly Moalin case, where the guy is giving money to someone to go and do an attack. [Note: Moalin's case is awaiting appeal.] It's fifty-four different events like that, where two programs—the metadata program and the 702 program—had some play. I was trying to think of the best way to illustrate what the intelligence people are trying to do. You know "Wheel of Fortune"? Here's the deal: I'm going to give you a set of big, long words to put on there. Then I'm going to give you some tools to guess the words. You get to pick a vowel or a consonant—one letter. There's a hundred letters up there. You'll say, I don't have a clue. O.K., so you've used your first tool in analysis. What the intelligence analysts are doing is using those tools to build the letters, to help understand what the plot is. This is one of those tools. It's not the only tool. And, at times, it may not be the best tool. It evolved from 9/11, when we didn't have a tool that helped us connect the dots between foreign and domestic. Around 9/11, we intercepted some of [the hijackers'] calls, but we couldn't see where they came from. So guys like [Khalid al-]Mihdhar, [one of the 9/11 hijackers who was living] in California—we knew he was calling people connected to Al Qaeda in Yemen. But we thought he was in the Middle East. We had no way to connect the dots. If you rewound 9/11, what you would have done is tipped the F.B.I. that a guy who is planning a terrorist attack is in San Diego. You may have found the other three groups that were with him.

The DA has an invisible risk, every form of data collection is useful because they give fragments to prevent attacks

James Andrew Lewis 14, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies, December 2014, “Underestimating Risk in the Surveillance Debate,”

http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf

NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success. Success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture.

In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspects. The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.

Every instance of surveillance is a necessity

Jessica Zuckerman 13, policy analyst at the Heritage Foundation, et al, 7/22/13, “60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism,”
<http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism>

Maintain essential counterterrorism tools. Support for important investigative tools such as the PATRIOT Act is essential to maintaining the security of the U.S. and combating terrorist threats. Key provisions within the act, such as the roving surveillance authority and business records provision, have proved essential for thwarting terror plots, yet they require frequent reauthorization. In order to ensure that law enforcement and intelligence authorities have the essential counterterrorism tools they need, Congress should seek permanent authorization of the three sun setting provisions within the PATRIOT Act.[208] Furthermore, legitimate government surveillance programs are also a vital component of U.S. national security, and should be allowed to continue. Indeed, in testimony before the house, General Keith Alexander, the director of the National Security Agency (NSA), revealed that more than 50 incidents of potential terrorism at home and abroad were stopped by the set of NSA surveillance programs that have recently come under scrutiny. That said, the need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well.

Surveillance is key to preventing violence before it happens- here's an example

Inserra and Walters 4-8-15, Policy Analyst, Homeland Security and Cybersecurity, and Research Assistant

David and Riley, "65th Islamist Terrorist Plot or Attack Since 9/11: Persistent Terrorism Requires Constant Vigilance", <http://www.heritage.org/research/reports/2015/04/65th-islamist-terrorist-plot-or-attack-since-911-persistent-terrorism-requires-constant-vigilance>

Terrorist Plot Details: U.S. citizens Noelle "Najma Samaa" Velentzas and Asia "Murdiiyah" Siddiqui were arrested for willfully conspiring to use a weapon of mass destruction in the United States.^[2] Using the Internet and relevant books, the two roommates researched and obtained the items needed to create an explosive device made from propane tanks. Velentzas noted several weeks ago that there are more "opportunities of pleasing Allah" in the United States, implying that she intended to launch an attack on U.S. soil rather than going to fight overseas.^[3] An investigation revealed that both defendants took to Islamist ideology several years ago. Velentzas admired Osama bin Laden and his mentor Abdullah Azzam and had been obsessed with pressure-cooker bombs since the 2013 Boston Marathon bombings. She also considered herself a citizen of the Islamic State (ISIS). Siddiqui showed an interest in Islamist ideology even earlier. In 2006, she became close to a prominent figure in the al-Qaeda in the Arabian Peninsula terrorist group, Samir Khan, who died in 2011. In 2009, she wrote a poem for a magazine called Jihad Recollections and called for readers to engage in violent jihad. In 2010, she sent a letter of support to Mohamed Mohamud, who was arrested for attempting to detonate a car bomb in Portland, Oregon.^[4] Through an undercover agent, the FBI began tracking both Velentzas and Siddiqui in July 2014. About that time, the two women showed an increased interest in learning how to construct and detonate explosive devices within the United States. Velentzas and Siddiqui read about how to make homemade grenades, pipe bombs, and pressure-cooker bombs and on electrical currents and chemistry. Velentzas showed a growing interest in attacking police, military, and other government targets, and discussed how she and Siddiqui could defend themselves with concealed knives or with stolen weapons in the event they were arrested.^[5] Ultimately, the FBI acted because Velentzas and Siddiqui had not only acquired the materials necessary to build a bomb, including multiple propane canisters, but Siddiqui had indicated a desire to proceed with independent planning and plots. With the potential for a bomb to be built, the undercover agent unable to track the progress of the work, and Siddiqui and Velentzas's clear desire to attack the U.S., the FBI arrested them before harm could come to the public.^[6] Terrorism on the Rise: Of the 65 Islamist terrorist plots or attacks since 9/11, this marks the 54th homegrown terrorist plot, as both individuals were U.S. citizens who were radicalized in the U.S. This case is also the third terror plot in less than three months, indicating an uptick in Islamist terrorism. This may be due to the success of terrorist campaigns by ISIS and other terrorist organizations inspiring individuals to radicalize and act on those extremist beliefs.^[7] The past three terrorist plots have all expressed at least some, if not direct, allegiance to ISIS and a desire to help ISIS by attacking targets here in the U.S. With the trend of homegrown terrorism continuing to grow and the recent increase in terrorist plots, both here in the U.S. and across the West, the U.S. must redouble its efforts. Specifically, the U.S. should: Maintain essential counterterrorism tools. Support for important investigative tools is essential to maintaining the security of the U.S. and combating terrorist threats. Legitimate government surveillance programs are also a vital component of U.S. national security and should be allowed to continue. The need

for effective counterterrorism operations, however, does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well.Emphasize community outreach. Federal grant funds should be used to create robust community outreach capabilities in higher-risk urban areas. Importantly, these funds must not be used for political pork or so broadly used that they are no longer targeted at those communities at greatest risk. Such capabilities are key to building trust in local communities, and if the United States is to be successful in thwarting lone-wolf terrorist attacks, it must put effective community outreach operations at the tip of the spear. Develop a comprehensive counterterrorism strategy. Since the inspirational source of domestic radicalization and terrorism often lies overseas, battling violent Islamist extremism abroad must be addressed in concert with the challenges presented by the terrorism at home. To this end, Congress should ensure that the Administration has a comprehensive strategy for addressing violent Islamist extremism both at home and abroad. This includes working with allies to strengthen intelligence sharing and collaborative counterterrorism efforts.

Mass Surveillance Links

Mass surveillance has thwarted many attacks – more transparency of the programs makes attacks very likely

Nakashima 13 [Ellen Nakashima, national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. “Officials: Surveillance programs foiled more than 50 terrorist plots”, https://www.washingtonpost.com/world/national-security/officials-surveillance-programs-foiled-more-than-50-terrorist-plots/2013/06/18/d657cb56-d83e-11e2-9df4-895344c13c30_story.html, June 18th, 2013//Rahul]

The U.S. government’s sweeping surveillance programs have disrupted more than 50 terrorist plots in the United States and abroad, including a plan to bomb the New York Stock Exchange, senior government officials testified Tuesday. The officials, appearing before a largely friendly House committee, defended the collection of telephone and Internet data by the National Security Agency as central to protecting the United States and its allies against terrorist attacks. And they said that recent disclosures about the surveillance operations have caused serious damage. “We are now faced with a situation that, because this information has been made public, we run the risk of losing these collection capabilities,” said Robert S. Litt, general counsel of the Office of the Director of National Intelligence. “We’re not going to know for many months whether these leaks in fact have caused us to lose these capabilities, but if they do have that effect, there is no doubt that they will cause our national security to be affected.” The hearing before the House Intelligence Committee was the third congressional session examining the leaks of classified material about two top-secret surveillance programs by Edward Snowden, 29, a former NSA contractor and onetime CIA employee. Articles based on the material in The Washington Post and Britain’s Guardian newspaper have raised concerns about intrusions on civil liberties and forced the Obama administration to mount an aggressive defense of the effectiveness and privacy protections of the operations. Gen. Keith B. Alexander, the head of the NSA, told the committee that the programs had helped prevent “potential terrorist events over 50 times since 9/11.” He said at least 10 of the disrupted plots involved terrorism suspects or targets in the United States. Alexander said officials do not plan to release additional information publicly, to avoid revealing sources and methods of operation, but he said the House and Senate intelligence committees will receive classified details of the thwarted plots. Newly revealed plots In testimony last week, Alexander said the surveillance programs had helped prevent an attack on the subway system in New York City and the bombing of a Danish newspaper. Sean Joyce, deputy director of the FBI, described two additional plots Tuesday that he said were stopped through the surveillance — a plan by a Kansas City, Mo., man to bomb the New York Stock Exchange and efforts by a San Diego man to send money to terrorists in Somalia. The officials said repeatedly that the operations were authorized by Congress and subject to oversight through internal mechanisms and the Foreign Intelligence Surveillance Court, whose proceedings are secret. Alexander said that more than 90 percent of the information on the foiled plots came from a program targeting the communications of foreigners, known as PRISM. The program was authorized under Section 702 of a 2008 law that amended the Foreign Intelligence Surveillance Act (FISA). The law authorizes the NSA to collect e-mails and other Internet communications to and from foreign targets overseas who are thought to be involved in terrorism or nuclear proliferation or who might provide critical foreign intelligence. No American in the country or abroad can be targeted without a warrant, and no person inside the United States can be targeted without a warrant. A second program collects all call records from U.S. phone companies. It is authorized under Section 215 of the USA Patriot Act. The records do not include the content of calls, location data, or a subscriber’s name or address. That law, passed in 2001 and renewed twice since then, also amended FISA. Snowden, a high school dropout who worked at an NSA operations center in Hawaii for 15 months as a contractor, released highly classified information on both programs, claiming they represent government overreach. He has been in hiding since publicly acknowledging on June 9 that he leaked the material. Several lawmakers pressed for answers on how Snowden, a low-level systems administrator, could have had access to highly classified material such as a court order for phone records. “We need to seal this crack in the system,” said Rep. C.A. Dutch Ruppersberger (Md.), the ranking Democrat on the intelligence panel. Alexander said he is working with intelligence officials to come up with a “two-person” rule to ensure that the agency can block unauthorized people from removing information from the system. But Alexander and the other witnesses focused more heavily on justifying the programs and arguing that they operate under legal guidelines. “As Americans, we value our privacy and our civil liberties,” Alexander said. “As Americans, we also value our security and our safety. In the 12 years since the attacks on September 11th, we have lived in relative safety and security as a nation. That security is a direct result of the intelligence community’s quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11.”

Bulk surveillance is crucial to detect and act on threats – many examples prove

Hines 13 [Pierre Hines is a defense council member of the Truman National Security Project, “Here’s how metadata on billions of phone calls predicts terrorist attacks” <http://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks>, June 19th, 2013//Rahul]

Yesterday, when NSA Director General Keith Alexander testified before the House Committee on Intelligence, he declared that the NSA’s surveillance programs have provided “critical leads to help prevent over 50 potential terrorist events.” FBI Deputy Director Sean Boyce elaborated by describing four instances when the NSA’s surveillance programs have had an impact: (1) when an intercepted email from a terrorist in Pakistan led to foiling a plan to bomb of the New York subway system; (2) when NSA’s programs helped prevent a plot to bomb the New York Stock Exchange; (3) when intelligence led to the arrest of a U.S. citizen who planned to bomb the Danish Newspaper office that published cartoon depictions of the Prophet Muhammad; and (4) when the NSA’s programs triggered reopening the 9/11 investigation. So what are the practical applications of internet and phone records gathered from two NSA programs? And how can “metadata” actually prevent terrorist attacks? Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted. Section 215 of the Patriot Act provides the legal authority to obtain “business records” from phone companies. Meanwhile, the NSA uses Section 702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases. One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists’ planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat. Even more useful than hindsight is a crystal ball that gives the intelligence community a look into the future. Simply knowing how many individuals are in a chat room, how many individuals have contacted a particular phone user, or how many individuals are on an email chain could serve as an indicator of how many terrorists are involved in a plot. Furthermore, knowing when a suspect communicates can help identify his patterns of behavior. For instance, metadata can help establish whether a suspect communicates sporadically or on a set pattern (e.g., making a call every Saturday at 2 p.m.). Any deviation from that pattern could indicate that the plan changed at a certain point; any phone number or email address used consistently and then not at all could indicate that a suspect has stopped communicating with an associate. Additionally, a rapid increase in communication could indicate that an attack is about to happen. Metadata can provide all of this information without ever exposing the content of a phone call or email. If the metadata reveals the suspect is engaged in terrorist activities, then obtaining a warrant would allow intelligence officials to actually monitor the content of the suspect’s communication. In Gen. Alexander’s words, “These programs have protected our country and allies . . . [t]hese programs have been approved by the administration, Congress, and the courts.” Now, Americans will have to decide whether they agree.

Surveillance is necessary and has very little negative consequences on civil liberty

Boot 13 [Max Boot, Max Boot is an American author, consultant, editorialist, lecturer, and military historian, "Stay calm and let the NSA carry on", <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>, June 9th, 2015//Rahul]

After 9/11, there was a widespread expectation of many more terrorist attacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon bombing of), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's monitoring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terrorist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists. For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it. But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic, Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours. Which brings us to the current kerfuffle over two NSA monitoring programs that have been exposed by the Guardian and the Washington Post. One program apparently collects metadata on all telephone calls made in the United States. Another program provides access to all the emails, videos and other data found on the servers of major Internet firms such as Google, Apple and Microsoft. At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to "non-U.S. persons" who are abroad and thereby enjoy no constitutional protections. These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities. It's possible that, like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these

programs have been effective in disrupting terrorist plots. Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a "scandal," to use a term now loosely being tossed around. The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

Unwarranted domestic surveillance is the most significant anti-terror tool available- allows us to infiltrate terror groups and prevent weapons proliferation- has solved 53 of 54 suppressed terror attacks in recent years

Clarke et al 2013 [Report and Recommendations of the President's Review Group on Intelligence and Surveillance Technologies, "Liberty and Security in a Changing World", https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, Accessed 7/3/15, AX]

According to NSA, section 702 "is the most significant tool in NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world." To cite just one example, collection under section 702 "was critical to the discovery and disruption" of a planned bomb attack in 2009 against the New York City subway system and led to the arrest and conviction of Najibullah Zazi and several of his co-conspirators. According to the Department of Justice and the Office of the Director of National Intelligence in a 2012 report to Congress: Section 702 enables the Government to collect information effectively and efficiently about foreign targets overseas and in a manner that protects the privacy and civil liberties of Americans. Through rigorous oversight, the Government is able to evaluate whether changes are needed to the procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. In addition, the Department of Justice provides the joint assessments and other reports to the FISC. The FISC has been actively involved in the review of section 702 collection.

Together, all of these mechanisms ensure thorough and continuous oversight of section 702 activities. . . . Section 702 is vital to keeping the nation safe. It provides information about the plans and identities of terrorists allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States. In reauthorizing section 702 for an additional five years in 2012, the Senate Select Committee on Intelligence concluded: [T]he authorities provided [under section 702] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets. The Committee has also found that [section 702] has been implemented with attention to protecting the privacy and civil liberties of US persons, and has been the subject of extensive oversight by the Executive branch, the FISC, as well as the Congress. . . . [The] failure to reauthorize [section 702] would "result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities."¹⁴⁷ Our own review is not inconsistent with this assessment. During the course of our analysis, NSA shared with the Review Group the details of 54 counterterrorism investigations since 2007 that resulted in the prevention of terrorist attacks in diverse nations and the United States. In all but one of these cases, information obtained under section 702 contributed in some degree to the success of the investigation. Although it is difficult to assess precisely how many of these investigations would have turned out differently without the information learned through section 702, we are persuaded that section 702 does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe.

Meta-data has stopped terror attacks

Schwartz 15 [Mattathias Schwartz, 1-26-2015, staff writer for the New Yorker and won the 2011 Livingston Award for international reporting "How to Catch a Terrorist," New Yorker, http://www.newyorker.com/magazine/2015/01/26/whole-haystack_jf]

The N.S.A. asserts that it uses the metadata to learn whether anyone inside the U.S. is in contact with high-priority terrorism suspects, colloquially referred to as "known bad guys." Michael Hayden, the

former C.I.A. and N.S.A. director, has said, “We kill people based on metadata.” He then added, “But that’s not what we do with *this* metadata,” referring to Section 215.

Soon after Snowden’s revelations, Alexander said that the **N.S.A.’s surveillance programs have stopped “fifty-four different terrorist-related activities.” Most of these were “terrorist plots.”** Thirteen involved the United States. **Credit for foiling these plots**, he continued, was partly due to the **metadata program, intended to “find the terrorist that walks among us.”**

President Obama also quantified the benefits of the metadata program. That June, in a press conference with Angela Merkel, the German Chancellor, **Obama said, “We know of at least fifty threats that have been averted because of this information.”** He continued, **“Lives have been saved.”**

Even if terror is unlikely meta-data surveillance is worth it

Lake 2014 [Eli Lake, 2-17-2014, senior national-security correspondent for the Daily Beast, "Spy Chief: We Should've Told You We Track Your Calls," Daily Beast, <http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html> jf]

Clapper still defends the 215 program, too. **The storage of the phone records allows NSA analysts to connect phone numbers of suspected terrorists overseas to a possible network inside the United States.** Other U.S. intelligence officials say its real value is that **it saves work** for the FBI and the NSA **in tracking down potential leads by ruling out suspicious numbers quickly.**

In the interview **Clapper said the 215 program was not a violation the rights of Americans.** “For me it was not some massive assault on civil liberties and privacy because of what we actually do and the safeguards that are put on this,” he said. **To guard against perhaps these days low probability but a very (high) impact thing if it happens.** Clapper compared the 215 program to fire insurance. **I buy fire insurance** ever since I retired, the wife and I bought a house out here and we buy fire insurance every year. **Never had a fire. But I am not gonna quit buying my fire insurance,** same kind of thing.”

Meta Data is key to damage control after terrorist attacks

Lewis 14 [James Andrew Lewis, Director and Senior Fellow of the Technology and Public Policy Program at the CSIS, December 2014, "Underestimating Risk in the Surveillance Debate", Center for Strategic and International Studies, http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf pg 9 jf]

The most controversial aspect of the surveillance program involved metadata. Metadata is information describing a telephone call, such as the number from which the call was placed, the number called, and the date, time, and length of the call. The content of the phone call (e.g., the conversation) is not collected. No locational data is collected, although commentators seem confused on this point. **Metadata analysis gave NSA the ability to identify individuals in the United States** or individuals outside the United States **who are in contact with terrorist groups.**¹⁰ In 2012, NSA looked at 288 primary telephone numbers and through “call chaining”

analysis reviewed 6,000 other numbers connected to these primary numbers. The 288 people had some connection to terrorism and NSA looked at the 6,000 people with whom they talked to see if they were also involved. Metadata acquired and retained under Section 215 of the Patriot Act program could only be queried when there is "reasonable articulable suspicion" that a telephone number is associated with foreign terrorist organizations. If a query merits further investigation, which requires looking at either content of the individual unmaking the call, this requires a specific, individual court order based on probable cause. If there is one constitutional requirement that was not fully observed in the metadata program authorized under the Patriot Act, it was that search requires a warrant from a court rather than an internal approval by the executive branch agency itself.¹¹ This was a significant error. **The 215 program allows law enforcement and intelligence officials to determine if a terrorist event is an isolated incident or the first of a series of attacks, and whether the attacker is a "lone wolf" or connected to a larger terrorist organization. The most important decision in the immediate aftermath of an attack is whether the incident is the first of a series. If it is the first of a series of attacks, additional steps must be taken without delay**, such as closing airports and other transportation hubs, putting police forces around the country on high alert, and mobilizing law enforcement agencies to locate and arrest the other attackers. **These steps are both disruptive and expensive and knowing that they are not necessary provides immediate benefit.**

Surveillance necessary to prevent ISIS attacks

Guardian, June 22, 2014 , Isis threat justifies greater surveillance powers in UK, says Liam Fox

Former defence secretary says first duty of state is to protect citizens and public will accept greater monitoring powers

Britain's security services may need to be given greater powers of surveillance to monitor extremists from Isis when they return home to Britain from Iraq and Syria, the former defence secretary Liam Fox has said. A majority of people will accept that **an "ideological battle" means that the authorities will need greater powers to intercept the communications of extremists**, Fox said. The former defence secretary, who was speaking on the Andrew Marr Show on BBC1, said that Britain should offer to put its airbases at the disposal of the US to avoid "horrendous" situation in Iraq as Isis forces pose a threat to Baghdad. Fox said: "There are those who say if we don't get involved, if we hunker down then we will be fine. There will be no backlash. That is utterly, utterly wrong because the jihadists don't hate us because of what we do. They hate us because of who we are. We can't change that. It is our values and our history that they detest more than anything else." Fox said that the authorities could deprive British citizens returning from Syria and Iraq of their passports. But he said that **the greatest effort should go**

towards increasing the power of the state to monitor the communications of extremists. He said: "We have the security services to ensure that they [extremists] are watched and that they don't pose a greater threat." Asked whether the powers of the security services were insufficient, the former defence secretary said: "That is a real question that we are going to have to ask - whether the security services have adequate resources for an increased threat. "That is a question politicians will have to take into account in judgments on spending allocations but also do the powers they have reflect the increasing [threat]? You've got people in the light of Snowden saying that the state has too many powers and we have to restrict the powers of the state." Asked which powers the state should be given, Fox said: "The whole areas of intercept that need to be looked at. We have got a real debate, and it is a genuine debate in a democracy, between the libertarians who say the state must not get too powerful and pretty much the rest of us who say the state must protect itself." Asked whether this meant more surveillance and increasing the manpower of the security services, he said: "If required is **the first duty of the state to protect its citizens** ... it is a real worry and it is a problem that is going to be with us for a very long time. At heart it is an ideological battle and we have to realise that we have to win the ideological battle as well." The remarks by Fox suggests that some figures, particularly on the right, will use the success of extremists in Iraq to challenge the claim by Edward Snowden that the state has amassed too many powers of surveillance. Snowden leaked a series of NSA files to the former Guardian journalist Glenn Greenwald last year.

Five reasons 9-11 proves surveillance is needed to prevent terror attacks

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

The September 11 attacks were a vivid demonstration of the need for detailed information about the activities of potential terrorists. This was so for several reasons. First, some information, which could have been useful, **was not collected and other information, which could have helped to prevent the attacks, was not shared** among departments. **Second, the scale of damage that 21st-century terrorists can inflict is far greater than anything that their predecessors could have imagined. We are** no longer **dealing with** threats from firearms and conventional explosives, but with **the possibility of weapons of mass destruction, including nuclear devices and biological and chemical agents**. The damage that such attacks could inflict on the nation, measured in terms of loss of life, economic and social disruption, and the consequent sacrifice of civil liberties, is extraordinary. The events of September 11 brought this home with crystal clarity. **Third, 21st-century terrorists operate within a global communications network that enables them both to hide their existence from outsiders and to communicate with one another across continents at the speed of light**. Effective safeguards against terrorist attacks require the technological capacity to ferret out such communications in an international communications grid. **Fourth, many of the international terrorists that the United States and other nations confront today cannot realistically be deterred by the fear of punishment.** The conventional means of preventing criminal conduct—the fear of capture and subsequent punishment—has relatively little role to play in combating some contemporary terrorists. Unlike the situation during the Cold War, in which the Soviet Union was deterred from launching a nuclear strike against the United States in part by its fear of a retaliatory counterattack, the terrorist enemy in the 21st-century is not a nation state against which the

United States and its allies can retaliate with the same effectiveness. In such circumstances, detection in advance is essential in any effort to “provide for the common defence.” **Fifth, the threat of massive terrorist attacks involving nuclear, chemical, or biological weapons can generate a chilling and destructive environment of fear and anxiety among our nation’s citizens.** If Americans came to believe that we are infiltrated by enemies we cannot identify and who have the power to bring death, destruction, and chaos to our lives on a massive scale, and that preventing such attacks is beyond the capacity of our government, the quality of national life would be greatly imperiled. Indeed, **if a similar or even more devastating attack were to occur in the future, there would almost surely be an impulse to increase the use of surveillance technology to prevent further strikes, despite the potentially corrosive effects on individual freedom and self-governance.** In the years after the attacks of September 11, a former cabinet member suggested a vivid analogy. He compared “the task of stopping” the next terrorist attack “to a goalie in a soccer game who ‘must stop every shot,’” for if the enemy “‘scores a single goal,’” the terrorists succeed. To make matters worse, “‘the goalie cannot see the ball—it is invisible. So are the players—he doesn’t know how many there are, or where they are, or what they look like.’” Indeed, the invisible players might shoot the ball “from the front of the goal, or from the back, or from some other direction—the goalie just doesn’t know.’” Although the analogy might be overstated, it is no surprise that after the September 11, 2001 terrorist attacks the government turned to a much more aggressive form of surveillance in an effort to locate and identify potential terrorists and prevent future attacks before they could occur. One thing seemed clear: If the government was overly cautious in its efforts to detect and prevent terrorist attacks, the consequences for the nation could be disastrous.

Surveillance critical to disrupt clandestine terrorist operations

Report and Recommendations of the President’s Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf DOA: 1-1-14

In the American tradition, the word “security” has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. Thus understood, it signals the immense importance of counteracting threats that come from those who seek to do the nation and its citizens harm. **One of the government’s most fundamental responsibilities is to protect** this form of **security**, broadly understood. Appropriately conducted and properly disciplined, **surveillance can help to eliminate important national security risks. It has helped to save lives in the past.** It will help to do so in the future. In the aftermath of the terrorist attacks of September 11, 2001, it should not be necessary to belabor this point. **By their very nature, terrorist attacks tend to involve covert, decentralized actors who participate in plots that may not be easy to identify or disrupt. Surveillance can protect, and has protected, against such plots.**

The wider the surveillance net, the more effective the surveillance

Report and Recommendations of the President’s Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf DOA: 1-1-14

When public officials acquire information, they seek to reduce risks, above all risks to national security. **If the government is able to obtain access to a great deal of information, it should be in a better position to mitigate serious threats of violence. And if the goal is to reduce such threats, a wide net seems far better than a narrow one, even if the government ends up acquiring a great deal of information that it does not need or want.** As technologies evolve, it is becoming increasingly feasible to cast that wide net. In the future, the feasibility of pervasive surveillance will increase dramatically. From the standpoint of risk reduction, that prospect has real advantages.

NSA surveillance has disrupted more than 50 terror plots

USA Today, JUN 07, 2013, <http://www.usatoday.com/story/news/nation/2013/06/18/nsa-surveillance-secret-programs-terror-plots/2434193/> [SEP]

NSA: Surveillance foiled 50 terror plots By: Kevin Johnson, DOA: 1-1-14

Director says NYSE was among targets

Section: News, Pg. 05a

National Security Agency Director Keith Alexander told a House committee Tuesday that more than 50 terror threats throughout the world have been disrupted with the assistance of two secret surveillance programs that were recently disclosed by former defense contractor Edward Snowden. More than 10 of the plots targeted the U.S. homeland, Alexander told the House Intelligence Committee, including a plan to attack the New York Stock Exchange. "I would much rather be here today debating this," Alexander said, "than explaining why we were unable to prevent another 9/11" attack.

At the rare open committee hearing, **Alexander and Deputy Attorney General Jim Cole told lawmakers that both surveillance operations** -- a domestic telephone tracking system that collects records of millions of Americans and an Internet monitoring program targeting non-citizens outside the U.S. -- **have been subject to rigorous oversight to guard against privacy abuses. "This isn't some rogue operation that some guys at the NSA are operating."** Alexander said. Deputy FBI Director Sean Joyce told the committee about a threat that was neutralized by the programs: **Investigators used the phone-tracking system to identify an operative in San Diego who was providing support to terrorists in Somalia.**

Joyce also referred to two disrupted plots that were disclosed last week as having been thwarted by the surveillance operations, including a 2009 plan to bomb the New York subway system. In that case, authorities used NSA's Internet monitoring program to identify overseas communications involving Najibullah Zazi in Colorado, who was later convicted in connection with the subway attack plan.

"This is not a program that is off the books," Cole said, outlining the executive, legislative and judicial controls. In the plot against the stock exchange, Joyce said investigators identified a former New York accountant working with contacts in Yemen who were in the early stages of planning an assault. Joyce did not name the man. In court documents, however, he is identified as Sabirhan Hasanoff, 37, who pleaded guilty last year to providing support to al-Qaeda. Hasanoff

was not charged in a plot against the stock exchange, but prosecutors, while arguing for a harsh prison sentence, alleged in court documents that he "cased the New York Stock Exchange" at the direction of a terror leader in Yemen. Hasanoff's attorney was not immediately available for comment. Lawmakers raised few questions about the intelligence officials' authority to conduct the operations, despite the heated national privacy debate that was prompted by Snowden's disclosures. Rep. Mike Rogers, R-Mich., the panel's chairman, said the programs were "designed" to protect Americans. Maryland Rep. Dutch Ruppersberger, the committee's ranking Democrat, said Snowden's unauthorized disclosures "put our country and allies in danger."

Intelligence gathering critical to defeat terrorism

Paul Rosenzweig, Heritage Senior Legal Research Fellow, 2004

["The Patriot Act Reader," w/ Alane Kochems & James Jay Carafano, 9/20,
<http://www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=69895>]

As should be clear from the outline of the scope of the problem, the suppression of terrorism will not be accomplished by military means alone. Rather, effective law enforcement and/or intelligence gathering activity are the key to avoiding new terrorist acts. Recent history supports this conclusion. In fact, police have arrested more terrorists than military operations have captured or killed. Police in more than 100 countries have arrested more than 3,000 al-Qaeda-linked suspects, while the military captured some 650 enemy combatants. Equally important, it is policing of a different form—preventative rather than reactive, since there is less value in punishing terrorists after the fact when, in some instances, they are willing to perish in the attack. The foregoing understanding of the nature of the threat from terrorism helps to explain why the traditional law enforcement paradigm needs to be modified (or, in some instances, discarded) in the context of terrorism investigations. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that “it is better that 10 guilty go free than that one innocent be mistakenly punished.” This embodies a fundamentally moral judgment that when it comes to enforcing criminal law, American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives). That preference arises from two interrelated grounds. One is the historical distrust of government that, as already noted, animates many critics of the Patriot Act. But the other is, at least implicitly, a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common-sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity. The post-September 11th world changes this calculus in two ways. First, and most obviously, it changes the cost of the Type II errors. Whatever the cost of freeing mob boss John Gotti or sniper John Muhammad might be, they are substantially less than the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that “better 10 terrorists go free than that one innocent be mistakenly punished.” Second, and less obviously, it changes the nature of the Type I errors that must be considered. In the traditional law enforcement paradigm, the liberty interest at stake is personal liberty—that is, freedom from the unjustified application of governmental force. We have as a model the concept of an arrest, the seizure of physical evidence, or the search of a tangible place. As we move into the Information Age, and deploy new technology to assist in tracking terrorists, that model is no longer wholly valid.

General NSA Surveillance

Broad NSA access to US data is crucial to preventing terrorist attacks in the US – their authors vastly underestimate the probability of attack. You need to evaluate link through a very high probability of attempted attack

Lewis 14 (senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies)

(James Andrew, Underestimating Risk in the Surveillance Debate, http://csis.org/files/publication/141209_-Lewis_UnderestimatingRisk_Web.pdf)

Americans are reluctant to accept terrorism is part of their daily lives, but attacks have been planned or attempted against American targets (usually airliners or urban areas) almost every year since 9/11. Europe faces even greater risk, given the thousands of European Union citizens who will return hardened and radicalized from fighting in Syria and Iraq. The threat of attack is easy to exaggerate, but that does not mean it is nonexistent. Australia's then-attorney general said in August 2013 that communications surveillance had stopped four "mass casualty events" since 2008. The constant planning and preparation for attack by terrorist groups is not apparent to the public. The dilemma in assessing risk is that it is discontinuous. There can be long periods with no noticeable activity, only to have the apparent calm explode. The debate over how to reform communications surveillance has discounted this risk. Communications surveillance is an essential law enforcement and intelligence tool. There is no replacement for it. Some suggestions for alternative approaches to surveillance, such as the idea that the National Security Agency (NSA) only track known or suspected terrorists, reflect wishful thinking, as it is the unknown terrorist who will inflict the greatest harm.

The Evolution of Privacy Some of the unhappiness created by the Edward Snowden leaks reflects the unspoken recognition that online privacy has changed irrevocably. The precipitous decline in privacy since the Internet was commercialized is the elephant in the room we ignore in the surveillance debate. America's privacy laws are both limited in scope and out of date. Although a majority of Americans believe privacy laws are inadequate, the surveillance debate has not led to a useful discussion of privacy in the context of changed technologies and consumer preferences. Technology is more intrusive as companies pursue revenue growth by harvesting user data. Tracking online behavior is a preferred business model. On average, there are 16 hidden tracking programs on every website. The growing market for "big data" to predict consumer behavior and target advertising will further change privacy. Judging by their behavior, Internet users are willing to exchange private data for online services. A survey in a major European country found a majority of Internet users disapproved of Google out of privacy concerns, but more than 80 percent used Google as their search engine. The disconnect between consumer statements and behavior reduces the chances of legislating better protections. We have global rules for finance and air travel, and it is time to create rules for privacy, but governments alone cannot set these rules, nor can a single region impose them. Rules also need to be reciprocal. NSA bears the brunt of criticism, but its actions are far from unique. All nations conduct some kind of communications surveillance on their own populations, and many collect against foreign targets. Getting this consensus will be difficult. There is no international consensus on privacy and data protection. EU efforts to legislate for the entire world ignore broad cultural differences in attitudes toward privacy, and previous EU privacy rules likely harmed European companies' ability to innovate. Finding a balance between privacy, security, and innovation will not be easy since unconstrained collection creates serious concerns while a too restrictive approach threatens real economic harm. Espionage and Counterterrorism NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success. Success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture. In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspects. The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this. Spying on Allies NSA's mass surveillance programs for counterterrorism were carried out in cooperation with more than 30 countries. Unilateral U.S. collection programs focused on national security problems: nonproliferation, counterintelligence (including Russian covert influence operations in Europe), and arms sales to China. The United States failed to exercise sufficient oversight over intelligence collection, but the objectives set for NSA reflect real security problems for the United States and its allies. The notion that "friends don't spy on friends" is naive. The United States has friends that routinely spy on it and yet are strong security partners. Relations among powerful states are complex and not explained by simple bromides drawn from personal life. The most startling thing about U.S. espionage against Germany was the absence of a strategic calculation of risk and benefit. There are grounds for espionage (what other major power has a former leader on Russia's payroll?), but the benefits were outweighed by the risk to the relationship. The case for spying on Brazil is even weaker. While Brazil is often antagonistic, it poses no risk to national security. If economic intelligence on Brazil is needed, the private sector has powerful incentives and legitimate means to obtain

information and usually has the best data. Risk Is Not Going Away Broad surveillance of communications is the least intrusive and most effective method for discovering terrorist and espionage activity.

Many countries have expanded surveillance programs since the 9/11 attacks to detect and prevent terrorist activity, often in cooperation with other countries, including the United States. Precise metrics on risk and effectiveness do not exist for surveillance, and we are left with conflicting opinions from intelligence officials and civil libertarians as to what makes counterterrorism successful. Given resurgent authoritarianism and continuing jihad, the new context for the surveillance debate is that the likelihood of attack is increasing. Any legislative change should be viewed through this lens.

Err Neg on the link – your default assumption should be that changing intel gathering could have big security risks.

Clarke '13

(et al; This is the Final Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. President Obama ordered a blue-ribbon task force to review domestic surveillance. This report releases the findings of that group. The report was headed by five experts – including Richard Alan Clarke, who is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. Other expert contributors include Michael Joseph Morell, who was the deputy director of the Central Intelligence Agency and served as acting director twice in 2011 and from 2012 to 2013 and Cass Robert Sunstein, who was the Administrator of the White House Office of Information and Regulatory Affairs in the Obama administration and is currently a Professor of Law at Harvard Law School. "LIBERTY AND SECURITY IN A CHANGING WORLD" – December 12th, 2013 – Easily obtained via a google search.
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=https%3A%2F%2Fwww.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fdocs%2F2013-12_12_rg_final_report.pdf&ei=Db0yVdDjKIKdNtTXgZgE&usg=AFQjCNH0S_Fo9dckL9bRarVpi4M6pq6MQ&bvm=bv.91071109,d.eXY

Most of these **challenges have a significant intelligence component.** Policymakers cannot understand the issues, cannot make policy with regard to those issues, and cannot successfully implement that policy without reliable intelligence. Any expert with access to open sources can provide insight on questions such as the Eurozone crisis and Japanese politics, but **insights on the plans, intentions, and capabilities of al-Qa'ida,** on the status of the Iranian nuclear weapons program, **and** on the development of **cyber warfare tools** by other nations **are simply not possible without reliable intelligence.** A wide range of intelligence collectors, including NSA, **have made important contributions to protecting the nation's security.** Notwithstanding recent controversies, and the importance of significant reforms, **the national security of the United States depends on the continued capacity of** NSA and other agencies to collect essential information. In considering proposals for reform now and for the future, **policymakers should avoid the risk of overreaction** and take care in making changes that could undermine the capabilities of the Intelligence Community.

Bulk Collection

Plan limits bulk collection programs. That increases terror risk. Claims that “bulk programs haven’t stopped an attack” are naïve.

Lewis ‘14

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy. Before joining CSIS, he worked at the US Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His diplomatic experience included negotiations on military basing in Asia, the Cambodia peace process, and the five-power talks on arms transfer restraint. Lewis received his Ph.D. from the University of Chicago. “*Underestimating Risk in the Surveillance Debate*” - CENTER FOR STRATEGIC & INTERNATIONAL STUDIES - STRATEGIC TECHNOLOGIES PROGRAM – December - <http://csis.org/publication/underestimating-risk-surveillance-debate>

NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence. Intelligence does not work as it is portrayed in films – solitary agents do not make startling discoveries that lead to dramatic, last-minute success. Success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture. In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspect. The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.

Storage, Super minimization

Plan “super-minimizes” data storage. But, historical analysis key to check sleeper cells

Shea ‘14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director’s Fellow. Since her tour as a Director’s Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda’s Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with “I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge”. Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

50. Specifically, when the NSA performs a contact-chaining query on a terrorist associated telephone identifier, it is able to detect not only the further contacts made by that first tier of contacts, but the additional tiers of contacts, out to the maximum number of permitted "hops" from the original identifier. The collected metadata thus holds contact information that can be immediately accessed as new terrorist-associated telephone identifiers are identified. Multi-tiered contact chaining identifies not only the terrorist's direct associates but also indirect associates, and, therefore provides a more complete picture of those who associate with terrorists and/or are engaged in terrorist activities. 51. Another advantage of the metadata collected in this matter is that it is historical in nature, reflecting contact activity from the past. Given that terrorist operatives often lie dormant for extended periods of time, historical connections are critical to understanding a newly identified target, and metadata may contain links that are unique pointing to potential targets that may otherwise be missed.

Data must be *Aggregated*

Individual company data can't solve – multi-company data must be aggregated

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

49. An advantage of bulk metadata analysis as applied to telephony metadata, which is interconnected in nature, is that it enables the Government to quickly analyze past connections and chains of communication. Unless the data is aggregated, it may not be feasible to detect chains of communications that cross communication networks. The ability to query accumulated telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations who might otherwise go undetected.

Meta-data must be aggregated. Alternatives hamper counter-terror efforts.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth*

Circuit Court of Appeals. Her testimony concludes with “I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge”. Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

63. If the telephony metadata are not aggregated and retained for a sufficient period of time, it will not be possible for the NSA to detect chains of communications that cross different providers and telecommunications networks. But for the NSA's metadata collection, the NSA would need to seek telephonic records from multiple providers whenever a need to inquire arose, and each such provider may not maintain records in a format that is subject to a standardized query. 64. Thus, the Government could not achieve the aforementioned benefits of Section 215 metadata collection through alternative means.

Link Wall – Detection

() Meta-data boost terror detection – it's a vital complimentary tool.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

53. Furthermore, the Section 215 metadata program complements information that the NSA collects via other means and is valuable to NSA, in support of the FBI, for linking possible terrorist-related telephone communications that occur between communicants based solely inside the U.S. 54. As a complementary tool to other intelligence authorities, the NSA's access to telephony metadata improves the likelihood of the Government being able to detect terrorist cell contacts within the U.S. With the metadata collected under Section 215 pursuant to FISC orders, the NSA has the information necessary to perform the call chaining that can enable NSA intelligence analysts to obtain a much fuller understanding of the target and, as a result, allow the NSA to provide FBI with a more complete picture of possible terrorist-related activity occurring inside the U.S.

Video Surveillance Links

Video surveillance essential to defeat terrorism

St. Louis Dispatch, August 13, 2013, "The Role of Surveillance Cameras in the War on Terror," <http://www.gopusa.com/news/2013/04/22/the-role-of-surveillance-cameras-in-crime-or-terror/> DOA: 5-1-15

Mere hours after the public release of grainy surveillance camera images in the Boston Marathon bombings, law enforcement officials had pinpointed suspects in one of the nation's most horrific terrorist acts. It was a stunning and swift break in the case, one that illustrates the potency surveillance photos have for the public and police in solving crime. For Howard Richards, the images captured in Boston are validation of a three-year project in St. Louis to link 150 surveillance cameras into a single security system throughout the city's central corridor, from the riverfront to Forest Park. **"Without those images, they would not have been able to solve this thing as quickly, there are no two ways about it,"** **Richards said of the Boston case.** "You can't overestimate the value of this technology." Richards is head of security at Harris-Stowe State University and chairs monthly meetings of the Central Corridor Security Group, formed about three years ago to address security issues. The group eventually brought on United for a Better St. Louis, a nonprofit organization formed in 2011 to enhance public safety efforts, to lead a fundraising campaign.

The St. Louis project would form a common network out of cameras owned and operated by a host of entities, such as the city's port authority and street department, the Partnership for Downtown St. Louis, the Locust Business District and the Central West End. The security system, which organizers hope to have in place in about three months, would equip police with tablet computers and software allowing officers to look through any of the cameras on the network. With newer cameras, police would be able to zoom, pan and tilt to get a better view. "It's going to make us cutting-edge and on board with other big cities in the country," said Michael Gerdine, a chiropractor and chairman of United for a Better St. Louis. Cities such as Baltimore, Chicago, Atlanta and Dallas use the technology, and their systems have been reviewed for the St. Louis project. New York operates a "Ring of Steel" that trains an estimated 3,000 cameras in Lower Manhattan. Boston has a network of cameras throughout its city and transit system. London -- known for its ubiquitous security cameras -- has also seen how **surveillance images can lead to a swift resolution to terrorism investigations.** In 2005, terrorism suspects were quickly identified with such images. Weeks later, a failed group of bombers was also caught, thanks to the cameras. In Baltimore, the cameras have been a valuable tool in prosecuting crimes, and have been successful in reducing crime in trouble spots, said Baltimore police spokesman Anthony Guglielmi. "We love them. It's a really great system," Guglielmi said. Still, he said, "they are in no way designed to replace those on patrol." Research further backs up the value that surveillance cameras have in solving crime. In St. Louis, the project grew out of meetings between members of the Locust Business District and the Downtown Partnership over security concerns. **Expanding and linking camera systems was proposed as a way to not only help solve crime, but prevent it.** From those early discussions, the Central Corridor Security Group was formed. The group's board includes representatives of the Downtown Partnership,

Grand Center Inc., St. Louis University and Barnes-Jewish Hospital. Two St. Louis police captains are on the board. Representatives of Metro, Sigma-Aldrich and Wells Fargo also attend meetings. Maggie Campbell, president of the Partnership for Downtown St. Louis, said live monitoring of cameras has been happening downtown for about five years. "But if we can grow it and leverage it with our neighboring business districts, then we can make it work better for everyone," she said. "It's all about multiplying the eyes that are watching." No public funds are being sought in the startup of the program, and the cameras would be limited to public areas. "We all decided it would be a good idea to basically look out for each other," Richards said. But increasing cameras and the number of people allowed to monitor them concerns privacy advocates.

Surveillance cameras critical to defeat terrorism

Farhad Manjo, April 18, 2013, Slate, We Need More Cameras and We Need them Now,"
http://www.slate.com/articles/technology/technology/2013/04/boston_bomber_photos_the_marathon_bombing_shows_that_we_need_more_security.html DOA: 4-5-15

Though DesLauriers did not indicate the source of the images, the **Boston Globe** reported earlier that authorities were focusing on video "from surveillance cameras on the same side of Boylston Street as the explosions." If it turns out that the people in the FBI's photos are the guys who did it, they shouldn't be surprised that surveillance cameras turned out to be their undoing. Neither should you. We should see this potential **break in the case as a sign of the virtues of video surveillance**. More than that, we should think about **how cameras could help prevent crimes, not just solve them once they've already happened**. Cities under the threat of terrorist attack should install networks of cameras to monitor everything that happens at vulnerable urban installations. Yes, you don't like to be watched. Neither do I. But of all the measures we might consider to improve security in an age of terrorism, installing surveillance cameras everywhere may be the best choice. They're cheap, less intrusive than many physical security systems, and—as will hopefully be the case with the Boston bombing—they can be extremely effective at solving crimes. Surveillance cameras aren't just the bane of hardcore civil libertarians. The idea of submitting to constant monitoring feels wrong, nearly un-American, to most of us. Cameras in the sky are the ultimate manifestation of Big Brother—a way for the government to watch you all the time, everywhere. In addition to normalizing surveillance—turning every public place into a venue for criminal investigation—there's also the potential for abuse. Once a city is routinely surveilled, the government can turn every indiscretion into a criminal matter. You used to be able to speed down the street when you were in a hurry. Now, in many places around the world, a speed camera will record your behavior and send you a ticket in the mail. Combine cameras with facial-recognition technology and you've got a recipe for governmental intrusion. Did you just roll a joint or jaywalk or spray-paint a bus stop? Do you owe taxes or child support? Well, prepare to be investigated—if not hassled, fined, or arrested. These aren't trivial fears. The costs of ubiquitous surveillance are real. But these are not intractable problems. Such abuses and slippery-slope fears could be contained by regulations that circumscribe how the government can use footage obtained from security cameras. In general, we need to be thinking about ways to make cameras work for us, not reasons to abolish them. **When**

you weigh cameras against other security measures, they emerge as the least costly and most effective choice. In the aftermath of 9/11, we've turned most public spaces into fortresses—now, it's impossible for you to get into tall buildings, airports, many museums, concerts, and even public celebrations without being subjected to pat-downs and metal detectors. When combined with competent law enforcement, surveillance cameras are more effective, less intrusive, less psychologically draining, and much more pleasant than these alternatives. As several studies have found, **a network of well-monitored cameras can help investigators solve crimes quickly, and there's even evidence that cameras can help deter and predict criminal acts, too.**

Surveillance cameras necessary to counter terrorism

Charlie Savage, August 12, 2007, "US doles out millions for street cameras, local efforts raise privacy concerns," Boston Globe,
http://www.boston.com/news/nation/articles/2007/08/12/us_doles_out_millions_for_street_cameras/?page=full DOA: 5-1-15

The Department of Homeland Security is funneling millions of dollars to local governments nationwide for purchasing high-tech video camera networks, accelerating the rise of a "surveillance society in which the sense of freedom that stems from being anonymous in public will be lost, privacy rights advocates warn. Since 2003, the department has handed out some \$23 billion in federal grants to local governments for equipment and training to help combat terrorism. Most of the money paid for emergency drills and upgrades to basic items, from radios to fences. But **the department also has doled out millions on surveillance cameras**, transforming city streets and parks into places under constant observation. The department will not say how much of its taxpayer-funded grants have gone to cameras. But a Globe search of local newspapers and congressional press releases shows that **a large number of new surveillance systems**, costing at least tens and probably hundreds of millions of dollars, are being **simultaneously installed around the country as part of homeland security grants**. In the last month, cities that have moved forward on plans for surveillance networks financed by the Homeland Security Department include St. Paul, which got a \$1.2 million grant for 60 cameras for downtown; Madison, Wis., which is buying a 32-camera network with a \$388,000 grant; and Pittsburgh, which is adding 83 cameras to its downtown with a \$2.58 million grant. Small towns are also getting their share of the federal money for surveillance to thwart crime and terrorism. Recent examples include Liberty, Kan. (population 95), which accepted a federal grant to install a \$5,000 G2 Sentinel camera in its park, and Scottsbluff, Neb. (population 14,000), where police used a \$180,000 Homeland Security Department grant to purchase four closed-circuit digital cameras and two monitors, a system originally designed for Times Square in New York City. "We certainly wouldn't have been able to purchase this system without those funds," police Captain Brian Wasson told the Scottsbluff Star-Herald. Other large cities and small towns have also joined in since 2003. Federal money is helping New York, Baltimore, and Chicago build massive surveillance systems that may also link thousands of privately owned security cameras. Boston has installed about 500 cameras in the MBTA system, funded in part with homeland security funds. Marc Rotenberg, director of the Electronic Privacy Information Center, said Homeland Security Department is the primary driver in spreading surveillance cameras, making their adoption more attractive by offering federal money to city and state leaders. Homeland Security Department spokesman Russ Knocke said that it is difficult to say how much money has been spent on surveillance cameras because many grants awarded to states or cities contained money for cameras and other equipment. Knocke defended **the funding of video networks as a valuable tool for protecting the nation.** "We will encourage their use in the future," he added. But privacy rights advocates say that the technology is putting at risk something that is hard to define but is core to personal autonomy. The proliferation of cameras could mean that Americans will feel less free because legal public behavior -- attending a political rally, entering a doctor's office, or even joking with friends in a park -- will leave a permanent record, retrievable by authorities at any time. Businesses and government buildings have used closed-circuit cameras for decades, so it is nothing new to be videotaped at an ATM machine. But technology specialists say the growing surveillance networks are potentially more powerful than anything the public has experienced. Until recently, most surveillance cameras produced only grainy analog feeds and had to be stored on bulky videotape cassettes. But the new, cutting-edge cameras produce clearer, more

detailed images. Moreover, because these videos are digital, they can be easily transmitted, copied, and stored indefinitely on ever-cheaper hard-drive space. In addition, police officers cannot be everywhere at once, and in the past someone had to watch a monitor, limiting how large or powerful a surveillance network could be. But technicians are developing ways to use computers to process real-time and stored digital video, including license-plate readers, face-recognition scanners, and software that detects "anomalous behavior." Although still primitive, these technologies are improving, some with help from research grants by the Homeland Security Department's Science and Technology Directorate. "Being able to collect this much data on people is going to be very powerful, and it opens people up for abuses of power," said Jennifer King, a professor at the University of California at Berkeley who studies privacy and technology. "The problem with explaining this scenario is that today it's a little futuristic. [A major loss of privacy] is a low risk today, but five years from now it will present a higher risk." As this technological capacity evolves, it will be far easier for individuals to attract police suspicion simply for acting differently and far easier for police to track that person's movement closely, including retracing their steps backwards in time. It will also create a greater risk that the officials who control the cameras could use them for personal or political gain, specialists said. The expanded use of surveillance in the name of fighting terrorism has proved controversial in other arenas, as with the recent debate over President Bush's programs for eavesdropping on Americans' international phone calls and e-mails without a warrant. But public support for installing more surveillance cameras in public places, both as a means of fighting terrorism and other crime, appears to be strong. Last month, an ABC News/Washington Post poll found that 71 percent of Americans favored increased use of surveillance cameras, while 25 percent opposed it.

Video surveillance necessary to defeat terrorism

Steven Simon is an adjunct senior fellow in Middle Eastern Studies at the Council on Foreign Relations and the co-author of "The Age of Sacred Terror" and "The Next Attack.", Times Square, Bombs, and Big Crowds, New York Times,
http://roomfordebate.blogs.nytimes.com/2010/05/03/times-square-bombs-and-big-crowds/?_r=0#steven DOA: 5-5-15

Video surveillance would not have stopped the Times Square attack. Does this mean that it would be useless? Not necessarily. Swift and accurate analysis of video surveillance information might prevent the next attack, even if it is powerless to stop the last one. Imagery can be used to assist in the identification and location of individuals at the scene of the crime. It can also be used to track the progress of the bomb-laden vehicle from its point of origin, or the point at which the truck was weaponized, to the place the terrorists have targeted. In combination with physical evidence acquired from the vehicle — fingerprints, hair, cloth fibers, soil, trash, forgotten personal items or a host of other bits of evidence — video surveillance can lead to the arrest of the bombers and to the unraveling of cells or networks and, if the attackers are foreign, the ratlines they exploited to enter the country. At this point, the U.S. does not have the kind of pervasive surveillance systems in place that, say, the British have deployed. In the U.K., there is about one surveillance camera for every thousand residents. It took British authorities years to reach this level of intensive surveillance. The U.S., as anyone who follows the debate over privacy loss in this country knows, is studded with cameras, but most of these are in stores to track consumption habits to facilitate marketing or deter shoplifters. They're not where they're needed, which is on the street. The two smallest jurisdictions in the U.K., very rural areas indeed, together deploy more surveillance cameras than the San Francisco police department. The U.S., of course, does not have to match Britain camera for camera. Surveillance can be enhanced in areas that are assessed to be likely targets, a category that can be inferred, at least in a general sense, from targeting patterns and what the terrorists actually have said about the desirability of attacking this or that; and they do discuss this in their literature and on their Web sites. More problematic, is the need to organize our law enforcement capabilities in ways that enable this visual information to be exploited effectively, while protecting the rapidly fading privacy available to ordinary citizens. Therein lies the real challenge.

Warrant Requirement Links

Warrantless surveillance necessary to combat Al Qaeda

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 903-4

It is al Qaeda's nature as a decentralized network that stresses the normal division between military and intelligence surveillance and the warrant-based approach of the criminal justice system. The Constitution vests the President with the executive power and designates him Commander-in-Chief. The Framers understood these powers to invest the executive with the duty to protect the nation from foreign attack and the right to control the conduct of military hostilities. **To exercise those powers effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy.** Regular **military intelligence need not follow standards of probable cause for a warrant or reasonableness for a search,** just as the use of force against the enemy does not have to comply with the Fourth Amendment. **During war, military signals intelligence might throw out a broad net to capture all communications within a certain area or by an enemy nation. Unlike the criminal justice system, which seeks to detain criminals, protection of national security need not rest on particularized suspicion of a specific individual.**

Warrant requirement for national security decisions undermines executive power needed for effective surveillance

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 904

This approach applies to national security activity that occurs within the United States as well as outside it. **In 1972, the Supreme Court refused to subject surveillance for national security purposes to the Fourth Amendment warrant requirement.** But it has extended this protection to purely domestic terrorist groups, out of concern that the government might use its powers to suppress political liberties. Lower **courts**, however, **have found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement.** In a leading 1980 case, the Fourth Circuit held that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities." **A warrant requirement for national security searches would reduce the flexibility of the executive branch, which possesses "unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance" and is "constitutionally designated as the pre-eminent authority in foreign affairs.** A warrant requirement would place national security

decisions in the hands of the judiciary, which "is largely inexperienced in making the delicate and complex decisions that lie behind foreign **intelligence surveillance.**" Under this framework, Presidents conducted national security surveillance using their executive authority for decades. President Nixon's abuses, however, led Congress to enact the Foreign Intelligence Surveillance Act (FISA) in 1978. FISA replaced presidentially-ordered monitoring of national security threats with a system similar to that used by law enforcement to conduct electronic surveillance of criminal suspects, but with important differences to protect classified information. FISA requires the government to show "probable cause" that a target is "an agent of a foreign power," which includes terrorist groups. A special court of federal district judges, the Foreign Intelligence Surveillance Court (FISC), examines classified information in a closed, ex parte hearing before issuing the warrant.

Stricter Court Review

Stricter Court review Link. Plan imposes stricter law enforcement warrants on intel agencies. That slows counter-terror operations to the point of failure. Yoo, 13

John Yoo. Alma mater: Harvard University (B.A. 1989), Yale Law School (J.D. 1992). Yoo has been a professor at the University of California, Berkeley, School of Law since 1993. "Ending NSA Surveillance is not the answer". National Review - 8/16/13 - www.nationalreview.com/corner/356027/ending-nsa-surveillance-not-answer-john-yoo

We should be careful not to put the NSA in an impossible position. Of course, we should be vigilant against the administrative state in all of its tangled tendrils, especially its collection of taxes (the IRS scandal) and enforcement of the laws (Obama's refusal to enforce Obamacare and immigration law). The problem here, however, is that we are placing these kinds of domestic law-enforcement standards on a foreign intelligence function. With domestic law enforcement, we want the Justice Department to monitor one identified target (identified because other evidence gives probable cause that he or she has already committed a crime) and to carefully minimize any surveillance so as not to intrude on privacy interests. Once we impose those standards on the military and intelligence agencies, however, we are either guaranteeing failure or we must accept a certain level of error. If the military and intelligence agencies had to follow law-enforcement standards, their mission would fail because they would not give us any improvement over what the FBI could achieve anyway. If the intelligence community is to detect future terrorist attacks through analyzing electronic communications, we are asking them to search through a vast sea of e-mails and phone-call patterns to find those few which, on the surface, look innocent but are actually covert terrorist messages. If we give them broader authority, we would have to accept a level of error that is inherent in any human activity. No intelligence agency could perform its mission of protecting the nation's security without making a few of these kinds of mistakes. The question is whether there are too many, not whether there will be any at all. Domestic law enforcement makes these errors too. Police seek warrants for the wrong guy, execute a search in the wrong house, arrest the wrong suspect, and even shoot unarmed suspects. We accept these mistakes because we understand that no law-enforcement system can successfully protect our communities from crime with perfection. The question is the error rate, how much it would cost to reduce it, the impact on the effectiveness of the program, and the remedies we have for mistakes. Consider those questions in the context of the NSA surveillance program. The more important question is not the top of the fraction but the bottom — not just how many mistakes occurred, but how many records were searched overall. If there were 2,000 or so mistakes, as the Washington Post suggests, but involving billions of communications, the error rate is well less than 1 percent. Without looking at the latest figures, I suspect that is a far lower error rate than those turned in by domestic police on searches and arrests. To end the NSA's efforts to intercept terrorist communications would be to willfully disregard the most valuable intelligence sources on al-Qaeda (now that the president won't allow the capture and interrogation of al-Qaeda leaders). The more useful question is whether there is a cost-effective way to reduce the error rate without detracting from the effectiveness of the program, which, by General Keith Alexander's accounting, has been high. Increasing judicial oversight might reduce errors — though I am dubious — but in a way that would seriously slow down the speed of the program, which is all-important if the mission is to stop terrorists. And perhaps Congress should think about ways to remedy any privacy violations in the future. But to end the program because it does not have an error rate of zero is to impose a demand on the NSA that no other government program, foreign or domestic, military or civilian, could survive.

Internet Surveillance

Terrorists coordinate and plan attacks over the internet – empirics prove Janbek, Ph.D, and Williams 14

(Williams and Valerie, Spring/Summer Ed. The Brown Journal of World Affairs, 20.2, "The Role of the Internet in post-9/11 Terrorism and Counterterrorism,")

Since 9/11, extremists have utilized the Internet in many ways such as inspiring potential recruits through online communication and mobilizing them to act on radical ideology. In addition to aiding the planning and execution of terrorist attacks, one of the Internet's most common uses today by terrorists is as a database of information to learn more about terrorist organizations and their causes. The use of the Internet as a communication medium by terrorists has historically taken place prior to terrorist attacks themselves. Extremists or potential terrorists use the Internet to frequent online extremist forums and websites. These websites usually offer a significant amount of information-including organizations' missions, doctrines, and histories-to their visitors, allowing terrorist organizations to communicate detailed information about themselves to potential recruits.¹ The organizations communicate their version of reality and how they perceive the world. In many cases, they specify who their enemies are and justify the use of violence against them, often while boasting about previous operations against enemies that were allegedly successful. Photos and videos of specific terrorist operations ensure that the websites remain entertaining and engaging for their audiences. Through personally maintaining their online presence, terrorist organizations are able to communicate directly with their target audiences without their message being distorted by mainstream media. Extremist websites and forums are maintained by sympathizers who are responsible for posting relevant content. Mohamed Jarmoune, a Moroccan-Italian in his twenties, was accused in 2012 of using his web skills to disseminate terrorist propaganda. Jarmoune "spent all his time up to 15 hours a day online, disseminating jihadist materials and connecting with interested individuals around the world."² Additionally, he administered a Facebook group that showed that he agreed with jihadist ideology. Similarly, Babar Ahmad and Syed Talha Ahsan, two British citizens, maintained a family of websites operating out of London known as Azzam Publications.³ The sites were utilized to solicit funds, personnel, and physical items like gas masks for the Taliban and other groups. The websites featured instructional training articles, biographies of mujahideen, as well as audio and video products for sale. The videos included actual footage of combat and deceased extremists. Ahmad and Ahsan's cases have been ongoing since 2004 and 2006 respectively. In a similar case in Sweden, Swedish citizen Oussama Kassir, who was hoping to establish a jihad training camp in Oregon, operated six websites since December 2001 that presented "instructions about how to make bombs and poisons."⁴ Kassir was a fan of Osama bin Laden and had previously received jihadist training in Pakistan.⁵ These cases serve as examples of how the Internet has been used by jihadist sympathizers to assist terrorist organizations in spreading their ideology online. The Internet also serves as a networking tool for extremists to connect with like-minded individuals or even leaders with whom they can discuss their ideologies. Such is the case of Major Nidal Malik Hasan, who communicated with the infamous American-born Muslim cleric Anwar al-Awlaki.⁶ Al-Awlaki represents a modern-day terrorist. He utilized online publications and videos, as well as individual emails, to recruit potential terrorists. During his search for spiritual guidance, Major Hasan became engaged with jihadist ideology posted online. His exchanges with Anwar al-Awlaki arguably further encouraged Hasan's thoughts of violence, leading to his ultimate decision to shoot several American soldiers in 2009 in Fort Hood, Texas.

Major Hasan attacked a processing center where soldiers were preparing to deploy to Afghanistan, resulting in the deaths of 13 people.⁷ The FBI intercepted emails between Hasan, who was a psychiatrist at the time, and the cleric about a year before the shootings took place. As a Muslim, Major Hasan was troubled by the war, which was causing the deaths of other Muslims in Afghanistan. After the attack, the cleric al-Awlaki praised Major Hasan for doing "the right thing."⁸ Although al-Awlaki acknowledged communicating with Major Hasan, the cleric "said that he neither ordered nor pressured Maj. Nidal M. Hasan to harm Americans, but that he considered himself a confidant of the Army psychiatrist who was given a glimpse via email into Hasan's growing discomfort with the U.S. military."⁹ In fact, this was not the first time that Major Hasan had come across the cleric. Back in 2001, Major Hasan worshipped at a mosque in Falls Church, Virginia, where al-Awlaki preached.¹⁰ There, he was exposed to radical ideas. In other words, Major Hasan came across the extreme teachings of al-Awlaki eight years prior to the Ford Hood shootings. Years later, before the shootings took place, Major Hasan relied on the Internet to seek advice from a former leader. This is an example of how the Internet can not only facilitate direct communication between those interested in terrorism and those who seek to inspire them, but also how it can reinforce existing radical ideology.¹¹ Faisal Shahzad, more famously known as the Times Square Bomber who intended to set off a bomb in Times Square in 2010, used the Internet to connect with extremists. As Professor John Mueller notes, "The Internet was crucial for Shahzad's entrance into the domain of religious fanatical terrorism. He initiated contact with Tehrik-i-Taliban Pakistan over the Internet. Through the initial connection, he was in communication with many jihadist contacts including Anwar al-Awlaki."¹² Similar to the case of Major Hasan, Shahzad was also troubled by the U.S. role in Muslim countries, the use of drones, and the killings of Muslims abroad, and used the Internet to connect with experienced jihadists who gave him both the necessary push and practical knowledge to pursue his attack. Both Major Hasan's and Shahzad's cases demonstrate the important role that the Internet played in connecting extremists. International organizations working on counterterrorism acknowledge that "the reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits."¹³ The Internet is also used to sway those who have some interest in extremist ideologies. Speeches by extremist leaders are posted online and can be accessed by anyone interested in their rhetoric. Nigerian Umar Farouk Abdulmutallab became known as the "Underwear Bomber" for his attempt to blow up a Michigan-bound flight in 2009 with material hidden in his underwear. He, too, had connections with the late al-Awlaki. U.S. government documents reveal that Abdulmutallab sought out al-Awlaki, who later trained him.¹⁴ The government argued that Abdulmutallab was manipulated by extremist lectures posted online. This case demonstrates the not inconsiderable potential influence of Internet videos in the radicalization process.¹⁵ In addition to connecting like-minded individuals and inspiring others to commit violent action, terrorist networks use the Internet to recruit new members. One of the cases that drew media attention was that of Colleen LaRose, more popularly recognized as "Jihad Jane" or Fatima LaRose.¹⁶ In 2008, LaRose, linked to other extremists online in Europe, had conspired to kill a Swedish cartoonist who depicted Prophet Muhammad in a negative light.¹⁷ This case captured the attention of many in the United States and Europe, especially since the accused was a white American female who had converted to Islam as an adult. LaRose used the Internet to successfully recruit and convince other women, such as Jamie Paulin Ramirez, to join her jihadist mission. According to the U.S. Department of Justice, "LaRose and her co-conspirators used the Internet to establish relationships with one another and to communicate regarding their plans...in order to wage violent jihad."¹⁸ Here, the Internet took on the role of recruiting potential terrorists for an international terrorist plot. As demonstrated in this case, "the

Internet becomes a virtual "echo chamber"-acting as a radicalization accelerant while creating the path for the ultimate stage of Jihadization.¹⁶ The Internet can also be used to communicate during the process of planning an attack. Najibullah Zazi, a Colorado resident responsible for planning an attack against the New York subway system in 2009, communicated with his contact in Pakistan via email to design the foiled attack.¹⁷ In addition to other recruits from the United Kingdom involved in the case, the two exchanged messages concerning the making of the bomb and the progress of the plot using coded language. Before heading to New York to execute his plot, Zazi wrote to his contact, letting him know that "the marriage is ready"-signaling that the attack was ready.¹⁸ The two used the term "wedding" to refer to the attack. They also used coded language to refer to explosives. In this example, the Internet was used by individuals to communicate the details and the logistics of their planned attack.

Tracing visited web content is key – Spam Mimicking is used to organize attacks

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 140)

7. Spam Mimicking One of the newest techniques exploited by terrorist operatives is to visit the Spam Mimic Web site, <http://www.spammimic.com>, and "embed encrypted messages in span in order to disguise the fact that confidential data has been exchanged."¹⁹ According to the SANS Institute, users wishing to transfer secret messages need only visit the site, "choose 'encode' from the menu, type in a short message, and press enter. This generates a realistic spam message with the secret message embedded inside it."²⁰ Upon receipt of the message, the end recipient of the span message can then visit the "Spam Mimic Web site to 'decode' the spam, and retrieve the original message. 123

Terrorists use the internet to distribute propaganda – monitoring that traffic is key

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 142-3)

Several other individuals and organizations operating in the United States during the late 1990s and early 2000s exploited the Internet to promote and materially support Islamic terrorism. Sami Omar Al-Hussayen, a Saudi Arabian computer science doctoral student at the University of Idaho developed and maintained content for more than fifteen Islamic extremist Web sites and Internet chat rooms "which contained materials designed and intended to recruit mujahideen and raise funds for violent jihad."²¹ Among the various items that al-Hussayen posted on his Web sites was the following fatwa²² posted at www.alasr.ws in June 2001, just three months prior to the September 11 th attacks: [T]he Mujahid (warrior) must kill himself if he knows that this will lead to killing a great number of the enemies, and that he will not be able to kill them without killing himself first, or demolishing a center vital to the enemy or its military force, and so on. This is not possible except by involving the human element in the operation. In this new era, this can be

accomplished with the modern means of bombing or bringing down an airplane on an important location that will cause the enemy great losses. Interrogation transcripts of detainees at the U.S. military base at Guantanamo Bay, Cuba, released by the Department of Defense in early 2006, also make frequent references to how the detainees were inspired to join Al Qaeda and the Taliban prior to September 11, 2001 by fatwas they viewed online.¹⁴⁰

Terrorists use websites to recruit newer members

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 146-7)

In addition to providing a method of outward communication, jihadist Websites glorify Islamic militancy in video testimonials of jihad operations. Sympathizers and potential recruits are thereby indoctrinated with virtuous messages of jihad and martyrdom that justify and legitimize violent action against non-Muslims. 165 A video entitled "The Attack on the Hotels: 'Badr al-Baghdad," posted on a Zarqawi-affiliated site in December 2005, glorifies strikes on foreign targets in Iraq by taking viewers inside a terrorist cell's pre-attack surveillance. 166 The video chronicles planning and practice runs for the suicide bombings of the Sheraton Ishtar and Meridian Palestine Hotels in Baghdad. 167 The video includes laudatory biographical profiles of the suicide bombers as well as their martyrdom statements.168 Palestinian Islamic Jihad ("PIJ") exploits the Internet to glorify the purported courage and selflessness of suicide bombers who attack Israeli targets. 169 The aim is to inspire new sympathizers and recruits to commit to sacrifices for the terrorist group. 170 Visitors to PIJ's QudsWay.net Web site hear background music and the voice of the group's founder, Fathi Shiqaqi, proclaiming that the "Islamic nation's covenant [is] with blood." The site features the picture of the suicide bomber who carried out the December 5, 2005, attack on a shopping mall in Netanya, Israel, that killed five Israeli citizens. The caption reads: "The suicide bomber Abu Sa'ad . . . waited for the Zionists to approach, smiled a broad smile and blew himself up." 172 The site also includes official PU publications, which can be downloaded by individuals who wish to learn about PIJ operations.173

Terrorists use the internet for fundraising

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 147-8)

According to Todd Hinnen, a terrorist financing expert who serves on the Bush administration's National Security Council, terrorists use the Internet in "four primary ways to solicit and collect funding and equipment in support of terrorist operations."¹⁷⁴ Terrorists: (1) solicit donations, indoctrinate adherents, share information, and recruit supporters directly via Web site chat groups, and targeted electronic mailings; (2) they take advantage of charitable organizations, soliciting funds with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors' largesse to fund acts of violence; (3) they perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support their mission with the proceeds of such crimes; (4) and they use the Internet as a pervasive, inexpensive, and anonymous medium of communication to organize and implement fund raising activities. 175 The U.K.-based Hamas front-organization Interpal is one of the largest

Internet-based fundraising organizations and utilizes many of the above methodologies. In addition to being a principal conduit through which funds are funneled (under the guise of charity) to Hamas, "Interpal is [a] fundraising... coordination point for other Hamas-affiliated charities... [As such, Interpal] supervis[es] activities of charities, develop[s] new charities in targeted areas, instruct[s] how funds should be transferred from one charity to another, and even determine[es] public relations policy.' 7 6 Despite enforcement actions by the United States and Israel to freeze the assets of Interpal and to shut down the Web site, the organization continues to operate and raise funds online. 1 7 Some prominent Islamic extremists issue public statements and writings referring followers to Web sites that provide instructions on how to exploit the Internet to raise funds for their deadly campaigns. Imam Samudra, Indonesian Al Qaeda terrorist and the leader of the 2002 Al Qaeda Bali bombings, 78 recently released an autobiography from his jail cell containing a chapter entitled, "Hacking, Why Not?" 1'79 The chapter "details basic information on money laundering, online credit card fraud, and computer programming languages, exhorting all would-be terrorists to use cyberspace to further jihad." 80 Other terrorist networks have combined multiple communications media to raise funds for terrorism-related operations. For example, Hezbollah maintains its own popular television station, Al Manar, 81 which is broadcast throughout the Middle East, and promoting violence against Israel and the United States. Al-Manar's Web site urges contributions "for the sustenance of the Intifadah" and provides bank accounts in Lebanon to which donations can be made for the purpose of carrying out violence against Israeli interests. 82 Each of these Internet fundraising techniques illustrates terrorists' technological sophistication and strategic manipulation of readily-available technology in order to raise funds for militant campaigns.

Websites are used to give instructions for attacks

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 148-9)

Many violent extremist Web sites have become one-stop terrorist training and planning centers. As traditional means of travel and communication have become increasingly difficult for many terrorist operatives since September 11 th, 183 a number of terrorist-related sites have expanded their use of the Internet as a command and control platform.¹ 84 With horrifying openness and audacity, jihadi webmasters utilize multimedia Web technologies to create virtual training and planning command centers. "If you want to conduct an attack, you will find what you need on the Internet."¹ 85 During 2005 and early 2006, a series of high-quality training films shot in Afghanistan were posted on Web sites associated with Al Qaeda affiliated groups. These Web videos include instructions for conducting a roadside assassination, raiding a house, shooting a rocket propelled grenade, blowing up a car, attacking a village, destroying a bridge and firing an SA-7 surface-to-air missile. 11 6 Al Qaeda operatives planning the March 14, 2004, Madrid train bombings studied a report on the Al Qaeda-affiliated Global Islamic Media front Web site, "in which a committee of al-Qaeda experts suggested an attack in Spain before the general elections of March 14, 2004." 1s17 In late 2003, a Web site entitled "Al Qa'ida University for Jihad Sciences" offered an online instruction manual for various terrorist attacks including "suicide operations."¹88 In August 2005, a site maintained by an Iraqi insurgency group posted an instructional pamphlet entitled "The New Road to Mesopotamia" for prospective foreign fighters seeking to enter Iraq to fight against U.S. and allied forces.¹⁸ 9 The pamphlet included very

specific tactical recommendations for crossing the Syria-Iraq border, based on what appeared to be first-hand accounts of fighters who had previously made the trip: Arrange your trip to take place over two stages. The first stage is to learn the area, the people and the roads, and then head toward the city of Dayr Al-Zawr [Syria] near the Iraqi border. It is recommended to enter the city using a car and do not carry large sums of money. If anyone asks, say you are here on a vacation and have come to go fishing in the Euphrates-therefore, bring some fishing equipment and another person with you so you won't look suspicious. It is an inexpensive region and usually you will end up paying \$300 for 15 days in a four star hotel. A tank of gas will cost you around \$10 A number of other Web sites include remarkably detailed instructional booklets on how to make suicide explosive belts. For instance, a 26-minute video on the Al-Ansar forum site discovered by the SITE Institute in December 2004 "shows how to estimate the impact of an explosion, how best to arrange the shrapnel for maximum destruction, how to strap the belt onto the bomber's body, [and] even how to avoid the migraine headache that can come from exposure to the recommended explosive chemicals."⁹¹

The internet is used to disseminate instructions for bioterror

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, p. 150)

Other sites have published a 15-page document authored by Al Qaeda operational leader Mustafa Setmariam Nasar with instructions for deploying potential biological weapons agents.¹⁹² The document explains how to develop a crude biological weapons delivery mechanism: "inject carrier animals, like rats, with the virus and how to extract microbes from infected blood... and how to dry them so that they can be used with aerosol delivery system."⁹³ Online manuals discovered by the Terrorism Research Center instruct operational activities on "how to extract explosive materials from missiles and land mines. Another offered a country-by-country list of explosive materials available in western markets 194

Terrorists use codes to pass messages – cracking these is key to counterterrorism

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, ES)

Terrorist groups, including Al Qaeda, use online coding techniques or programs, known as steganography,⁹⁸ which allow illicit computer users, to hide a message inside another message, image, or file posted on the Internet.⁹⁹ For example, French intelligence officials assert that "suspects arrested in an alleged plot to blow up the U.S. Embassy in Paris were to get the go-ahead for the attack via a message hidden in a picture posted on the Internet."¹⁰⁰ Other extremists utilize "Internet bulletin boards carrying pornographic and sports information" to relay steganographic operational information to associates located elsewhere in the world.¹⁰¹ According to Internet security expert Chet Hosmer, other terrorist operatives transfer messages via "images that might be in an email message... [inside an] image that no one else would be able to detect or see."¹⁰² September 11th ringleader, Mohamed Atta, may have used steganographic tactics to

encode e-mail messages to his co-conspirators. Atta was "seen repeatedly by witnesses using his Hotmail account at public libraries in Florida to surf the Internet, downloading what appeared to be pictures of children and scenes of the Middle East."¹⁰ Even where a terrorist's e-mail is not encrypted, terrorist operatives are known to utilize previously identified code words to signal that a particular event or action is going to take place. In the weeks preceding the September 11th attacks, September 11th ringleader Mohammed Atta e-mailed his Al Qaeda associates: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering."¹¹

Status quo internet surveillance prevents terrorism

Janbek, Ph.D, and Williams 14

(Williams and Valerie, Spring/Summer Ed. The Brown Journal of World Affairs, 20.2, "The Role of the Internet in post-9/11 Terrorism and Counterterrorism,")

The way in which terrorists utilize the Internet has continuously evolved since 9/11. U.S. intelligence, law enforcement, and security agencies have responded by significantly expanding their counterterrorism workforce, conducting undercover operations, and increasing surveillance of communications and online activity. Collaboration between these agencies has been vital to the nation's counterterrorism efforts; information gathered by the National Security Agency (NSA)'s surveillance technology is shared with the FBI for use in investigations.²⁰ Though these strategies have arguably stopped potential attacks on U.S. soil, media outlets have questioned the ethics behind undercover operations and advanced surveillance technologies.²¹ Due to varying motivations, levels of expertise, and tactics of extremist groups and individuals, the FBI acknowledges terrorism as a complex threat. As a response, the agency has increased its number of agents by 40 percent and now allocates approximately half of its resources to counterterrorism and the remaining half to all other criminal activity.²² Between 2001 and 2011, the agency has almost tripled its intelligence analyst workforce.²³ It has also increased the number of Joint Terrorism Task Force (JTTF) partnerships from 35 to over 100.²⁴ JTTF partnerships exist between law enforcement agencies across the country that share essential information with each other. These partnerships contribute resources, enhance operational capability, and significantly expand the FBI's intelligence base. According to the FBI, "JTTFs have been instrumental in breaking up cells...[and] they've foiled attacks on the Fort Dix Army base in New Jersey, on the JFK International Airport in New York, and on various military and civilian targets in Los Angeles."²⁵ In addition to expanding its labor force, the FBI has adapted its investigative approach to more proactive, intelligence-led strategies to combat terrorist attacks. These strategies are specifically tailored to the targeted suspect, requiring agents to utilize unique skill sets and language abilities for undercover operations. The FBI implements a variety of undercover tactics on the Internet, at times creating terrorist-network recruiting websites convincing enough to attract potential terrorists. When 18-year-old would-be terrorist Abdella Ahmad Tounisi was searching the Internet for Jabhat al-Nusra, an al-Qaeda branch in Syria, he found one of these sites. Created and maintained by the FBI, the page featured pictures and videos of armed fighters in masks and fatigues intended to depict terrorist training.²⁶ A section of the site, titled "A Call for Jihad in Syria," urged visitors to "come and join your lion brothers of Jabhat Al-Nusra who are fighting under the true banner of Islam, come and join your brothers, the heroes of Jabhat Al-Nusra."²⁷ When Tounisi contacted the website's recruiter, who in reality was an FBI agent, they exchanged email messages in which the teen divulged his detailed plan to engage in jihad in Syria. As a result of this communication, the agency was able to arrest Tounisi

in 2013 at Chicago's O'Hare International Airport before his flight across seas. Tounisi was ultimately charged with attempting to provide material support to a foreign terrorist organization and lying to federal authorities.¹ The FBI utilizes specially trained undercover agents to befriend and earn the trust of domestic terror suspects similar to Tounisi. This strategy allows agents to monitor terrorism plots in their beginning stages and intercept forum posts and emails from individual suspects before they catch the attention of authentic extremist organizations. For example, after posting violent messages on an online extremist forum, teenaged Texas resident Hosam Maher Husein Smadi was befriended by an Arabic-speaking FBI agent posing as a member of an al-Qaeda sleeper cell.²⁷ Within months, Smadi and three undercover agents devised a plot to bomb a 60-story corporate building in Dallas, Texas. On the last day of the sting operation in 2009, Smadi attempted to detonate the fake bomb provided by the FBI and was immediately arrested.¹ Once an agent befriends a targeted suspect, plans are developed and if necessary, resources are provided at the target's request. Throughout this process, FBI agents attempt to dissuade the suspect, offering him or her a chance to abandon the plan.²⁸ If the individual is adamant in completing the mission-at times seen in attempts to purchase weapons, to leave the country, or to detonate an FBI-provided bomb-he or she is arrested and tried for the crime. This scenario is not uncommon; there have been several cases of homegrown violent extremism fueled by extremist websites, even in individuals as young as 14.²⁹ In cases like these, the FBI asserts that if an individual is susceptible to an undercover agent, he or she would be just as susceptible to an extremist group.³⁰ Although sting operations have been used by law enforcement for decades, this process of befriending and working with potential terrorists online has sparked an ethical debate. Furthermore, some have questioned whether sting operations are the best use of counterterrorism resources. Some consider these operations to be entrapment since the FBI partially devises the plan and provides money, fake bombs, and even vehicles to suspects. In a recent New York Times article, author David Shipley questioned the legitimacy of cultivating potential terrorists instead of finding real ones.³¹ Shipley dismisses some terror suspects as "incompetent wannabes looking for a cause that the informer or undercover agent skillfully helps them find."³² Cases like that of Hosam Smadi exemplify these arguments; Smadi's defense team described him as a troubled youth who suffered from depression and schizophrenia.³³ According to the defense, Smadi was motivated by the undercover agents' praise and companionship.³⁴ Despite their efforts to portray him as a misguided victim of entrapment, Smadi was charged in 2010 with one count of attempting to use a weapon of mass destruction and one count of bombing a public place. He was sentenced to 24 years in prison and deportation upon release. According to investigative journalist Trevor Aaronson, no terrorism defendant since 9/11 has won an acquittal using entrapment as a defense.³⁵ Collaborating with prosecutors, undercover operatives determine strategies to prove the suspect's predisposition to committing the crime. Working together, prosecutors and FBI employees document proof to use in court later.³⁶ Though its ethical standards are in question by the public, the FBI's strategies have been successful under legal standards.¹ Undercover operations represent just one investigative technique for identifying terrorists and their networks. FBI operatives also investigate activities of known terrorist organizations, interview locals, and monitor foreign press for intelligence. These traditional, preventative policing techniques are employed in collaboration with online data to compile evidence necessary to prosecute terrorists.³⁷ Although controversy surrounds the agency's sting operations, the FBI reports that it has removed more than 20 of al-Qaeda's top 30 leaders due to the FBI's improvements since 9/11.³⁸ These changes hinder al-Qaeda's efforts in fundraising, recruiting, training, and planning attacks outside their local region. The FBI also says that every major al-Qaeda affiliate has lost its key leader.³⁹ Although these leaders can be replaced, al-

Qaeda is forced to use less experienced leaders, degrading their overall efficiency. The FBI credits their achievements to their expansion in intelligence and access to digital records, due in part to post- 9/11 legislation.⁴¹ Post-9/11 legislation, including the PATRIOT Act and the FISA (Foreign Intelligence Surveillance Act of 1978) Amendments Act, enables the NSA to gain access to individuals' online activity, employ advanced surveillance technology, and increase the use of National Security Letters. National Security Letters, commonly used in counterterrorism investigations, enable agents to collect noncontent consumer information including Internet records, telephone records, and credit reports from third party service providers. Additionally, section 215 of the PATRIOT Act permits the FBI to seize anything tangible from a person for investigations against international terrorism.⁴⁰ Intelligence officials admit that "the National Security Agency is searching the contents of vast amounts of Americans' email and text communications into and out of the country" for mentions of foreign terrorist suspects under surveillance.⁴¹ Relevant data collected by this surveillance is shared with the FBI and their JTTFs to aid investigations.⁴²

XKEYSCORE

XKEYSCORE key to solve terrorism – shows networks and provides invaluable intelligence

Pham, 14 (Cassidy, San Jose State University, 2/27/14, “Effectiveness of Metadata Information and Tools Applied to National Security”, Library Philosophy and Practice (e-journal), University of Nebraska-Lincoln,
<http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=2608&context=libphilprac>)

With this wealth of metadata, and the tools to organize and graphically visualize the information, the IC can apply sophisticated analytics techniques to identify persons of interests and associates. The first experiment is applicable as a national security tool since it efficiently connects contacts, and isolates social groups. This is particularly useful in disassociating contacts that are unaware or uninvolved with the person interest. It is also valuable in finding unknown associates of targets he or she already knows about. The second experiments provide additional contextual information. Naturally, metadata explains the who, what, where and when. It does not explain the why and how. These questions are left for analysts to fill in by using contextual information, such world cloud experiment, to develop a so-called picture. Though the experiments were innately limited in scope, the relative success in the application of metadata shows its effectiveness as a national security tool.¶ As noted in the literature review, metadata tools, such as the XKeyscore are truly invaluable as intelligence gathering tools. According to leaked documents, over 300 terrorists were captured using the XKeyscore (The Guardian, 2013). Also, examples from various case studies, such as the killing of Osama Bid Laden indicate successful use and application of metadata. With the added benefit of the interoperability of these various tools, the IC can lighten the burden and share information. Rather than having one agency find a needle in a haystack—a haystack of infinite size, it is far more efficient and effective to divide the hay into multiple stacks among multiple players.¶ Conclusion¶ Much of the information and sources are conjecture since they are based on leaked documents. And of course, the government has yet to fully disclose the information on the tools, which exasperates the problem. Nonetheless, declassified documents, journal articles, and metadata tools that are relatively similar to the ones used by the IC, insure legitimacy to the evidence. Overall, the results from the experiments indicate a high success rate since untrained observers were able to analyze the metadata diagrams, and accurately determine social groups and personal backgrounds for most of the participants. Evidence from various sources, such as case studies, journal articles, and leaked government documents further support the effectiveness of metadata as part of a national security platform. As the country, and the rest of the world becomes more dependent on smart devices, social media sites, the internet, and other 21st century necessities, metadata and the associated tools are equally necessary for the IC to effectively face the threats of national security.

Court Action, stricter legal standards

Court action and stricter standards create legal uncertainty – hampering the government's counter-terror interests.

Branda '14

(et al; JOYCE R. BRANDA, Acting Assistant Attorney General, BRIEF FOR THE APPELLEES - Amicus Brief for Smith v. Obama – before the United States Ninth Circuit Court of Appeals. “Amici” means “friend of the court” and – in this context - is legal reference to the Reporters Committee – October 2nd – “She” is not gendered language in this instance – as the particular plaintiff identified as a “she”. <https://www.eff.org/document/governments-smith-answering-brief>)

Plaintiff does not address how she has **a privacy interest in business records produced pursuant to congressionally authorized judicial orders.** She does, however, **argue that she has a privacy interest in telephony metadata, and that Smith is distinguishable.** Pl. Br. 15-26. **Those arguments do not withstand analysis.** First, **plaintiff suggests that it “obvious[ly] makes a difference that “[t]he surveillance in Smith continued for three days,” whereas under the Section 215 program the government obtains and retains business records containing telephony metadata over a longer time period.** Pl. Br. 16. But the **greater time** over which metadata may be collected **does not validly distinguish Smith, which held that individuals lack a privacy interest in any** of the telephony **metadata voluntarily transmitted to a telephone company** because the company’s customers “voluntarily convey[] those numbers to the telephone company” and because ““a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” California v. Greenwood, 486 U.S. 35, 41 (1988) (quoting Smith, 442 U.S. at 743-44). That holding did not depend on the number of days the pen register operated, and **any other rule would inject needless uncertainty into an area in which certainty is crucial to enable government personnel to implement these rules in the field.** See, e.g., Atwater, 532 U.S. at 347.

Plan undermines Judicial deference – critical to effective counter-terrorism operations – secrecy and expertise

Posner 12 (Eric A. – Kirkland & Ellis Professor, University of Chicago Law School, “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER SEPTEMBER 11: CONGRESS , THE COURTS , AND THE OFFICE OF LEGAL COUNSEL”, 1/11, Harvard Journal of Law & Public Policy, <http://www.harvard-jlpp.com/wp-content/uploads/2012/01/PosnerFinal.pdf>)

The deference thesis states that during emergencies the **legislature and judiciary should defer to the executive.** 8 It assumes that **the executive is controlled by the President**, but to the extent that the President could be bound by agents within the executive, the deference thesis also holds that those **agents should follow the President’s orders**, not the other way around. In normal times, the three branches of government share power. For example, if the executive believes that a new, dangerous drug has become available, but possession of the drug is not yet illegal, the executive may not act on its own to detain and prosecute those who deal and use the drug. The legislature must first enact a statute that outlaws the drug. The executive also depends on the legislature for financial appropriations and other forms of support. The executive also faces constraints from the courts. If the executive arrests drug dealers and seeks to imprison them, it must first obtain the approval of courts. The courts ensure that the executive does not go beyond the bounds of the new law, does not violate earlier-enacted laws that have not been superseded by the new law, and does not violate the Constitution. **In emergencies, the executive often will contemplate actions that do not have clear legislative authority and might be constitutionally dubious.** For example, **after September 11, the U.S. government engaged in immigration sweeps, detained people without charges, used coercive interrogation, and engaged in warrantless wiretapping** of American citizens. 9 Many, if not all, of these actions would have been considered violations of the law and the U.S. Constitution if they had been undertaken against normal criminal suspects the day before the attacks. After September 11, both **the legislature and the courts gave the executive some deference.** The legislature gave explicit authorizations to

the executive that it had initially lacked; 10 the courts did not block actions that they would have blocked during normal times. 11 But neither body was entirely passive. Congress objected to coercive interrogation and did not give the executive all the authorities that it requested. 12 After a slow start, the courts also resisted some of the assertions the executive made. There is some dispute about whether this resistance was meaningful and caused the executive to change policy or merely reacted to the same stimuli that caused the executive to moderate certain policies independently. 13 In any event, no one disputes that the courts gave the executive a nearly free pass over at least the first five to seven years of the conflict with al Qaeda. The deference thesis, then, can be strong-form or weak-form. This ambiguity has had unfortunate consequences for debates about post-September 11 legal policies. Few people believe that the courts should impose exactly the same restrictions on the executive during an emergency as during normal times. Indeed, doctrine itself instructs courts to balance the security value of a course of action and its cost to civil liberties, implying that certain actions might be legally justified to counter high-stakes threats but not to counter low-stakes threats. 14 Nor does anyone believe that the executive should be completely unconstrained. The debate is best understood in the context of the U.S. government's post-September 11 policies. Defenders of these policies frequently invoked the deference thesis—not so much as a way of justifying any particular policy, but as a way of insisting that the executive should be given the benefit of the doubt, at least in the short term. 15 The deference thesis rests on basic intuitions about institutional competence: that the executive can act more decisively and with greater secrecy than Congress or the courts because it is a hierarchical body and commands forces that are trained and experienced in countering security threats. The other branches lack expertise. Although they may have good ideas from time to time, and are free to volunteer them, the ability of the executive to respond to security threats would be unacceptably hampered if Congress and the courts had the power to block it to any significant degree. Secrecy is an important part of the argument. Policymaking depends on information, and information during emergencies often must be kept secret. Congress and the courts are by nature and tradition open bodies: if they were to act in secret, their value would be diminished. Meanwhile, the argument continues, the fear of an out-of-control executive who would engage in abuses unless it was constrained by the other branches is exaggerated. The President has strong electoral and other political incentives to act in the public interest (at least, in the United States). Even if the executive can conceal various "inputs" into counterterrorism policy, it cannot conceal the "output"—the existence, or not, of terrorist attacks that kill civilians. Thus, it was possible for defenders of the Bush Administration's counterterrorism policies to express discomfort with certain policy choices, while arguing nonetheless that Congress and the courts should not try to block executive policymaking or the duration of the emergency—at least not as a matter of presumption. Critics of the Bush Administration argued that deference was not warranted—or at least not more than a limited amount of deference was warranted, although again these subtleties often were lost in the debate—for a variety of reasons. I now turn to these arguments.

Surveillance programs are state secrets – case law proves

Bazzle 12 (Tom – J.D., Georgetown University Law Center, 2011, “Shutting the Courthouse Doors: Invoking the State Secrets Privilege to Thwart Judicial Review in the Age of Terror”, 2012, 23 Geo. Mason U. Civ. Rts. L.J. 29, lexis)

A. No Harm, No Judicial Review: State Secrets and the Terrorist Surveillance Wiretapping Program Revelations in late 2005 and early 2006 about the TSP – a secret terrorist surveillance wiretapping program operated by the NSA without judicial supervision,ⁿ⁶⁶ whose existence the Bush Administration later confirmedⁿ⁶⁷ – triggered numerous lawsuits against telecommunications providers for violations of subscribers' constitutional and statutory rights.ⁿ⁶⁸ These lawsuits were not the first legal challenges to government wiretapping nor were they the first time the government had invoked state secrets to thwart judicial inquiry of wiretapping challenges.ⁿ⁶⁹

Rather than revisit that history, this Article instead focuses only on post-9/11 circuit court decisions to consider the extent [*41] to which courts have acquiesced to government assertions of the state secrets privilege. While circuit courts have tended to recognize state secrets claims in these cases, it is significant that many of these decisions actually reversed district court decisions that had rejected the state secrets claims. Perhaps the most thorough treatment of whether the state secrets privilege precludes judicial review of the terrorist surveillance program occurred in *Hepting v. AT&T Corp.*, where the plaintiffs argued that AT&T's alleged warrantless wiretapping of its communications violated their First and Fourth Amendment rights.ⁿ⁷⁰ The Bush Administration intervened, moving for dismissal on state secrets grounds.ⁿ⁷¹ After reviewing the purportedly secret evidence in camera,ⁿ⁷² the District Court for the Northern District of California denied the government's motion to dismiss, ruling that discovery should commence because the state secrets claim was inapplicable in light of the government's repeated admissions about the existence of the program.ⁿ⁷³ The district court's thoughtful opinion offers a framework for review of state secrets claims in the war-on-terror context. The district court's threshold inquiry in resolving the state secrets claim was determining whether

the NSA surveillance program that gave rise to the suit actually qualified as a "secret."ⁿ⁷⁴

Because the government had disclosed the existence of the program and AT&T admitted to assisting the government in classified matters when asked, the court concluded that state secrets did not foreclose discovery.ⁿ⁷⁵ While the state secrets privilege did not support pre-discovery dismissal of the case, the court found that there was sufficient ambiguity about the extent of AT&T's involvement in the program, and the contents of any communication records surveyed, so as to permit AT&T to not disclose the extent of its participation in the TSP.ⁿ⁷⁶ The court [*42] made clear, however, that if information about AT&T's role in supporting the TSP became public during the course of the litigation, the government could no longer invoke state secrets to resist disclosing this information.ⁿ⁷⁷

Surveillance information is classified as a state secret – the plan must circumvent the doctrine

Bazzle 12 (Tom – J.D., Georgetown University Law Center, 2011, "Shutting the Courthouse Doors: Invoking the State Secrets Privilege to Thwart Judicial Review in the Age of Terror", 2012, 23 Geo. Mason U. Civ. Rts. L.J. 29, lexis)

The war on terror has led to an increased use of the state secrets privilege by the Executive Branch - to dismiss legal challenges to widely publicized and controversial government actions - ostensibly aimed at protecting national security from terrorist threats.ⁿ¹ Faced with complaints that allege indiscriminate and warrantless surveillance,ⁿ² tortious detention, and torture that flouts domestic and international law,ⁿ³ courts have had to reconcile impassioned appeals for private justice with the government's unyielding insistence on protecting national security. Courts, almost unanimously, have cast their lot with national security, granting considerable deference to government assertions of the state secrets

principle. This deference to state secrets shows no signs of abating; indeed, the growing trend is for courts to dismiss these legal challenges pre-discovery,ⁿ⁴ even before the private litigants have had the chance to present actual, non-secret evidence to meet their burden of proof. Although many looked optimistically at President Obama's inauguration as a chance to break decisively from the Bush Administration's aggressive application of the state secrets [*30] privilege,ⁿ⁵ the Obama Administration has largely disappointed on the state-secrets front, asserting the privilege with just as much fervor - if not as much regularity.ⁿ⁶ as its predecessor.ⁿ⁷

Courts are normally minimalist – the aff collapses executive independence – key to counter terrorism

Keynes 10 -- Professor of Political Science at Pennsylvania State University, University of Wisconsin Ph.D. (Edward, 2010, "Undeclared War: Twilight Zone of Constitutional Power," p. 83)

While the constitutional separation of powers does not preclude judicial review of war-powers controversies or require absolute deference to congressional and presidential judgment that the political-question doctrine sometimes suggests, the separation of powers provides a broad standard for judicial intervention in the vast, complex, and uncertain realm of foreign affairs. When the courts intervene in boundary disputes in order to protect an individual's constitutional rights or society's interest in constitutional government, they should not impair the performance of legislative or executive functions that are essential to protecting national-security interests.¹²⁶ Although the courts do not owe Congress or the President absolute deference in defining the boundaries of legislative and executive power, the principle of comity suggests that the judiciary should search for formulas that least restrict each branch in the performance of its functions, i.e., formulas that maximize each department's independence. As Robert Nagel recommends, when the courts challenge the exercise of legislative or executive power, they should pause to examine the effect of their decisions on the other department's operation. In cases that involve conflicting claims of power, the courts should first determine how broadly and deeply their decisions cut into another department's functions before marching into the political thicket.¹²⁶

Judicial deference is critical to effective counter-terrorism operations – secrecy and expertise

Posner 12 (Eric A. – Kirkland & Ellis Professor, University of Chicago Law School, “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER SEPTEMBER 11: CONGRESS , THE COURTS , AND THE OFFICE OF LEGAL COUNSEL”, 1/11, Harvard Journal of Law & Public Policy, <http://www.harvard-jlpp.com/wp-content/uploads/2012/01/PosnerFinal.pdf>)

The deference thesis states that during emergencies the legislature and judiciary should defer to the executive.⁸ It assumes that the executive is controlled by the President, but to the extent that the President could be bound by agents within the executive, the deference thesis also holds that those agents should follow the President's orders, not the other way around. In normal times, the three branches of government share power. For example, if the executive believes that a new, dangerous drug has become available, but possession of the drug is not yet illegal, the executive may not act on its own to detain and prosecute those who deal and use the drug. The legislature must first enact a statute that outlaws the drug. The executive also depends on the legislature for financial appropriations and other forms of support. The executive also faces constraints from the courts. If the executive arrests drug dealers and seeks to imprison them, it must first obtain the approval of courts. The courts ensure that the executive does not go beyond the bounds of the new law, does not violate earlier-enacted laws that have not been superseded by the new law, and does not violate the Constitution. In emergencies, the executive often will contemplate actions that do not have clear legislative authority and might be constitutionally dubious. For example, after September 11, the U.S. government engaged in immigration sweeps, detained people without charges, used coercive interrogation, and engaged in warrantless wiretapping of American citizens.⁹ Many, if not all, of these actions would have been considered violations of the law and the U.S. Constitution if they had been undertaken against normal criminal suspects the day before the attacks. After September 11, both the legislature and the courts gave the executive some deference. The legislature gave explicit authorizes to the executive that it had initially lacked;¹⁰ the courts did not block actions that they would have blocked during normal times.¹¹ But neither body was entirely passive. Congress objected to coercive interrogation and did not give the executive all the authorities that it requested.¹² After a slow start, the courts also resisted some of the assertions the executive made. There is some dispute about whether this resistance was meaningful and caused the executive to change policy or merely reacted to the same stimuli that caused the executive to moderate certain policies independently.¹³ In any event, no one disputes that the courts gave the executive a nearly free pass over at least the first five to seven years of the conflict with al Qaeda. The deference thesis, then, can be strong-form or weak-form. This ambiguity has had unfortunate consequences for debates about post-September 11 legal policies. Few people believe that the courts should impose exactly the same restrictions on the executive during an emergency as during normal times. Indeed, doctrine itself instructs courts to balance the security value of a course of action and its cost to civil liberties, implying that certain actions might be legally justified to counter high-stakes threats but not to counter low-stakes threats.¹⁴ Nor does anyone believe that the executive should be completely unconstrained. The debate is best understood in the context of the U.S. government's post-September 11 policies. Defenders of these policies frequently invoked the deference thesis—not so much as a way of justifying any particular policy, but as a way of insisting that the executive should be given the benefit of the doubt, at least in the short term.¹⁵ The deference thesis rests on basic intuitions about institutional competence: that the executive can act more decisively and with greater secrecy than Congress or the courts because it is a hierarchical body and commands forces that are trained and experienced in countering security threats. The other branches lack expertise. Although they may have good ideas from time to time, and are free to volunteer them, the ability of the executive to respond to security threats would be unacceptably hampered if Congress and the courts had the power to block it to any significant degree. Secrecy is an important part of the argument. Policymaking depends on information, and information during emergencies often must be kept secret. Congress and the courts are by nature and tradition open bodies: if they were to act in secret, their value would be diminished. Meanwhile, the argument continues, the fear of an out-of-control executive who would engage in abuses unless it was constrained by the other branches is exaggerated. The President has strong electoral and other political incentives to act in the public interest (at least, in the United States). Even if the executive can conceal various "inputs" into counterterrorism policy, it cannot conceal the "output"—the existence, or not, of terrorist attacks that kill civilians. Thus, it was possible for defenders of the Bush Administration's counterterrorism policies to express discomfort with certain policy choices, while arguing nonetheless that Congress and the courts should not try to block executive policymaking or the duration of the emergency—at least

not as a matter of presumption. Critics of the Bush Administration argued that deference was not warranted—or at least not more than a limited amount of deference was warranted, although again these subtleties often were lost in the debate—for a variety of reasons. I now turn to these arguments.

FISA Courts Too Slow to solve counter-terror

FISA Courts are too slow for modern counter-terror operations.

CFR '13

(The Council on Foreign Relations (CFR) is a United States nonprofit organization, publisher, and think tank specializing in U.S. foreign policy and international affairs. Its membership has included senior politicians, more than a dozen Secretaries of State, CIA directors, bankers, lawyers, professors, and senior media figures – December 18, 2013
– Modified for potentially objectionable language - <http://www.cfr.org/intelligence/us-domestic-surveillance/p9763>)

The Bush administration maintained that the Foreign Intelligence Surveillance Act (FISA) was an outdated law-enforcement mechanism that was **too time-consuming given the highly fluid, modern threat environment**. Administration officials portrayed the NSA program as an "early warning system" (PDF) with "a **military nature** that **requires speed and agility**." Moreover, the White House stressed that the program was one not of domestic surveillance but of monitoring terrorists abroad, and publicly referred to the operation as the "Terrorist Surveillance Program." Opponents of the program referred to it as "domestic spying."

Encryption

Encrypted data makes it harder to catch terrorists

Raf Sanchez, September 25, 2014, Daily Telegraph, Tech giants slammed by FBI over encrypted smartphones;

Apple and Google's policy to encrypt their smartphones will make it more difficult to rescue kidnapping victims and foil terror plots, US says,

<http://www.telegraph.co.uk/news/worldnews/nor DOA: 3-21-15>

The FBI has warned that decisions by Apple and Google to encrypt their smartphones will make it more difficult to rescue kidnapping victims and foil terror plots. The two Silicon Valley giants have both decided to add new **encryption** systems in the face of privacy concerns sparked by Edward Snowden's disclosure of mass government **surveillance**. Both Apple and Google were criticised for allegedly handing over reams of customer data over to the National Security Agency (NSA). Now, the companies are offering encryption software as a default on smartphones, claiming it would make it impossible for them comply with US government searches. **"It's not technically feasible for us to respond to government warrants for the extraction of this data from devices," an Apple statement said.** The announcement has alarmed American law enforcement and on Thursday, James Comey, the director of the FBI, added his voice to the criticism. Mr Comey cited child kidnapping and terrorism cases as two examples of situations where quick access by authorities to phone data can save lives. He told reporters at FBI headquarters that US officials are in talks with the two companies and accused the companies of letting people put themselves beyond the law's reach. Law enforcement could still intercept telephone conversations if they had a wiretap warrant from a court. However, the new encryption systems would block access to call data, contacts, photos and email stored on the phone. Ronald **Hosko, a former assistant director of the FBI Criminal Investigative Division, said the encryption would "protect many thousands of criminals who seek to do us great harm, physically or financially".**

Encryption undermines snooping needed to stop terrorist attacks

New York Times, December 24, 2014, Why Democracy is Failing,

http://www.nytimes.com/2014/12/27/opinion/why-democracy-is-failing.html?_r=0 DOA: 3-21-15

Re "War on **surveillance**" (Turning Points, Dec. 6): Julian Assange's article on the Orwellian side of the Internet is provocative. But the remedy for electronic tyranny -- encryption -- fails to take into account modern terrorism. The encryption that would justifiably limit official snooping would equally frustrate the equally justifiable attempt to short-circuit terrorist plots. One could argue about the relative importance of the two imperatives, but not about the two-faced character of all aspects of Internet surveillance.

Encryption makes information needed to prevent and prosecute crimes unavailable

Bloomberg, October 2, 2014, Apple's encryption will slow not stop snooping by cops and spies, <http://www.bloomberg.com/news/articles/2014-10-02/apple-s-encryption-will-slow-not-stop-cops-and-spies> DOA: 3-20-15

The companies announced in recent weeks that their new phones will automatically scramble data so that a digital key kept by the owner is needed to unlock it, making it harder for detectives to examine the content of suspects' phones without their knowledge or cooperation. Previously, such encryption was an option that required users to endure a time-consuming process to activate. "This is going to have a very big impact on law enforcement," said Stewart Baker, a former general counsel for the NSA and now a partner at the law firm Steptoe and Johnson in Washington. "There will be crimes that people get away with because this information is not available."

Encryption decimates effective law enforcement. The impact is rampant terrorism and crime.

Glasser 14 — Ellen Glasser, President of the Society of Former Special Agents of the Federal Bureau of Investigation, Adjunct Professor in the Criminology & Criminal Justice Department at the University of North Florida, served as an FBI Agent for 24 years, 2014 ("Tech companies are making it harder for the nation's law enforcement," *The Baltimore Sun*, November 6th, Available Online at <http://www.baltimoresun.com/news/opinion/oped/bs-ed-fbi-apple-20141106-story.html>, Accessed 07-05-2015)

FBI Director Comey has been on the job for just over a year and is working to change perceptions. In addressing the myriad challenges that face our nation, he brings a positive, reasoned approach to the public discussion of privacy versus safety. While appreciating the public's concern over privacy, he has been very clear that the marketing of these new devices will seriously impede law enforcement's ability to protect Americans. Put simply, legal access to unencrypted mobile device information is needed to keep our citizens and our country safer.

Here is some FBI reality. We live in an apocalyptic, post-9/11 world, where the FBI is confronted with a dizzying array of threats from terrorist bombings to beheadings of innocent victims. Over the years, the FBI has also responded to anthrax attacks, shoe and underwear bombers, White House fence jumpers, child molesters, school shootings, human trafficking, kidnappings and massive fraud schemes. The FBI investigates these matters within the scope of the law and with great, abiding respect for the right of individuals to privacy.

Let me bring this close to home. What if your child was abducted, and the FBI developed mobile device information and had a court order, but FBI agents were unable to access the critical, time-sensitive, unencrypted information that was necessary to save your child's life? Thankfully, most people will never be in a life-or-death situation like this, but it does happen. When it does — any FBI agent can tell you from experience — people want help. Let's start by helping them now.

Public perception needs to change so the focus is on handcuffing the bad guys, not tying the hands of the good guys. Please contact your elected representatives to tell them that **corrective legislation is necessary to require companies like Apple and Google to work with law enforcement and find a solution to this problem.**

Law enforcement can't break strong encryption. ISIS loves this.

Wittes 15 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2015 (“Thoughts on Encryption and Going Dark: Part I,” *Lawfare*—a national security blog curated by the Brookings Institution, July 9th, Available Online at <http://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-i>, Accessed 07-13-2015)

FBI Director James Comey has been on a public offensive of late, arguing against end-to-end encryption that prevents law enforcement access to communications even when authorities have appropriate legal process to capture those communications. The offensive began with a speech at Brookings some months ago. More recently, Comey made these comments on CNN, these comments in a private conversation with me, and wrote this piece for Lawfare.

Yesterday, he was on Capitol Hill, testifying both before the Senate Judiciary Committee (video at this link, prepared statement here) and before the Senate Select Committee on Intelligence (video below):

[Video Omitted]

Comey made some news yesterday. For one thing, he stated very clearly to the Judiciary Committee—and with evident reluctance—that some of the encryption the bureau is now facing is beyond its capacity to crack:

[I]f we intercept data in motion between two encrypted devices or across an encrypted mobile messaging app and it's strongly encrypted, we can't break it.

Now, this is sometimes—I hate that I'm here saying this, but I actually think the problem is severe enough that I need to let the bad guys know that. That's the risk in what we're talking about here. The bad—I'm just confirming something for the bad guys.

Sometimes people watch TV and think, "Well, the FBI must have some way to break that strong encryption." We do not, which is why this is such an important issue.

At another point, he stated that while some companies have designed systems that they lack the capacity to decrypt, in other instances, some companies have simply declined to assist investigators in decrypting signal even where decryption was possible—a matter on which at least one senator fought further information. (See Comey's comments at 1:17:00 and his subsequent exchange with Senator Sheldon Whitehouse at 1:20:00 of the Judiciary Committee hearing.)

All in all, Comey's reception on the Hill was significantly warmer than I expected. The Bureau has clearly done a lot of quiet behind-the-scenes work with members to familiarize them with the problem as the FBI sees it, and many members yesterday seemed to require little persuasion.

But Comey has a very heavy lift ahead of him if he is to make progress on the "Going Dark" problem. For one thing, it's not entirely clear what constitutes progress from the Bureau's

perspective. The administration is, at this stage, not asking for legislation, after all. It's merely describing an emergent problem.

But this is a bit of a feint. The core of that emergent problem, at least as Comey's joint statement with Deputy Attorney General Sally Yates frames it, is that CALEA—which mandates that telecommunications providers retain the capacity for law enforcement to get access to signal for lawful wiretapping—does not reach internet companies. So even if Apple and Google were to voluntarily retain encryption keys, some other actor would very likely not do so. Absent a legal requirement that companies refrain from making true end-to-end encrypted services available without a CALEA-like stop-gap, some entity will see a market hole and provide those services. And it's fair to assume that ISIS and the most sophisticated bad actors will gravitate in the direction of that service provider.

In other words, I think Comey and Yates inevitably are asking for legislation, at least in the longer term. The administration has decided not to seek it now, so the conversation is taking place at a somewhat higher level of abstraction than it would if there were a specific legislative proposal on the table. But the current discussion should be understood as an effort to begin building a legislative coalition for some sort of mandate that internet platform companies retain (or build) the ability to permit, with appropriate legal process, the capture and delivery to law enforcement and intelligence authorities of decrypted versions of the signals they carry.

The plan risks catastrophic terrorism.

Weissmann 14 — Andrew Weissmann, Senior Fellow at the Center for Law and Security and the Center on the Administration of Criminal Law at New York University, former General Counsel for the Federal Bureau of Investigation, holds a J.D. from Columbia Law School, 2014 (“Apple, Boyd, and Going Dark,” *Just Security*, October 20th, Available Online at <http://justsecurity.org/16592/apple-boyd-dark/>, Accessed 07-05-2015)

To my mind – although, as in many areas of the law, there is no perfect solution — the cost of a system where we may be more at risk to illegal hacking is outweighed by the vital role lawful electronic interception plays in thwarting crime – including devastating terrorist attacks. Law enforcement and intelligence officials, including most recently FBI Director James Comey, have noted that we all – including criminals – increasingly use non-telephonic means to communicate. The ability to monitor electronic communications is decreasing with every new encryption tool on such communication systems. Law enforcement authorities in the US and overseas rightfully note how such data is critical to solving everyday crimes, such as kidnapping, fraud, child pornography and exploitation, among many others. And at least as important, preventing terrorist attacks requires such ability, as intelligence agencies note (although due to the Snowden leaks, resulting in the public perception that the intelligence community has too much, not too little, access to information, the ramifications from encryption on traditional law enforcement is likely to be relied on by the government in the public debate on this issue).

This is a judgment Congress needs to make, and soon. In weighing the interests, however, it is no answer to say that the government should revert to means other than lawful intercepts obtained through court orders based on probable cause to prevent crimes. The reality of electronic communications is here to stay and plays a vital role in how crimes are perpetrated by allowing

people to communicate with conspirators and to carry out their nefarious plans. In this regard, the government and privacy advocates both need to be consistent in their arguments: it is the latter who usually remind us that the advent of smartphones and “big data” makes traditional Fourth Amendment line-drawing obsolete. And they have a point, as the Supreme Court is starting to recognize. But by the same token, it is increasingly important to have an ability to monitor such communications, after meeting the necessary Fourth Amendment standard upon a showing to an independent Article III court.

The plan substantially increases the risk of catastrophic *crime and terrorism*.

Rubin 14 — Jennifer Rubin, Columnist and Blogger for the *Washington Post*, holds a J.D. from the University of California-Berkeley, 2014 (“Silicon Valley enables terrorists and criminals,” *Right Turn*—a *Washington Post* blog, October 19th, Available Online at <http://www.washingtonpost.com/blogs/right-turn/wp/2014/10/19/silicon-valley-enables-terrorists-and-criminals/>, Accessed 07-05-2015)

Google chairman Eric Schmidt likes to brag that his company is “on the right side of history.” He pats himself on the back for pulling out of China because of that country’s censoring practices. His company even has a slogan, “Don’t be evil,” meant to remind Google employees that they aspire to the highest ethical standards. But, to be blunt, Google is violating its own “don’t be evil” rule by insisting on encryption technology which locks out anti-terrorist and law enforcement agencies. That gives terrorists and common criminals alike huge protection and puts their fellow Americans at risk.

Benjamin Witten of the Brookings Institution explains this is not about “encryption,” as some reports characterize it. No one is talking about eliminating encryption, he explains, “Without it, you couldn’t have electronic commerce. Nobody wants to get rid of encryption.” He explains, “The only question is whether there should be government access with lawful process — or not.”

In a scantily covered speech this week, FBI Director James Comey explained:

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren’t seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple’s new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple’s announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won’t be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

That is a problem that is not solved, as Apple claims, by providing access to the cloud. "But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement," Comey said. "And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data."

In fact, the blocked phones are simply part of a marketing pitch to cater to young people who are misinformed and paranoid about what information the government has access to. Comey observed that "it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?"

Well, some terrorists will use it to plan and execute murderous schemes, organized crime will use it to hide from law enforcement and the American people will be less safe and less secure.

Maybe the president (whose party benefits from liberal high-tech donors) should call these people in for a chat and explain why they should stop this. Alternatively, Congress should hold open hearings and have these execs explain why they want to give terrorists an e-hideout. Then again, maybe concerned Americans who want to combat terrorists should simply not use these products. (Hang onto your old phone until they drop the "locked safe," for example.) What President Obama, Congress and the American people should not do is sit idly by while they put us at risk for pecuniary gain.

Comey went out of his way to be nice to these companies: "Both companies are run by good people, responding to what they perceive is a market demand." Too nice, in my mind. Instead he should have just told them flat out, "Don't be evil."

Especially true of ISIS.

AP 15 — Associated Press, 2015 ("US Officials: Encryption Hinders Monitoring Extremists," Byline Eric Tucker, June 4th, Available Online at <http://www.forensicmag.com/news/2015/06/us-officials-encryption-hinders-monitoring-extremists>, Accessed 07-06-2015)

The growing use of encrypted communications and private messaging by supporters of the Islamic State group is complicating efforts to monitor terror suspects and extremists, U.S. law enforcement officials said Wednesday.

Appearing before the House Homeland Security Committee, the officials said that even as thousands of Islamic State group followers around the world share public communications on Twitter, some are exploiting social media platforms that allow them to shield their messages from law enforcement.

"There are 200-plus social media companies. Some of these companies build their business model around end-to-end encryption," said Michael Steinbach, head of the FBI's counterterrorism division. "There is no ability currently for us to see that" communication, he said.

Encryption helps terrorists — Zazi proves.

Crovitz 14 — L. Gordon Crovitz, Columnist and Former Publisher of *The Wall Street Journal*, former Executive Vice-President of Dow Jones, 2014 (“Terrorists Get a Phone Upgrade,” *Wall Street Journal*, November 23rd, Available Online at <http://www.wsj.com/articles/gordon-crovitz-terrorists-get-a-phone-upgrade-1416780266>, Accessed 07-20-2015)

It's a good thing Najibullah Zazi didn't have access to a modern iPhone or Android device a few years ago when he plotted to blow up New York City subway stations. He was caught because his email was tapped by intelligence agencies—a practice that Silicon Valley firms recently decided the U.S. government is no longer permitted.

Apple, Google, Facebook and others are playing with fire, or in the case of Zazi with a plot to blow up subway stations under Grand Central and Times Square on Sept. 11, 2009. An Afghanistan native living in the U.S., Zazi became a suspect when he used his unencrypted Yahoo email account to double-check with his al Qaeda handler in Pakistan about the precise chemical mix to complete his bombs. Zazi and his collaborators, identified through phone records, were arrested shortly after he sent an email announcing the imminent attacks: “The marriage is ready.”

The Zazi example (he pleaded guilty to conspiracy charges and awaits sentencing) highlights the risks that Silicon Valley firms are taking with their reputations by making it impossible for intelligence agencies or law enforcement to gain access to these communications. In September, marketers from Apple bragged of changes to its operating system so that it will not comply with judicial orders in national-security or criminal investigations.

“Unlike our competitors,” Apple announced, “it’s not technically feasible for us to respond to government warrants.” This encryption was quickly matched by Google and the WhatsApp messaging service owned by Facebook.

In a private meeting last month, Deputy Attorney General James Cole asked the general counsel of Apple why the company would want to market to criminals. As the Journal reported last week, Mr. Cole gave the hypothetical of the police announcing that they would have been able to rescue a murdered child if only they could have had access to the killer’s mobile device. Apple’s response was that the U.S. can always pass a law requiring companies to provide a way to gain access to communications under court orders.

Since then, U.S. and British officials have made numerous trips to Silicon Valley to explain the dangers. FBI Director James Comey gave a speech citing the case of a sex offender who lured a 12-year-old boy in Louisiana in 2010 using text messages, which were later obtained to get a murder conviction. “There should be no one in the U.S. above the law,” Mr. Comey said, “and also no places within the U.S. that are beyond the law.”

Robert Hannigan, the head of Britain’s electronic-intelligence agency, Government Communications Headquarters, warned in a Financial Times op-ed earlier this month: “However much they may dislike it,” Silicon Valley firms “have become the command-and-control networks of choice for terrorists and criminals.”

Even without terrorism attacks that could have been prevented, Mr. Hannigan said, he thought Internet users may be “ahead” of Silicon Valley: “They do not want the media platforms they use with their friends and families to facilitate murder or child abuse.”

It looks like Silicon Valley has misread public opinion. The initial media frenzy caused by the Edward Snowden leaks has been replaced by recognition that the National Security Agency is among the most lawyered agencies in the government. Contrary to initial media reports, the NSA does not listen willy-nilly to phone and email communications.

Last week, the Senate killed a bill once considered a sure thing. The bill would have created new barriers to the NSA obtaining phone metadata to connect the dots to identify terrorists and prevent their attacks. Phone companies, not the NSA, would have retained these records. There would have been greater risks of leaks of individual records. An unconstitutional privacy advocate would have been inserted into Foreign Intelligence Surveillance Court proceedings.

The lesson of the Snowden accusations is that citizens in a democracy make reasonable trade-offs between privacy and security once they have all the facts. As people realized that the rules-bound NSA poses little to no risk to their privacy, there was no reason to hamstring its operations.
Likewise, law-abiding people know that there is little to no risk to their privacy when communications companies comply with U.S. court orders.

Finding no willingness by Silicon Valley to rethink its approach without being required by law, FBI Director Comey recently asked Congress to update the Communications Assistance for Law Enforcement Act of 1994. This requires traditional phone companies to comply with court orders to provide access to records. He wants the law updated to cover Apple, Google and other digital companies.

Silicon Valley firms should find ways to comply with U.S. court orders or expect Congress to order them to do so. They also shouldn't be surprised if their customers think less of companies that go out of their way to market technical solutions to terrorists and criminals.

Strong encryption greatly increases chance of successful terror attack

RT 15 (RT, “Apple, Google helping terrorists with encryption- Manhattan DA” 04/21/15, <http://www.rt.com/usa/251469-apple-google-encryption-terrorists/>)

Allowing users to take advantage of advanced encryption in order to keep their messages and mobile communication out of the government's hands will only help terrorists plot future attacks, a top New York law enforcement official said. The new encryption services offered by Apple and Google will make it harder to protect New Yorkers, Manhattan District Attorney Cyrus Vance Jr. told local AM970 radio host John Cats. He mentioned built-in encryption – which Apple claims its own engineers cannot break – means that federal and local law enforcement bodies won't be able to intercept communications between potential criminals and terrorists, even if they acquire a warrant. When Cats suggested, “terrorists are running out to buy iPhones,” Vance responded by saying, he was “absolutely right.” If individuals who are seeking to do serious harm to our citizenry know they have a device that they can use with impunity and that the contents of their messages and images on their phones cannot be accessed by law enforcement that's going to be the terrorists' community device of choice. he added, according to the Daily Dot. In addition to Apple, Google is also incorporating encryption into its mobile devices. The two tech giants’ smartphones comprise 96 percent of the global market, the New York Post mentions. “Apple has created a phone that is dark, that cannot be accessed by law enforcement even when a court has authorized us to look at its contents,” Vance said. In response, Vance wants police departments around the country to register their opposition with politicians and for hearings on the issue to take place. On its website, Apple says that encryption is enabled “end-to-end” on its devices and that it has “no way to decrypt iMessage and FaceTime data when it's in transit between devices.” Additionally, the company states, “We wouldn't be able to comply with a wiretap order even if we wanted to.” Other features such as iCloud and Mail also offer some encryption protections. READ MORE: FBI director lashes out at Apple, Google for encrypting smartphones Vance isn’t the only law enforcement official to come out against widespread encryption. In October, New York Police Department Commissioner Bill Bratton heavily criticized Apple and Google for

the move, and FBI Director James Comey also blasted the development. "There will come a day -- well it comes every day in this business -- when it will matter a great, great deal to the lives of people of all kinds that we be able to with judicial authorization gain access to a kidnapper's or a terrorist or a criminal's device," Comey said. "I just want to make sure we have a good conversation in this country before that day comes." In a blog post at the Wall Street Journal, Amy Hess of the FBI clarified the bureau's position on the issue, which has seen a surge in support since former government contractor Edward Snowden revealed a massive domestic and international surveillance operation. She said law enforcement officials will need "some degree of access" to encrypted messages in order to stop criminal and violent plots in the future. "No one in this country should be beyond the law," she wrote. "The notion that electronic devices and communications could never be unlocked or unencrypted – even when a judge has decided that the public interest requires accessing this data to find evidence — is troubling. It may be time to ask: Is that a cost we, as a society, are prepared to pay?"

Encryption decks counter-terror effectiveness

Hess 15 (Amy Hess, Executive Assistant Director Federal Bureau of Investigation, Before the Subcommittee on Information Technology Oversight and Government Reform U.S. House of Representatives Concerning Encryption and Cybersecurity for Mobile Electronic Communication Devices, page 6-7, April 29, 2015.)\\mwang

Examples

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that evidence that was once found in filing cabinets, letters, and photo albums will now be available only in electronic storage. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications. Each of the following examples demonstrates how important information stored on electronic devices can be to prosecuting criminals and stopping crime. As encryption solutions become increasingly inaccessible for law enforcement, it is cases like these that could go unsolved, and criminals like these that could go free. Another investigation in Clark County, Nevada, centered on allegations that a woman and her boyfriend conspired together to kill the woman's father who died after being stabbed approximately 30 times. Text messages which had been deleted from the phone and recovered by investigators revealed the couple's plans in detail, clearly showing premeditation. Additionally, the communications around the time of the killing proved that both of them were involved throughout the process and during the entire event, resulting in both being charged with murder and conspiracy to commit murder. Following a joint investigation conducted by the FBI and Indiana State Police, a pastor pleaded guilty in Federal court to transporting a minor across state lines with intent to engage in illicit sexual conduct in connection with his sexual relationship with an underage girl who was a student at the church's high school. During this investigation, information recovered from the pastor's smart phone proved to be crucial in showing the actions taken by the pastor in the commission of his crimes. Using forensic software, investigators identified Wi-Fi locations, dates, and times when the pastor traveled out of state to be with the victim. The analysis uncovered Internet searches including, "What is the legal age of consent in Indiana", "What is the legal age of consent in Michigan", and "Penalty for sexting Indiana." In addition, image files were located which depicted him in compromising positions with the victim. These are examples of how important evidence that resides on smart phones and other devices can be to law enforcement – evidence that might not have been available to us had strong encryption been in place on those devices and the user's consent not granted. The above examples serve to show how critical electronic evidence has become in the course of our investigations and how timely, reliable access to it is imperative to ensuring public safety.

Today's encryption methods are increasingly more sophisticated, and pose an even greater challenge to law enforcement. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop – evidence that may be the difference between an offender being convicted or acquitted – but we cannot access it. Previously, a company that manufactured a communications device could assist law enforcement in unlocking the device. Today, however, upon receipt of a lawful court order, the company might only be able to provide information that was backed up in the cloud – and there is no guarantee such a backup exists, that the data is current, or that it would be relevant to the investigation. **If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.**

Encryption is getting stronger—cloaks terrorists.

Hess 15 (Amy Hess, Executive Assistant Director Federal Bureau of Investigation, Before the Subcommittee on Information Technology Oversight and Government Reform U.S. House of Representatives Concerning Encryption and Cybersecurity for Mobile Electronic Communication Devices, page 4-5, April 29, 2015.)\mwang

Court-Ordered Access to Stored Encrypted Data Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks. In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default – without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice. Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search warrant for photos, videos, email, text messages, and documents can be an exercise in futility. **Terrorists and other criminals know this and will increasingly count on these means of evading detection.** Additional Considerations Some assert that although more and more devices are encrypted, users back-up and store much of their data in "the cloud," and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many companies impose fees to store information there – fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves – devices which are increasingly encrypted.

Strong encryption facilitates terrorist recruitments and plots

Ybarra 15 (Maggie Ybarra, military affairs and Pentagon correspondent for the Washington Times, Washington Times, “FBI director James Comey flags dangers of encryption services, 07/7/15, <http://www.washingtontimes.com/news/2015/jul/7/fbi-encryption-fosters-furtive-terrorism/>)

FBI Director James B. Comey will be arguing for a robust debate on message-encryption technology to lawmakers Wednesday, as he takes to Capitol Hill to plead his case that terrorist groups such as the Islamic State could take advantage of such technology to recruit Americans into their organization. The technology, commonly referred to as “going dark” allows people to send messages to one another that cannot be traced by the government. Google has reported about 80 percent of its Gmail messages to other addresses in the last month were encrypted, and Apple has said it uses encryption on its iMessage and FaceTime tools which is so secure that even the company can’t read or decode the communications. But for all the good encryption services provide — protecting innovation, private thoughts and other things of value — the technology can also be used for nefarious purposes, Mr. Comey wrote in a blog posting Monday. “There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption,” Mr. Comey wrote. The Senate Judiciary Committee is prepared to hear Mr. Comey’s testimony about the technology, along with the testimony of Sally Quillian Yates, the deputy attorney general at the Department of Justice. “Today’s hearing is intended to start a conversation in the Senate about whether recent technological changes have upset the balance between public safety and privacy.” Sen. Chuck Grassley, Iowa Republican and the panel, said in prepared remarks. “In particular, Director Comey has talked about the challenges this issue presents the FBI in the national security context. According to the Director, ISIS is recruiting Americans on-line and then directing them to encrypted communication platforms that are beyond the FBI’s ability to monitor, even with a court order. If this is accurate, it obviously represents a dangerous state of affairs.” Despite the danger, a group of computer scientists and security experts are trying to counter Mr. Comey’s message by defending the need for encrypted technology. The same day that FBI director made a rare social media effort to flag the dangers of “going dark,” the Computer Science and Artificial Intelligence Laboratory released a 34-page technical report that advocates against providing federal authorities access to encrypted conversations. “We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago,” the report states. “In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution.” President Obama has been trying to ease the concerns of Mr. Comey and the other heads of U.S. government intelligence agencies by searching for a middle ground solution that protects the privacy of U.S. citizens while providing federal agencies with the tools they need to track down and halt potential terrorist threats. Mr. Obama said during a joint January press conference with British Prime Minister David Cameron that his administration has been communicating with companies about how to provide agencies with legal access to conversations that might be taking place via technologies that are constantly evolving. “If we get into a situation in which the technologies do not allow us at all to track somebody that we’re confident is a terrorist, if we … have specific information, we are confident that this individual or this network is about to activate a plot and, despite knowing that information, despite having a phone number or despite having a social media address or a e-mail address, that we can’t penetrate that, that’s a problem,” he said. The solution to that problem will likely be complicated and involve consideration of legislation, regulation, cooperation among lawmakers and with private companies, Mr. Comey said during a June 18 press conference at the Department of Justice. “The companies that are providing communication services don’t want folks killed by people using their platforms,” he said. “So we’re having good conversations with them. I’m sure a big part of it’s going to be international cooperation.”

Backdoor searches protect privacy and are key to law enforcement

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.2-3, <http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy> //wx

As you know, the Fourth Amendment of the United States Constitution authorizes reasonable searches and seizures, providing law enforcement agencies access to places where criminals hide evidence of their crimes – from car trunks, to storage facilities, to computers, mobile devices, and digital networks. In order to safeguard Fourth Amendment rights, these searches are conducted pursuant to judicial warrants, issued upon a neutral judge's finding of probable cause. The probable cause standard represents a balance between privacy and public safety carefully calibrated by centuries of jurisprudence, and it guides individuals and companies in developing their expectations of privacy. Through this judicial process, my Office obtains smartphone evidence to support all types of cases – homicides, sex crimes, child abuse, fraud, assaults, robberies, cybercrime, and identity theft. Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on computers and smartphones. Between October 2014 and June 2015, 35 percent of the data extracted from all phones by my Office was collected from Apple devices; 36 percent was collected from Android devices.² That means that when smartphone encryption is fully deployed by Apple and Google, 71 percent of all mobile devices examined – at least by my Office's lab – may be outside the reach of a search warrant. I want to emphasize I am testifying from a state and local perspective. I am not advocating bulk data collection or unauthorized surveillance. Instead, I am concerned about protecting local law enforcement's ability to conduct targeted requests for information, scrutinized by an impartial judge for his or her evaluation as to whether probable cause has been established. Importantly, and by Apple's own admission, governmental request for information have affected only .00571 percent of Apple's customers.

Strong encryption decks law enforcement abilities – can't obtain any data

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.3-5, <http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf>>//wx

Last fall, Apple and Google, whose operating systems run 96 percent of smartphones worldwide, announced with some fanfare, but without notice to my Office or other law enforcement offices I have spoken to, that they had engineered their new mobile operating systems such that they can no longer assist law enforcement with search warrants written for passcode- protected smartphones. According to Apple's website: On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode... Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess. [Emphasis added.]⁵ Apple's announcement led to an immediate response by law enforcement officials who pointed out that allowing a phone or tablet to be locked such that it would be beyond the reach of lawful searches and seizures was unprecedented and posed a threat to law enforcement efforts – in effect, a boon to criminals. Unless law enforcement officials can obtain the passcode from the user, which will be difficult or impossible in many cases, or can use “brute force” to obtain the passcode (again, difficult or impossible, and attempts to do this would likely lead to the destruction of evidence on the iPhone), the search warrant would be of no consequence, because no one will be able to unlock the phone, notwithstanding the court order. Law enforcement's warnings are hardly idle. Recently, a father of six was murdered in Evanston, Illinois. City of Evanston Police believe that prior to his murder, the victim was robbed of a large sum of money. There were no eyewitnesses to or surveillance footage of the killing. Found alongside the body of the deceased were an iPhone 6 and a Samsung Galaxy S6 Edge running Google Android. Cook County prosecutors served Apple and Google with judicial warrants to unlock the phones, believing that relevant evidence might be stored on them. Apple and Google replied, in substance, that they could not, because they did not know the user's passcode. Information that might be crucial to solving the murder, therefore, had effectively died with the victim. His homicide remains unsolved. His killer remains at large. It is not hyperbole to say that beginning in September 2014, Americans conceded a measure of their protection against everyday crimes to Apple and Google's new encryption policies. Yet, I would note that, before the changes, neither company, to our knowledge, ever

suggested that their encryption keys, held by the companies, were vulnerable to hacking or theft. Fully one-quarter of our felony cases now involve cybercrime or identity theft, so I am keenly aware of the dangers and impact of these crimes on our community (which happens to be situated in a world financial center and is the number one target for terrorism in the world). Because of this, my Office has invested heavily in becoming highly proficient and active in the prosecution of these crimes, and in the promotion of best cybersecurity practices for New York consumers and companies. From my vantage point, and in my opinion, for reasons set forth later in my testimony, Apple and Google's new encryption policies seem to increase protection for consumers from hackers only minimally, if at all. But those policies create serious new risks for my constituents and the millions of visitors and workers passing through Manhattan every day.

Access to smartphone data is key to law enforcement – numerous cases prove

Vance 7/8 <Cyrus R., New York District Attorney, 7/8/15, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy", p.3-5,
<http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf>>//wx

The Cost of Evidence Made Inaccessible Through Apple's Encryption Although encryption has been often discussed in the context of international terrorism, the NSA, and the CIA, the greatest cost of these new encryption policies may well be borne by local law enforcement. Smartphones are ubiquitous, and there is almost no kind of case in which prosecutors have not used evidence from smartphones. My Office (and, I expect, every other local prosecutor's office) has used evidence from cellphones in homicides, rape cases, human trafficking, assaults, domestic violence cases, narcotics cases, kidnappings, larcenies, frauds, identity theft, cybercrime, and robberies. Indeed, it is the rare case in which information from a smartphone is not useful. The following list of recent cases is representative:

Homicide: People v. Hayes, Indictment Number 4451/12: The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life. • Sex Trafficking: People v. Brown, Indictment Numbers 865/12, 3908/12, and 3338/13: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices lawfully seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's cellular phones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his 14 nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison. • Cybercrime and Identity Theft: People v. Jacas et al., Indictment Number 42/12 and People v. Brahms et al., Indictment Number 5151/11: This case involved the successful prosecution of a 29-member identity theft ring, which was able to be investigated and prosecuted, in large part, because of evidence obtained early in the investigation from an iPhone, pursuant to a search warrant. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was lawfully searched, law enforcement officials discovered text messages between members of the group regarding the ring's crimes. Investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole property worth over \$1,000,000. All of the defendants pleaded guilty, and more than \$1,000,000 in cash and merchandise were seized and forfeited. • Sex Offenses: United States v. Juarez, Case No. 12-CR-59: The defendant was arrested for unlawful surveillance by an NYPD officer after the officer observed the defendant using a cell phone to film up women's skirts. My Office obtained a search warrant for the phone. During the subsequent search of the phone's micro SD card, forensic analysts discovered a series of images, taken by the defendant, showing a seven-year-old girl lying down on a bed and an adult man pushing aside her underwear, revealing her genitals. The case was referred to the United States Attorney's Office for the Eastern District of New York, which charged the defendant with producing child pornography. • Physical and Sexual Abuse of a Child: U.S. v. Patricia and Matthew Ayers, Case No. 5:14 CR 0117 LSC SGC: In case after case, law enforcement has been able to discover and prosecute child abuse by using video or photographic evidence taken by the abuser. This case is illustrative: From 2010 to 2013, the defendants abused and exploited a young child in their care who, during that period, was six to nine years old. The couple took photographs of the child in lewd poses, as well as of each other engaged in sexual acts with the child. The defendants recorded the abuse with their smartphones and downloaded the images to a computer. In at least one instance, one of the defendants transmitted images to another individual, indicating that she would travel interstate with the child

to the individual's home so the individual could also have sexual relations with the child. The federal judge overseeing the case described it as the worst case he has personally dealt with, including murders, in his 16 years on the bench. The defendants were ultimately convicted of producing child pornography, in violation of 18 U.S.C. § 2251(a), and were sentenced to 1,590 and 750 years, respectively, in federal prison. There are many other cases—almost too many to count—that I might have selected, but the point is clear: We would risk losing crucial evidence in all of these cases if the contents of passcode-protected smartphones were unavailable to us, even with a warrant. 16 The enormity of the loss is fully appreciated by wrongdoers who use smartphones. Recently, a defendant in a serious felony case told another individual on recorded jailhouse call that “Apple and Google came out with these softwares that can no longer be encrypted [sic: decrypted] by the police. . . If our phones is running on the iO[S]8 software, they can’t open my phone. That might be another gift from God.” This defendant’s appreciation of the safety that the iOS 8 operating system afforded him, is surely shared by criminal defendants in every jurisdiction in America charged with all manner of crimes, including rape, kidnapping, robbery, promotion of child pornography, larceny, and presumably by those interested in committing acts of terrorism. Criminal defendants across the nation are the principal beneficiaries of iOS 8, and the safety of all American communities is imperiled by it.

Data on encrypted devices is crucial to law enforcement and counterterrorism

Yates and Comey 7/8 <Sally Quillian Yates, Deputy Attorney General, and James B. Comey, Director of the FBI, 7/8/2015, “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”, p.3-4, <http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf>>//wx

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications. When changes in technology hinder law enforcement’s ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence. These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole. Of course, encryption is not the only technology terrorists and criminals use to further their ends.

Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from State to State and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that - 4 - phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker. In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully-authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other

types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders. Legal Framework

Encryption blocks successful investigation – Investigators locked out

Ellen Nakashima and Barton Gellman '15 (Ellen Nakashima is a national security reporter for The Washington Post. Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post. He is a senior fellow at the Century Foundation and visiting lecturer at Princeton's Woodrow Wilson School.

https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html)CK

Bitkower cited a case in Miami in December in which a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from state to state and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. His defense, Bitkower said, was that she engaged in consensual sex. As it turned out, the trucker had video-recorded his assault, and the phone did not have device encryption enabled. Law enforcement agents were able to get a warrant and retrieve the video. It "revealed in quite disturbing fashion that this was not consensual," Bitkower said. The jury convicted the trucker. Officials and former agents say there will be cases in which crimes will go unsolved because the data was unattainable because only the phone owner held the key. "I just look at the number of cases I had where, if the bad guy was using one of these [locked] devices, we never would have caught him," said Timothy P. Ryan, a former FBI supervisory special agent who now leads Kroll Associates' cyber-investigations practice.

Encryption decks efforts to combat ISIS- online recruiting

Clare Hopping 7/8/15--Freelance editor and journalist as well as editorial editor for Longneck and Thunderfoot. Cites FBI. (Hopping, "FBI director complains encryption makes his job harder", ITpro. <http://www.itpro.co.uk/security/24943/fbi-encryption-helps-isis-recruit-new-members.//ET>)

Universal encryption will help terrorists spread their creeds through secure messaging services, according to the FBI. James Comey, director of the agency, claimed in a blog post that worldwide encryption will help groups like ISIS ahead of his appearance at the Senate Intelligence Committee. He wrote that secure messaging services and social media will help ISIS recruit new members online. "When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public safety." he wrote on pro surveillance website Lawfare. "That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment."

Backdoors would allow criminals to bypass encryption

Phys.org 15 ("Security experts warn against encryption 'backdoors'", 7/7/15, <http://phys.org/news/2015-07-experts-encryption-backdoors.html>)

A group of computer code experts said Tuesday that law enforcement cannot be given special access to encrypted communications without opening the door to "malicious" actors. A research report published by the Massachusetts Institute of Technology challenges claims from US and British authorities that such access is the policy response needed to fight crime and terrorism. Providing this kind of access "will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend," said the report by 13 scientists. The paper was released a day after FBI Director James Comey called for public debate on the use of encrypted communications, saying Americans may not realize how radical groups and criminals are using the technology. Comey argued in a blog post that Islamic State militants are among those using encryption to avoid detection. The New York Times, which reported earlier on the study, said Comey was expected to renew a call at a congressional hearing for better access to encrypted communications to avoid "going dark." The computer scientists said, however, that any effort to build in access for law enforcement could be exceedingly complex and lead to "unintended consequences," such as stifling innovation and creating hostility toward new tech products. "The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict," the report said. "The costs to developed countries' soft power and to our moral authority would also be considerable." In the 1990s, there was a similar debate on the "clipper chip" proposal to allow "a trusted third party" to have access to encrypted messages that could be granted under a legal process. The clipper chip idea was abandoned, but the authors said that if it had been widely adopted, "it is doubtful that companies like Facebook and Twitter would even exist." The computer scientists said the idea of special access would create numerous technical and legal challenges, leaving unclear who would have access and who would set standards.

NSA decryption is vital to counterterrorism – international consensus

Robertson 13 (Adi Robertson, tech policy correspondent for The Verge, "Intelligence chief says the US attacks encryption because the bad guys use it", 10/4/13, <http://www.theverge.com/2013/10/4/4803646/james-clapper-justifies-tor-breaking-as-necessary-to-fight-terrorists>) -LL

Director of National Intelligence James Clapper has responded to leaks showing how the NSA tried (and largely failed) to break through Tor's encryption network. While his statement doesn't shed much new light on the situation, it encapsulates the intelligence community's general response to criticism since the first leaks were published: that the threat of terrorism or other threats to national security makes any arguably legal tactic not only ethical, but vital. Recently published news articles discuss the intelligence community's interest in tools used to facilitate anonymous online communication. The articles accurately point out that the intelligence community seeks to understand how these tools work and the kind of information being concealed. However, the articles fail to make clear that the intelligence community's interest in online anonymity services and other online communication and networking tools is based on the undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies. Clapper accuses the articles' authors (unnamed, but likely journalist Glenn Greenwald and security expert Bruce Schneier) of painting an "inaccurate and misleading picture of the intelligence community. "The reality is that the men and women at the National Security Agency and across the intelligence community are abiding by the law, respecting the rights of citizens and doing everything they can to help keep our nation safe," he says. To do this, they must "use every intelligence tool available to understand the intent of our foreign adversaries." In the modern telecommunications era, our adversaries have the ability to hide their messages and discussions among those of innocent people around the world. They use the very same social networking sites, encryption tools and other security features that protect our

daily online activities. These are promises and warnings we've heard many times, and they're all valid defenses of the overall surveillance apparatus. What they don't do, unfortunately, is address the implicit questions that Greenwald and Schneier have posed: should one wing of the US government attempt to undermine the very tools that other branches have helped create? And is it valuable to be able to keep some communications almost completely private, even if terrorists can also exercise this privacy? If the dismissive GCHQ comments of "pseudo-legitimate" Tor uses are any indication, the international intelligence community's answer may be a resounding "No."

Decryption Methods Prevent Terrorism

Peterson 6/4-15(Andrea Reporter for Washington Post, “FBI official: Companies should help us ‘prevent encryption above all else’”, Washington Post, “<http://www.washingtonpost.com/blogs/the-switch/wp/2015/06/04/fbi-official-companies-should-help-us-prevent-encryption-above-all-else/>”)

The debate over encryption erupted on Capitol Hill again Wednesday, with an FBI official testifying that law enforcement's challenge is working with tech companies "to build technological solutions to prevent encryption above all else." At first glance the comment from Michael B. Steinbach, assistant director in the FBI's Counterterrorism Division, might appear to go further than FBI Director James B. Comey. Encryption, a technology widely used to secure digital information by scrambling data so only authorized users can decode it, is "a good thing," Comey has said, even if he wants the government to have the ability get around it. [Special report: The Internet's founders saw its promise but didn't foresee users attacking one another] But Steinbach's testimony also suggests he meant that companies shouldn't put their customers' access to encryption ahead of national security concerns -- rather than saying the government's top priority should be preventing the use of the technology that secures basically everything people do online. "Privacy, above all other things, including safety and freedom from terrorism, is not where we want to go," Steinbach said. He also disputed the "back door" term used by experts to describe such built-in access points. "We're not looking at going through a back door or being nefarious," he argued, saying that the agency wants to be able to access content after going through a judicial process.

Decryption is effective for counter-terrorism

Ataide 2/7/-13(Rui As a security conscious individual, I've learned to educate people on the advantages of encryption, “The Man in the Middle: Advantages of SSL Decryption “, RSA“<https://blogs.rsa.com/author/rui-ataide/>”)

I'm currently involved on a lot of security analytics, security response, and other defensive activities. While encryption provides a level of protection when it comes to defense, it also causes a lack of visibility when analyzing network traffic. More and more, even the “bad guys” are using encryption to cover their tracks and avoid detection. It's therefore no surprise that more and more organizations are using SSL inspection devices to monitor their traffic and infrastructure. I actually find myself recommending that they do use the technology and how to best implement it.
SSL inspection devices are nothing more than a well designed man-in-the-middle attack that breaks the encryption into two separate encrypted streams. Therefore, they still provide an adequate level of protection to end-users while allowing security analysts and devices to properly monitor and alert when malicious or unwanted activity takes place. This could be something as simple as a user uploading a confidential document to his/her personal webmail account or more elaborate as someone using an SSL VPN to connect back to a host using a Dynamic DNS name service (a technique commonly used by current malware and advanced attackers).

Decryption is crucial to fighting cyberattacks

Butler 13 (J. Michael Butler, Associate Professor of Humanities at Flagler College, “Finding Hidden Threats by Decrypting SSL”, November 2013, <http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840>)

SSL encryption is crucial to protecting data in transit during web transactions, email communications and the use of mobile apps. Data encrypted with this common method can sometimes pass uninspected through almost all the components of your security framework, both inbound and outbound. As such, SSL encryption has become a ubiquitous tool for the enemy to hide sensitive data transfers and to obfuscate their command and control communications. For example, suppose a user has succumbed to one of the many phishing emails she receives every day, has followed a bad URL link and inadvertently downloaded encrypted Zeus malware to the financial officer’s computer used for ACH bank transfers. Under the cover of encryption, Zeus sends that password information and other sensitive data to an external user, making it possible for the remote attacker to capture a login session, use the transmitted password and deposit the organization’s money in an offshore account. With all commands and traffic transmitted into and out of the network via SSL, the company’s security tools were blind to these activities. Now companies are accepting even more encrypted traffic as they shift toward greater use of cloud services. This means malware will find more innovative ways to take advantage of this common form of transport encryption. For example, attackers can use cloud services to bypass the firewall and synchronize malware from one computer to another, as described in an August 2013 article in “Technology Review News.” 1 With the good guys and bad guys both using encryption, making malicious traffic visible through decryption—and inspecting it—becomes essential. The decryption must be conducted in a way that doesn’t interfere with legitimate network traffic, while working with other security systems for optimum accuracy and performance. Then, the traffic must be re-encrypted before sending it on to its destination to protect sensitive information that might be caught up in the packets being decrypted. This whitepaper describes the role of SSL, the role SSL decryption/inspection tools play in security, options for deploying inspection tools, and how the information generated by such inspection can be shared with other security monitoring systems.

NSA decryption Program Works

Insider Surveillance 12/30/-14(“NSA Decryption: New Snowden Leak is Ancient History “,Insider surveillance”[https://insidersurveillance.com/nsa-decryption-new-snowden-leak-is-ancient-history/”](https://insidersurveillance.com/nsa-decryption-new-snowden-leak-is-ancient-history/))

Well-known for many months now is that the NSA views encryption as a threat to national security, and classifies five types of network communications challenges ranging from “trivial,” “minor” and “moderate” on the low end to the most serious, “major” and “catastrophic.” Small time stuff for NSA Decryption experts: Peer-to-Peer. Skype, still touted as a “secure” form of voice & video communication by owner Microsoft, has been an open book to NSA analysts since at least 2011. Secure Socket Layer — Not so Much. Web connections via https — with the “s” standing for secure, and using secure socket layer (SSL) for encryption, are a snap to break into. NSA routinely captures untold number of SSL handshakes, then analyzes metadata about the connections and metadata from the encryption protocols to break the keys and decrypt any traffic on the Internet via man-in-the-middle attacks. Virtual Private Networks. Long considered highly

secure, and still used to connect mediation devices/routers with law enforcement end points, VPNs have for quite some time been readily opened and their contents reviewed by NSA analysts. "Major" encryption challenges deemed difficult but not impossible: Zoho and Tor. As of 2012 the NSA had problems cracking messages sent through encrypted email service providers Zoho. Monitoring users of the Tor network was also a challenge. Truecrypt. The leaked files point to Truecrypt, a program for "on the fly encryption," as a major headache for the NSA several years ago. Truecrypt was discontinued in May 2014 and developers urged site visitors to find another source for encryption. Read: The NSA figured it out. Off-the-Record (OTR). OTR is an open source protocol for encrypting instant messaging in an end-to-end encryption process. OTR once proved a formidable challenge by combining AES symmetric key algorithm, the Diffie-Hellman method of securely exchanging cryptographic keys over a public channel, and SHA-1 (secure hash algorithm) cryptographic hash function developed by the NSA itself in the mid-1990s. Any combination of encryption modes raises the bar for network penetration. In addition, open source software is harder to attach back doors to without the public noticing. Back in 2011 – 2012, released documents showed that OTR occasionally created problems for NSA. One internal comment reads, "No decrypt available for this OTR encrypted message." However, tech moves on. The NSA — being a significant user of encryption itself — is often directly behind new developments in the field like SHA-1. Like all honest brokers in the field, NSA likes to crack its own work, find the weak spots, fix them and move on. New and improved versions of the hash function include SHA-2 and SHA-3. Companies are following NSA's lead. Microsoft announced in Nov 2013 its "depracation" policy for discontinuing use of SHA-1. Google followed suit for Chrome in Sept 2014. Does this mean that the SHA-1 component of OTR is no longer a head-scratcher for NSA? Yep. What earns the moniker "catastrophic" at NSA? At the head of the list, at least in 2012, was the challenge of users combining Tor with other anonymizing services such as ZRTP, which encrypts VoIP voice and text chats on mobile phones. The "Z" stands for its author, Phil Zimmerman, and the "RTP" for Real-Time Transport Protocol." ZRTP uses Diffie-Hellman secure key cryptography, and auto-senses for other VoIP clients that support ZRTP. It is common to open source programs such as Signal and Redphone. While Tor and ZRTP penetration may have seemed insurmountable several years, the UK's NSA equivalent — GCHQ — has proposed methods for breaking into Tor and defeating other encryption methods.

Targeting terrorist use of encryption is key

Davis, United States representative to Palestine, Congressional aide, lawyer, 2006 (Benjamin R. , European Journal for Criminology, "ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE" 2006, HeinOnline, ES)

As law enforcement and security services' interception of terrorists' messages in some countries has grown, 92 operatives have increasingly utilized encryption technologies to communicate online via e-mail. 93 As the Washington Post reported, "Al Qaeda members have taught individuals ... how to use the Internet to send messages and how to encrypt those communications to avoid detection." 94 For example, Wadih El-Hage, Osama bin Laden's former personal secretary and a senior planner of the 1998 Al Qaeda bombings of U.S. Embassies in Kenya and Tanzania, "sent en- crypted e-mails under various names to associates in Al Qaeda." 95 In addition, "Khalik Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bombings in Jordan at the turn of the millennium." 96 The convicted planner of the

1993 World Trade Center bombing, Ramzi Yousef, "used encrypted files to hide details of a plot to destroy eleven U.S. airliners over the Pacific Ocean. 97

Targeting encrypted data key to countering terrorist backdoors

Barfield 6/9/15 [Claude Barfield, a former consultant to the office of the U.S. Trade Representative, researches international trade policy (including trade policy in China and East Asia), the World Trade Organization (WTO), intellectual property, and science and technology policy. “Encryption: The next battle between security and privacy”, American Enterprise Institute, <https://www.aei.org/publication/encryption-the-next-battle-between-security-and-privacy/>] Schuler 20

Over the past several weeks, we have witnessed an intense debate over cybersecurity and privacy, revolving around the USA Freedom Act. A badly divided Congress, finally—in a rebuke to Senate Majority Leader Mitch McConnell (R-KY) and other defenders of the status quo—mandated the end of the so-called NSA metadata (bulk collection) program that swept up data on the dates, times and location of phone calls. The battle over the NSA metadata program, however, is only the first of what are likely to be a series of clashes over the balance between security and privacy. Looming as the next faceoff is the conflict over encryption and the moves by a number of US technology companies to protect their customers against hackers, whether private or public. In the US, the current skirmish was precipitated by announcements from Apple and Google that they were installing encryption protection in their cellphones that would allow only users—and no outside individual or public official—to unblock the devices. Text messaging services such as WhatsApp and iMessage have followed suit. FBI Director James Comey has taken the lead in strenuous opposition to the encryption moves, denouncing “companies that are marketing something expressly to allow people to place themselves beyond the law.” Following up, last week FBI Assistant Director Michael Steinbach warned a congressional committee that crime groups and terrorists organizations such as ISIS were “going dark” with encryption, heightening the chance that future attacks would go unmasked. House Homeland Security Committee Chairman Michael McCaul (R-TX) responded by labeling the use of encryption a “threat to the homeland.” Thus far, US tech companies are defiant and determined to increase encryption applications to their technologies. Google’s Eric Schmidt argued that the security agencies had only themselves to blame: “The people who criticized this are the ones who should have expected this.” And Apple CEO Tom Cook recently delivered an impassioned defense of encryption, labeling attempts to undermine encryption “incredibly dangerous.” The companies make two arguments. First, technologically, there is no way to introduce “backdoors” for the government without allowing criminals or terrorists to exploit the same flaws. Second, they argue that the government has a number of alternatives: much cellphone data is now stored in the providers’ cloud services and can be retrieved; legal wiretaps of smartphones are not affected; and finally, officials can still retrieve real-time phone records and logs of text messages. There is also an international dimension to the conflict. British Prime Minister David Cameron, new re-elected, has vowed to push through legislation that would force tech companies doing business in Great Britain to provide encryption to police and security officials or risk being banned from that country. In France, in the wake of the Hebdo massacre, new security legislation gives sweeping powers to the government to undertake a host of new tactics against future terrorist attacks. And the loose language may allow similar action against encrypted devices. Back in the United States, the resolution of the standoff is unclear. Chairman McCaul and others have yet to push hard for legislation. And the position of the Obama administration remains indeterminate. President Obama has been equivocal. When queried insistently by the press, he responded that he

sympathized with the tech companies: "They're patriots." But the president went on to note: "If we find evidence of a terrorist plot...and despite having a phone number, despite having a social media address or e-mail address, we can't penetrate that, that's a problem." If the syntax was garbled, so was the message.

Encryption cracking necessary to prevent terrorism

Network World, September 19, 2013, NSA wants even closer partnership with tech industry;

NSA's Debora Plunkett says NSA's now is real-time automated information sharing on a large scale, <http://www.networkworld.com/news/2013/091913-nsa-tech-industry-274011.html> DOA: 2-1-15

The National Security Agency's director of information assurance today said the "way to achieve confidence in cyberspace" is to increase collaboration between the government and the high-tech industry -- remarks that rang ironic given former NSA contractor Edward Snowden's revelations about how NSA works with industry. NSA documents leaked by Snowden showed that the NSA's goal is to build backdoors into commercial products and weaken encryption to make it easier for surveillance, allegations that the U.S. government has not even tried to refute. When asked about that today, NSA director of information assurance Debora Plunkett, who gave the keynote address at the New York Institute of Technology Cyber Security Conference here, flatly refused to discuss the topic. But her keynote address was intended to get hardware and software vendors to work in ever-closer partnership with the NSA. Cyberattacks that could take electricity grids offline and disrupt transportation systems are possible. Plunkett said in her keynote, pointing out the destructive attack that hit Saudi Aramco last year and impacted data systems there. [RELATED: Reported NSA actions raise serious questions about tech industry partnerships MORE: Black Hat: Top 20 hack-attack tools] It's a simple matter to hire hacking services to carry out attacks such as denial-of-service, she said, and the fear now is of "integrity attacks" that would destroy or alter critical data. These are all "cyber security challenges," she noted, and the government today is largely dependent on commercial hardware and software for which the NSA itself cannot "provide indemnification." NSA's needs industry's help, she said. Plunkett said "we have to have a community come together" to collaborate on security in mobility and the cloud especially. The NSA expects that the future of network security lies in "more automated cyber defense" based on "large-scale automation" that would reduce the need for manpower where there would be more real-time sharing of findings. She said there's a need for collaboration with ISPs and hardware companies to achieve all of this. "We have to build a close partnership," she said, adding, there can be "confidence in cyberspace" if "we stay the course." Plunkett is a 29-year veteran of the NSA who worked her way up through the ranks to have a hand in guiding strategic direction for the agency, which carries out surveillance to help defend the country against cyberthreats. But NSA documents recently leaked by Snowden show that the NSA views its partnership with industry in part as a way to subvert security in commercial products and services to make cyber-spying easier. This revelation casts NSA's call for industry partnership and its insistence that there can be "confidence in cyberspace" in a questionable light.

The Bullrun program is key to decrypting internet communications and data relevant to international terrorism

Larson, Perlroth, and Shane, 9/5/13 (Jeff, Data Editor at ProPublica; Nicole, The New York Times; Scott, The New York Times; ProPublica, the organization that Snowden gave his leaks, "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security"
<http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>, accessed 7/14/15)

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor. Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own "back door" in all encryption, it set out to accomplish the same goal by stealth. The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated. The N.S.A. hacked into target computers to snare messages before they were encrypted. And the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world. "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable." When the British analysts, who often work side by side with N.S.A. officers, were first told about the program, another memo said, "those not already briefed were gobsmacked!" An intelligence budget document makes clear that the effort is still going strong. "We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet traffic," the director of national intelligence, James R. Clapper Jr., wrote in his budget request for the current year. In recent months, the documents disclosed by Mr. Snowden have described the N.S.A.'s broad reach in scooping up vast amounts of communications around the world. The encryption documents now show, in striking detail, how the agency works to ensure that it is actually able to read the information it collects. The agency's success in defeating many of the privacy protections offered by encryption does not change the rules that prohibit the deliberate targeting of Americans' e-mails or phone calls without a warrant. But it shows that the agency, which was sharply rebuked by a federal judge in 2011 for violating the rules and misleading the Foreign Intelligence Surveillance Court, cannot necessarily be restrained by privacy technology. N.S.A. rules permit the agency to store any encrypted communication, domestic or foreign, for as long as the agency is trying to decrypt it or analyze its technical features. The N.S.A., which has specialized in code-breaking since its creation in 1952, sees that task as essential to its mission. If it cannot decipher the messages of terrorists, foreign spies and other adversaries, the United States will be at serious risk, agency officials say. Just in recent weeks, the Obama administration has called on the intelligence agencies for details of communications by Qaeda leaders about a terrorist plot and of Syrian officials' messages about the chemical weapons attack outside Damascus. If such communications can be hidden by unbreakable encryption, N.S.A. officials say, the agency cannot do its work.

Without access to backdoors, law enforcement won't have the capacity to collect intelligence data because of increasingly complex encryption

AP 7/8 (Eric Tucker, "FBI, JUSTICE DEPT. TAKE ENCRYPTION CONCERNS TO CONGRESS" Associated Press,
http://hosted.ap.org/dynamic/stories/U/US_FBI_ENCRYPTION?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2015-07-08-06-22-03)

WASHINGTON (AP) -- Federal law enforcement officials warned Wednesday that data encryption is making it harder to hunt for pedophiles and terror suspects, telling senators that consumers' right to privacy is not absolute and must be weighed against public-safety interests. The testimony before the Senate Judiciary Committee marked the latest front in a high-stakes dispute between the Obama administration and some of the world's most influential tech companies, placing squarely before Congress an ongoing discussion that shows no signs of an easy resolution. Senators, too, offered divided opinions.FBI and Justice Department officials have repeatedly asserted that encryption technology built into smartphones makes it harder for them to monitor and intercept messages from criminal suspects, such as Islamic State sympathizers who communicate online and child predators who conceal pornographic images. They say it's critical that they be able to access encrypted communications during investigations, with companies maintaining the key to unlock such data.¶ But they face fierce opposition from Silicon Valley companies who say encryption safeguards customers' privacy rights and offers protections from hackers, corporate spies and other breaches. The companies in recent months have written to the Obama administration and used public speeches to argue for the value of strong encryption.¶ FBI Director James Comey, who has pressed his case repeatedly over the last year before think tanks and in other settings, sought Wednesday to defuse some of the tension surrounding the dispute. He told senators that he believed technology companies were fundamentally on the same page as law enforcement, adding, "I am not here to fight a war."¶ "Encryption is a great thing. It keeps us all safe. It protects innovation," Comey said. "It protects my children. It protects my health care. It is a great thing."¶ But he warned that criminals were using encryption to create a safe zone from law enforcement. He said that concern was especially acute at a time when the Islamic State has been recruiting sympathizers through social media and then directing them to encrypted platforms that federal agents cannot access.¶ "Our job is to look at a haystack the size of this country for needles that are increasingly invisible to us because of end-to-end encryption," he said.¶

--AT metadata solves

Encryption prevents access to key communication data

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))^{*Edited for easier flow}

Law enforcement and national security investigators need to be able to access communications and information to obtain the evidence necessary to prevent crime and bring criminals to justice in a court of law. We do so pursuant to the rule of law, with clear guidance and strict judicial oversight. But increasingly, even armed with a court order based on probable cause, we are* [the FBI is] too often unable to access potential evidence. The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers to be able to implement court orders for the purpose of intercepting communications. But that law wasn't designed to cover many of the new means of communication that exist today. Currently, thousands of companies provide some form of communication service, but most do not have the ability to isolate and deliver particular information when ordered to do so by a court. Some have argued that access to metadata about these communications - which is not encrypted - should be sufficient for law enforcement. But metadata is incomplete information, and can be difficult to analyze when time is of the essence. It can take days to parse metadata into readable form, and additional time to correlate and analyze the data to obtain meaningful and actionable information.

--AT cloud solves

Cloud storage fails – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

Additional Considerations Some assert that although more and more devices are encrypted, users back-up and store much of their data in ``the cloud,`` and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many companies impose fees to store information there - fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves devices which are increasingly encrypted.

--AT hacking solves

Brute force attacks fail – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets. A common misperception is that we can simply break into a device using a ``brute force`` attack - the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today's highlevel encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data. Finally, a reasonable person might also ask, ``Can't you just compel the owner of the device to produce the information in a readable form?'' Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court's order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography. Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can't provide us with the password, especially when time is of the essence.

NSA can't crack encryption—Need encryption keys to access

The Nation '15 (The Nation is America's oldest continuously published weekly magazine, devoted to reporting on politics and culture. The Nation has bureaus in Washington, D.C., London, and South Africa, with departments covering architecture, art, corporations, defense, environment, films, legal affairs, music, peace and disarmament, poetry, and the United Nations, <http://www.nationmultimedia.com/breakingnews/NSA-can't-crack-common-encryption-software-top-hack-30251390.html>)CK

Publicly available encryption programmes are so tough that they can't be cracked by the experts at the US National Security Agency (NSA), an authoritative expert has told one of the world's top hacker jamborees. The assurance, delivered by Jacob Applebaum during this month's Chaos Communication Congress (CCC) in Hamburg, Germany, ends months of speculation that the NSA may have found a backdoor into such privacysoftware. Services like PGP for protecting emails and OTR (off the record) for protecting messaging are pretty safe, agreed experts at CCC, which attracts some of the globe's top hacking experts every January. "PGP and OTR are two ways to keep spies from looking through your stuff," says US activist Applebaum. He said communications protected end to end with these services cannot be read by the NSA. Period. Options like the SSL encryption protocol can be surmounted though, he said. SSL is used - often by banks and internet retail - to keep prying eyes from seeing which websites are being accessed and what's sent to them. SSH, used by system administrators to get into other computers and run them, can also be cracked. It's not clear, though, if the NSA has actually cracked their protocols. Instead, it seems the US electronic intelligence agency is trying to collect keys so it can crack encrypted communication by other methods. That's according to documents released by

whistleblower Edward Snowden, a former NSA contractor, which have been published by German news magazine Der Spiegel.

--AT court order solves

Court orders can't compel decryption – backdoors are key

Crocker, attorney at the Electronic Frontier Foundation, 14 (Andrew Crocker, Graduate of Harvard Law and attorney at the Electronic Frontier Foundation in civil liberties, “Sifting Fact from Fiction with All Writs and Encryption: No Backdoors”, 12/3/14, [//EM*Edited for easier flow](https://www.eff.org/deeplinks/2014/12/sifting-fact-fiction-all-writs-and-encryption-no-backdoors)

Following recent reports in the Wall Street Journal and Ars Technica, there's been new interest in the government's use of a relatively obscure law, the All Writs Act. According to these reports, the government has invoked the All Writs Act in order to compel the assistance of smartphone manufacturers in unlocking devices pursuant to a search warrant. The reports are based on orders from federal magistrate judges in Oakland and New York City issued to Apple and another unnamed manufacturer (possibly also Apple) respectively, requiring them to bypass the lock screen on seized phones and enable law enforcement access. These reports come at an interesting time. Both Apple and Google have announced expanded encryption in their mobile operating systems. If a device is running the latest version of iOS or Android, neither company will be able to bypass a user's PIN or password and unlock a phone, even if the government gets a court order asking it to do so.

The announcements by Apple and Google have in turn led to calls for “golden keys”—hypothetical backdoors in devices intended to allow only law enforcement to access them. As we've explained, we think these proposals to create backdoors totally misunderstand the technology and make for terrible policy. Amid this prospect of a second “Cryptowar” is the lurking fear that the government might force unwilling companies to include backdoors in their products, even if they're not required by Congress to do so. We sometimes hear from jaded developers and others who think that all it would take to force a backdoor is one National Security Letter. While NSLs are unconstitutional, even the government admits that they* [NSLs] can only be used to obtain limited information, which does not include forcing anyone to backdoor a product. Nevertheless, this fear is feeding some of the interest generated by the press reports about the government's invocation of All Writs Act in the unlocking cases.

Court orders fail – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 (Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM)

Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks. In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default - without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice. Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search

warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection.

Data encryption eviscerates the third party doctrine – Lack of encryption permits government access

Christopher Soghoian Ph.D 06 (Principal Technologist with the Speech, Privacy, and Technology Project at the American Civil Liberties Union. He is also a Visiting Fellow at Yale Law School's Information Society Project. Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era Privacy and Law Enforcement pg. 391
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553CK

“The third party doctrine is the Fourth Amendment rule that scholars love to hate. It is . . . widely criticized as profoundly misguided. Decisions applying the doctrine *top[] the chart of [the] most-criticized Fourth Amendment cases.”⁹⁵ However, for the purposes of this article, it can be summarized by stating that online service providers can be compelled to reveal their customers’ private documents with a mere subpoena.⁹⁶ As such, the government is not required to obtain a search warrant,⁹⁷ demonstrate probable cause⁹⁸ or go before a judge. While the third party doctrine is certainly the current tool of choice for the government’s evisceration of the Fourth Amendment, is not completely to blame for the lack of privacy online. The real and often overlooked threat to end-user privacy is not this legal rule, but the industry-wide practice of storing customers’ data in plain text, forgoing any form of encryption. Simply put, if encryption were used to protect users’ stored data, the third party doctrine would for the most part be moot.

--AT voluntary solves

Compelling fails – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets. A common misperception is that we can simply break into a device using a “brute force” attack - the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today’s highlevel encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data. Finally, a reasonable person might also ask, “Can’t you just compel the owner of the device to produce the information in a readable form?” [Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court’s order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography.](#) Without access to the right evidence, we fear [we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can’t provide us with the password.](#) especially when time is of the essence.

Business Records/Section 2015>Email and Phone Surveillance Restriction Links

Signals intelligence from business records needed to stop WMD attacks

Stuart Taylor, April 29, 2014, The Big Snoop: Life, Liberty, and the Pursuit of Terrorists, <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.) DOA: 2-25-15

Over the five years that she has been chairman of the Intelligence Committee, Feinstein has seen more inside information on NSA activities than most of her fellow lawmakers. She is convinced that, since the FISA reforms of the seventies put safeguards and multiple layers of oversight in place, there has been no evidence of the NSA's seriously violating those strictures. She is also convinced that signals intelligence is, if anything, more indispensable than ever at a time when human intelligence—that is, information from undercover U.S. operatives operating abroad or inside hostile organizations like al Qaeda—is so hard to come by. That leads her to worry that curbs on the phone records program might increase the exposure of Americans to danger from terrorists and other enemies, perhaps including mass-casualty cyber, biological, or even nuclear attacks.

Al Qaeda activity can be detected with email and phone record surveillance

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 908-9

Members of the al Qaeda network can be detected, with good intelligence work or luck, by examining phone and e-mail communications, as well as evidence of joint travel, shared assets, common histories or families, meetings, and so on. As the time for an attack nears, "chatter" on this network will increase as operatives communicate to coordinate plans, move and position assets, and conduct reconnaissance of targets. When our intelligence agents successfully locate or capture an al Qaeda member, they must be able to move quickly to follow new information to other operatives before news of the capture causes them to disappear. The NSA database is particularly important because it will point the way to al Qaeda agents within the United States, where they are closest to their targets and able to inflict the most harm on civilians. The September 11 hijackers themselves provide an example of the way that the NSA could use business record information to locate an al Qaeda cell. Links

suggested by commercially available data might have turned up ties between every single one of the al Qaeda plotters and Khalid al Mihdhar and Nawar al Hazmi, the two hijackers known to the CIA to have been in the country in the summer of 2001. Mihdhar and Hazmi had rented apartments in their own names and were listed in the San Diego phone book. Both Mohammad Atta, the leader of the September 11 al Qaeda cell, and Marwan al-Shehi, who piloted one of the planes into the World Trade Center, had lived there with them. Hijacker Majed Moqed used the same frequent flier number as Mihdhar; **five hijackers used the same phone number as Atta when booking their flights**; the remaining hijackers shared addresses or phone numbers with one of those hijackers, Ahmed Alghamdi, who was in the United States in violation of his visa at the time. **Our intelligence agents**, in fact, **had strong leads that could conceivably have led them to all of the hijackers before 9/11**. CIA agents had identified Mihdhar as a likely al Qaeda operative because he was spotted at a meeting in Kuala Lumpur and mentioned in Middle East intercepts as part of an al Qaeda "cadre." Hazmi too was known as likely to be al Qaeda. But in neither case was there enough evidence for a criminal arrest because they had not violated any American laws. **If our intelligence services had been able to track immediately their cell phone calls and e-mail, it is possible that enough of the hijacking team could have been rounded up to avert 9/11.** Our task is much more difficult today, because we might not have even this slender information in hand when the next al Qaeda plot moves toward execution.

Database needs to be broad to find terrorist cells

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 911-12

A critic, however, might argue that billions of innocent calling records are not "relevant" to a terrorism investigation. Even if terrorist communications take place over the phone, that cannot justify the collection of all phone call records in the United States, the vast majority of which have nothing to do with the grounds for the search. The FISC rejected this argument because, **to be useful, a database has to be broad enough to find terrorist calls. "Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations,"** the Court observed, **"the production of the information sought meets the standard for relevance under Section 215."** **Aggregating calling records** into a database, the court found, **was necessary to find the terrorist communications and the links between terrorists.** It may not even be possible to detect the links unless such a database is created. If a database is not comprehensive, in other words, then the government will only be able to glimpse incomplete patterns of terrorist activity, if it can glimpse any at all.

Broad-based records approaches are often used in national security cases

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA

SURVEILLANCE PROGRAMS,

<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, P 911-12

Relevance is a slippery concept, but it cannot require that every piece of information obtained by subpoena must contain information related to guilt. Even when grand juries subpoena the business records or communications of a criminal suspect, it is likely that the large majority of the items will not have any relationship to the crime. Nonetheless, a grand jury may subpoena all of a suspect's financial records to find those that pertain to a criminal conspiracy. A different way to view the NSA's telephone calling record program is that the "relevant" tangible "thing" is the database itself, rather than any individual calling record.

Of course, the NSA program differs from a subpoena to a financial institution for the records of a known criminal suspect. The amount of data collected by the NSA program is many orders of magnitude greater, and hence the percentage of directly involved communications much smaller. Also, unlike a regular subpoena, it is important to have as large a searchable database as possible because the breadth will bring into the sharpest contrast the possible patterns of terrorist activity. On the other hand, the magnitude of harm that the government seeks to prevent exceeds by several orders that of regular crime. The magnitude of the harm should be taken into account in judging relevance as well as the unprecedented difficulties of locating al Qaeda operatives disguised within the United States.

Mass records collection is needed to catch terrorists because they are not all in one place

Joshua Kapstein, May 16, 2014, "The NSA Can 'Collect it All,'" but what would it do with the data?, <http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html> DOA: 2-23-15

The NSA and its allies are staunch defenders of these "haystacks," even though multiple studies concluded the database containing millions of Americans' phone records played little or no role in preventing terrorist attacks. They've countered that it's foolish to assume all terrorists hang out in one isolated section of the Internet, therefore mass-collection becomes a necessary obsession to find that ever-elusive needle.

Business record 215 program has been used to stop a terror attack

Sean M. Joyce, Deputy Director, Federal Bureau of Investigation (FBI), July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hsdl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

As you mentioned another instance when we used the business record 215 program, as Chairman Leahy mentioned, Basaaly Moalin. So initially the FBI opened a case in 2003 based on a tip. We investigated that tip. We found no nexus to terrorism and closed the case. In 2007 the NSA advised us, through the business record 215 program, that a number in San Diego was in contact with an al-Shabab and east -- al-Qaida east -- al-Qaida East Africa member in Somalia. We served legal process to identify that unidentified phone number. We identified Basaaly Moalin. Through further investigation, we identified additional co-conspirators, and Moalin and three other individuals have been convicted -- and some pled guilty -- to material support to terrorism.

Business records closes holes in intelligence in order to defeat terrorism

Sean M. Joyce, Deputy Director, Federal Bureau of Investigation (FBI), July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hsl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

SEN. GRASSLEY: OK.

Mr. Joyce, one part of the balance that we have to strike, protecting privacy of Americans -- the other part, national security. Thankfully, until the Boston bombing, we had prevented large-scale terrorist attacks on American soil. I have a few questions about how valuable the role of Section 215 and 702 programs have played in predicting (sic) our national security. Two questions, and then I'll have to stop and go to our colleagues. Can you describe any specific situations where Section 215 and Section 702 authorities helped disrupt a terrorist attack or identify individuals planning to attack, the number of times? And then secondly, if you didn't have the authority to collect phone records in bulk the way that they are now under Section 215, how would you have affected those investigations?

MR. JOYCE: So to your first question, Senator, as far as a specific example of when we have utilized both of these programs is the one I had first mentioned, the first al-Qaida-directed plot since 9/11, in September of 2009, when Najibullah Zazi and others conspired plot to bomb the New York subway system. We initially found out about Zazi through an NSA 702 coverage, and he was actually talking to an al-Qaida courier who was -- he was asking for his help to perfect an explosives recipe. So but for that, we would not have known about the plot. We followed that up with legal process and then had FISA coverage on him and others as we fully investigated the plot. Business records 215 was also involved, as I had previously mentioned, where we also through legal process were submitting legal process for telephone numbers and other email addresses, other selectors. But NSA also provided another number we are unaware of of a co-conspirator, Adis Medunjanin. So that is an instance where a very serious plot to attack America on U.S. soil that we used both these programs.

But I say, as Chairman Leahy mentioned, there is a difference in the utility of the programs. But what I say to you is that each and every program and tool is valuable. There were gaps prior to 9/11. And what we have collectively tried to do, the members of the committee, other members of the other oversight committees, the executive branch and the intelligence community, is we have tried to close those gaps and close those seams. And the business record 215 is one of those programs that we have closed those seams. So I respectfully say to the chairman that the utility of that specific program initially is not as valuable. I say you are right. But what I say is it plays a crucial role in closing the gaps and seams that we fought hard to gain after the 9/11 attacks.

Section 702 and Section 215 programs have prevented terror attacks

Sean M. Joyce, Deputy Director, Federal Bureau of Investigation (FBI), July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hsl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

SEN. FEINSTEIN: Good.

Now, the NSA has produced and declassified a chart, which I'd like to make available to all members. It has the 54 total events. It includes a Section 702 authority and Section 215 authority, which essentially work together. And it shows the events disrupted based on a combination of these two programs, 13 in the homeland, 25 in Europe, five in Africa and 11 in Asia. Now, I remember I was on the Intelligence Committee before 9/11, and I remember how little information we have and the great criticism of the government because of those stovepipes, the inability to share intelligence, the inability to collect intelligence. We had no program that could've possibly caught two people in San Diego before the event took place. I support this program. I think, based on what I know, they will come after us. And I think we need to prevent an attack wherever we can from happening. That doesn't mean that we can't make some changes.

Business records program has stopped many attacks

Rep. Mike Rogers, Miami Times (Florida), June 18, 2013, (Rep. Mike Rogers, R-Mich., is chairman of the House Permanent Select Committee on Intelligence,
<http://www.usatoday.com/story/opinion/2013/06/18/nsa-mike-rogers-house-intelligence-committee-editorials-debates/2436541/>, DOA: 2-24-15

The gross distortion of two vital National Security Agency [NSA] programs is dangerous and unfortunate. Neither program authorizes NSA to read e-mails or listen to phone calls of

American citizens. Both are constitutional with numerous checks and balances by all three branches of government. **They have been authorized and overseen by Congress and presidents of both parties. And they have produced vital intelligence, preventing dozens of terrorist attacks around the world, including plots against New York City subways and the New York Stock Exchange.** **The first program** allows NSA to preserve a limited category of business records. It **preserves only phone numbers and the date, time and duration of calls. It doesn't include any names or the content of calls. These records can only be accessed when NSA is investigating a foreign terrorist.** If a foreign terrorist is found linked to an American, the tip is passed to the FBI and requires a court order before additional action can be taken. **This is a critical tool for connecting the dots between foreign terrorists plotting attacks in the U.S.** The second program allows the NSA to target foreigners overseas to collect certain foreign intelligence with court approval. It doesn't create a "back door" to any company's server, and doesn't authorize monitoring of U.S. citizens. No U.S. person anywhere in the world can be intentionally monitored without a specific order. Any comparison to government abuses in decades past is highly misleading. Today's programs are authorized in law, with a thorough system of oversight and checks and balances in place, and a court review not present in the past. Now each of the agencies has an inspector general and general counsels who ensure that these authorities are exercised in accordance with the law. The House and Senate each have Intelligence Committees charged with overseeing these authorities. Additionally, electronic surveillance for foreign intelligence purposes occurs with approval of the Foreign Intelligence Surveillance Court. None of these structures and protections was in place in the 1950s, '60s or '70s. These narrowly targeted programs are legal, do not invade Americans' privacy, and are essential to detecting and disrupting future terrorist attacks.

Metadata collection needed to cast a wide net

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 907-8

A. Phone Call Metadata Collection

Like business records, phone call metadata falls within Section 215's definition of tangible items. Collection of such metadata relates to an authorized investigation to protect against international terrorism. Several investigations into al Qaeda plots remain open, as shown by the repeated indictments against bomb plotters in the last five years. **The examination of records also helps protect the nation against terrorist attacks.** According to the NSA, only the information contained in the billing records is collected; the content of calls is not. There can be no First Amendment violation if the content of the calls remains untouched. A critic might argue that the terms of the search are too broad because ninety-nine percent of the calls are unconnected to terrorism. **But an intelligence search,** as Judge Richard Posner has described it, "**is a search for the needle in a haystack.**" Rather than **focus on foreign agents who are already known, counterterrorism agencies must search for clues among millions of potentially innocent connections, communications, and links.** "**The intelligence services,**" Posner writes, "**must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented.**" For this reason, the FISC approved the NSA program in 2006 and has continued to renew it since.

Section 215 necessary to defeat terrorism

James Carafano, May 21, 2015, Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward, Dr. Carafano is

Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow, Charles Stimson is Manager, National Security Law Program and Senior Legal Fellow, Dr. Steven Bucci is Director, Douglas and Sarah Allison Center for Foreign and National Security Policy, John Malcolm is Director, Edwin Meese III Center for Legal and Judicial Studies, and the Ed Gilbertson and Sherry Lindberg Gilbertson Senior Legal Fellow, <http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward> DOA: 5-24-15

The United States is in a state of armed conflict against al-Qaeda, the Afghan Taliban, ISIS, and associated forces. It must therefore rely on all lawful tools of national security, including but not limited to robust signals intelligence.

As the 9/11 Commission Report made crystal clear, one of the key failures of the United States before the 9/11 attacks was the government's inability to "connect the dots" between known or suspected terrorists. The artificial "wall" between domestic law enforcement and U.S. intelligence agencies, enacted during the 1990s, proved to be America's Achilles' heel. **Some analysts believe that had America had a Section 215-type program in place before 9/11, U.S. intelligence, along with domestic law enforcement, would have been able to connect the dots and prevent at least some of the hijackers from launching their devastating attack.** In fact, according to a report by the House Permanent Select Committee on Intelligence, using **the authorities under Section 215 and 702 of the PATRIOT Act has contributed to thwarting 54 total international terrorist plots in 20 countries. Thirteen of those plots were directed inside the United States.**

Section 702 Programs/PRISM Necessary to Defeat Terrorism

PRISM is key to disrupt foreign safe havens.

Dahl, Naval Postgraduate School national security affairs professor, 2013

(Erik, “Discussion Point: It’s not Big Data, but Little Data, that Prevents Terrorist Attacks”, 7-25, http://calhoun.nps.edu/bitstream/handle/10945/35903/Discussion%20Point_%20It%E2%80%99s%20not%20Big%20Data%2c%20but%20Little%20Data%2c%20that%20Prevents%20Terroris.pdf?sequence=1)

Research I am currently conducting for the National Consortium for the Study of Terrorism and Responses to Terrorism (START), together with my colleagues Martha Crenshaw and Margaret Wilson, can shed some light on how this NSA data may be used. We are studying unsuccessful terrorist plots, in hopes of finding out what tools and techniques are the most useful in preventing attacks. One finding supports the NSA’s argument that the data they are collecting can be useful in preventing future attacks. Opponents have suggested that the NSA data might only be useful in tracking down terrorists after the fact; because those haystacks of information are not apparently being looked at in real time, they are unlikely to help prevent future attacks. But the history of terrorist plots and attacks within the United States since 9/11 shows that most plots take a long time to develop. Even terrorist actions involving only one or two people typically take months or even years to plan and attempt. This is good news, because it gives law enforcement time to discover what’s going on, and it also gives the NSA time to search those haystacks it’s been collecting. But another one of our findings is that the most effective tools in preventing terrorist attacks are relatively simple, old fashioned police methods, such as the use of undercover officers, informants, and tips from the public. This is especially true for domestic plots and attacks: of the 109 failed plots within the United States since 9/11, more than 75 percent were foiled at least in part because of traditional law enforcement methods, and not—from what we can gather—from NSA surveillance. Thus it is not surprising that government officials have said most of the 50 or so plots that have been foiled by the NSA monitoring programs were overseas³. In other countries we can’t necessarily rely on local authorities, and spying—whether conducted by the NSA or the CIA—is a critical tool for our national security. But here in the U.S., the most important terrorism prevention tool remains the country’s 800,000 police officers, deputy sheriffs, and other local law enforcement officials, supported by members of the public who “see something and say something,” calling authorities when something doesn’t look right. These NSA programs do appear to be important for preventing terrorist attacks, and they make sense from an intelligence perspective. But their greatest value concerns threats overseas, and this is probably a good thing, because it means that if the programs are managed properly, and if our intelligence oversight mechanisms work as they should (which are admittedly big ifs), the NSA collection of big data will have relatively little impact on most Americans’ lives.

Program 702 has a track record of success.

Margulies, Roger Williams law professor, 2014

(Peter, “Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden”, 9-10, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2400809)

According to the President’s Review Group, which President Obama commissioned to study surveillance after the Snowden disclosures, § 702 has played a concrete role in keeping the nation safe.⁹¹ The Review Group’s report asserted that § 702 was “critical” to the uncovering of the Zazi planned subway attack in New York in 2009 and led to the arrest of Zazi and his accomplices.⁹² The § 702 program resulted in fifty-three out of fifty-four instances in obtaining information that “contributed in some degree” to a successful outcome regarding thwarted terrorist attacks in the U.S. and other countries.⁹³ According to

the Review Group, § 702 “does in fact play an important role in the nation’s effort to prevent terrorist attacks across the globe.” The Privacy and Civil Liberties Oversight Board (PCLOB) agreed with this assessment, concluding that collection under § 702 “significantly aids the government’s efforts to prevent terrorism... combat weapons proliferation and gather foreign intelligence.”⁹⁴

The plan enforces too much of a law enforcement paradigm on the NSA which is not designed to disrupt national security threats.

Yoo, Berkeley law professor, 2013

(John, “The Legality of the National Security Agency’s Bulk Data Surveillance Programs”, 12-1, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192)

The real problem with FISA, and even the Patriot Act, as they existed before the 2008 Amendments, is that they remained rooted in a law enforcement approach to electronic surveillance. They tied the government’s counter-terrorism efforts to individualized suspicion. Searches and wiretaps had to target a specific individual already believed to be involved in harmful activity. But detecting al Qaeda members who have no previous criminal record in the United States, and who are undeterred by the possibility of criminal sanctions, requires the use of more sweeping methods. To successfully prevent attacks, the government has to devote surveillance resources where there is a reasonable chance that terrorists will appear, or communicate, even if their specific identities remain unknown. What if the government knew that there was a fifty percent chance that terrorists would use a certain communications pipeline, such as e-mails provided by a popular Pakistani ISP, but that most of the communications on that channel would not be linked to terrorism? An approach based on individualized suspicion would prevent computers from searching through that channel for the keywords or names that might suggest terrorist communications, because there are no specific al Qaeda suspects, and thus no probable cause. Rather than individualized suspicion, searching for terrorists depends on playing the probabilities, just as roadblocks or airport screenings do. The private owner of any website has detailed access to information about the individuals who visit the site that he can exploit for his own commercial purposes, such as selling lists of names to spammers, or gathering market data on individuals or groups. Is the government’s effort to find violent terrorists a less legitimate use of such data? Individualized suspicion dictates the focus of law enforcement, but war demands that our armed forces defend the country with a broader perspective. Armies do not meet a “probable cause” requirement when they attack a position or fire on enemy troops or intercept enemy communications on a frequency. In the criminal justice system the purpose is to hold a specific person responsible for a discrete crime that has already happened. It does not make sense when the purpose of intelligence is to take action, such as killing or capturing members of the enemy, to prevent future harm to the nation from a foreign threat. FISA should be regarded as a safe harbor that allows the fruits of an authorized search to be used for prosecution. Using FISA sacrifices speed and breadth of information in favor of individualized suspicion but it provides a path for using evidence in a civilian criminal prosecution. If the President chooses to rely on his constitutional authority alone to conduct warrantless searches, then he should generally only use the information for military purposes. The primary objective of the NSA program is to “detect and prevent” possible al Qaeda attacks on the United States, whether another attack like September 11; a bomb in apartment buildings, bridges, or transportation hubs such as airports; or a nuclear, biological, or chemical attack. These are not hypotheticals; they are all al Qaeda plots, some of which U.S. intelligence and law enforcement agencies have already stopped. A President will want to use information gathered by the NSA to deploy military, intelligence, and law enforcement personnel to stop the next attack. The price to pay for speed, however, is foregoing any future criminal prosecution. If the President wants to use the NSA to engage in warrantless searches, he

cannot use its fruits in an ordinary criminal prosecution. Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them. The primary way to stop those attacks is to find and stop al Qaeda operatives, and the best way to find them is to intercept their electronic communications. Properly understood, the Constitution does not subject the government to unreasonable burdens in carrying out its highest duty of protecting the nation from attack.

Speed is vital to track intelligence leads—the threshold for a burdensome delay is low.

Yoo, Berkeley law professor, 2013

(John, “The Legality of the National Security Agency’s Bulk Data Surveillance Programs”, 12-1, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192)

As the United States fought the Afghanistan and Iraq wars, and continues to pursue al Qaeda groups in the Middle East and Africa, it captured al Qaeda laptops, cell phones, financial documents, and the other signs of modern high-tech life. This gave intelligence officers the information on dozens or hundreds of e-mail addresses, telephones, bank and credit account numbers, and residential and office addresses used by their network.³⁵ To exploit this, U.S. intelligence services must follow those leads as fast as possible, before the network of al Qaeda operatives can migrate to a new leader. An e-mail lead can disappear as fast as it takes someone to open a new e-mail account. FISA, and the law enforcement mentality it embodies, creates several problems. FISA requires “probable cause” to believe that someone is an agent of a foreign power before one can get a warrant to collect phone calls and e-mails.³⁶ An al Qaeda leader could have a cell phone with 100 numbers in its memory, 10 of which are in the United States and thus require a warrant. Would a FISA judge have found probable cause to think the users of those 10 numbers are al Qaeda too? Probably not. Would our intelligence agencies even immediately know who was using those numbers at the time of captured al Qaeda leader’s calls? The same is true of his e-mail, as to which it will not be immediately obvious what addresses are held by U.S. residents. In our world of rapidly shifting e-mail addresses, multiple cell phone numbers, and internet communications, FISA imposes slow and cumbersome procedures on our intelligence and law enforcement officers.³⁷ These laborious checks are based on the assumption that we remain within the criminal justice system, and looking backward at crimes in order to conduct prosecutions, rather than within the national security system, which looks forward in order to prevent attacks on the American people.³⁸ FISA requires a lengthy review process, in which special FBI and DOJ lawyers prepare an extensive package of facts and law to present to the FISC.³⁹ The Attorney General must personally sign the application, and another high-ranking national security officer, such as the President’s National Security Advisor or the Director of the FBI, must certify that the information sought is for foreign intelligence.⁴⁰ Creating an existing database of numbers that can be quickly searched can allow the government to take advantage of captured al Qaeda numbers abroad, before the cells within the United States break their contacts.

PRISM key to CT – 2NC

Collection increases efficiency

Margulies, Roger Williams law professor, 2014

(Peter, “Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden”, 9-10, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2400809)

Both bulk collection of metadata under § 215 and foreign content collection under §702 served this fiduciary goal. While the metadata program’s benefits were more diffuse, it allowed the government to quickly and reliably map out the contacts of known terrorist entities and operatives.²⁸ That capability generated investigative leads, even granting critics’ contention that the program did not by itself foil a specific attack.²⁹ Moreover, the program played a useful role in allocating government resources. In chaotic situations such as the aftermath of the Boston Marathon bombing, the program enabled investigators to discern early on that the Tsarnaev brothers acted without foreign help, freeing officials to concentrate on the domestic realm.³⁰ **Even critics of the metadata program have agreed that § 702 has assisted the government in obtaining information “efficiently and effectively about foreign targets overseas.”**³¹

Broad NSA capabilities are key to respond to adaptive threats.

Gjelten, NPR correspondent, 2013

(Tom, “The Case For Surveillance: Keeping Up With Terrorist Tactics”, 6-15, <http://www.npr.org/2013/06/15/191694315/high-tech-surveillance-targets-evolving-terrorist-tactics>)

Since public revelations that the National Security Agency is collecting telephone records and reviewing Internet communications in the U.S. and abroad, officials have been making the case that the programs are vital. They argue that the tactics match the new ways terrorists are planning and communicating. There was a time when America’s enemies conspired face-to-face, or communicated through couriers, or by leaving messages for each other somewhere. But in the digital age, that has changed. FBI Director Robert Mueller made that point back in 2008, as Congress considered whether to amend the Foreign Intelligence Surveillance Act. “In this day and age, our ability to gain intelligence on the plans, the plots of those who wish to attack us is dependent on us obtaining information relating to cellphones, Internet, email, wire transfers, all of these areas,” he said. If all the action was in that electronic space five years ago, it's even more so today, as intelligence and security officials constantly point out. Speaking in February, the NSA’s general counsel, Rajesh De, threw out some figures on the explosive growth in communication data. “More data crosses the Internet every second today than existed on the Internet 20 years ago. Global mobile traffic grew 70 percent last year alone,” he said. **Officials say these trends highlight the challenge facing spy agencies: With so much communication now taking place in the digital world, intelligence officers have to be able to follow that communication.** James Bamford, the author of several books on the NSA, says spies used to focus on getting human sources inside an organization — agents who could report on what people in the organization were saying and doing. But human sources no longer matter so much, Bamford says. Intelligence officers use new approaches because their adversaries are interacting in new ways. “During the day, they're on cellphones, or they're on email, or they're on social-networking sites. By intercepting that information, you develop patterns and look at who these people might be

involved with," he says. To justify the NSA's collection of telephone records and its selective monitoring of online communication overseas, U.S. officials cite these "revolutionary" changes in the information space. John Negroponte was the director of National Intelligence when wiretapping programs were expanded during the Bush administration. He defends the NSA's new emphasis. "I'd say it's a testament to how surveillance methods have kept up with the geometric progression of these communication methods," he says. Congressional critics of the expanded surveillance operations say they're not convinced that these programs have really proved their value in fighting terrorism. They ask whether other types of intelligence gathering might be just as effective. Negroponte, who served as U.S. ambassador to Iraq, says no one method is sufficient. He recalls how in 2006, the combination of different intelligence sources led the U.S. military to the head of al-Qaida in Iraq, Abu Musab al-Zarqawi. "I believe his phone number was detected through human intelligence. Somebody gave us his phone number. Then, that phone number was monitored through signals intelligence. And then his movements were tracked by geo-spatial intelligence — drones and so forth," he says. "So it's actually the integration of these different methodologies that actually give you the best results." The expanded use of telephone and Internet surveillance is in part an adaptation to the information revolution. The NSA, the CIA and other agencies will defend these programs vigorously on that basis, despite concerns that Americans' privacy has been put at risk. But that's not the whole story: **It's also clear that the programs are popular in the spy business simply because they're convenient and efficient. They make intelligence gathering easier**

PRISM Key to Cyber

PRISM is vital to securing internet communications to disrupt cyber terrorism and foreign espionage.

Dart, CIO and ICT director veteran, 2013

(Martin, “Doing their job: in defence of PRISM”, 6-11, <http://www.abc.net.au/news/2013-06-12/dart-in-defence-of-prism/4749108>)

With all developed countries hugely dependent upon electronic communications it is unthinkable to leave these systems unmonitored and undefended, writes Martin Dart. So the NSA monitors the Internet and captures email, phone calls, SMS message and... well whatever else travels over the internet. As soon as the 'news' broke civil libertarians were wailing about what an evil act this was, and wagging their fingers at the NSA as they finally had their proof that the NSA is a... well, a signals interception agency. That spies on things and collects data. Secretly. Oh come on. I can't be the only person longing for a little adult conversation about this. Surely? Don't forget that network monitoring and data gathering is what the NSA has done for over 60 years. Their mission is clearly up there on their website for all to see: Executive Order 12333 delineates the NSA role...to... Collect (including through clandestine means), process, analyze... signals intelligence information and data for foreign intelligence and counterintelligence purposes. (My emphasis - try reading just those words!) Therefore what is the NSA, this publicly professed signals intercept agency, with a published remit to conduct counterintelligence supposed to do - where do you think their field of battle should be? With all developed countries hugely dependent upon electronic communications it is unthinkable to leave these systems unmonitored and undefended. The abuse and destruction that could be unleashed by criminals and foreign intelligence services would be unprecedented and catastrophic, and to have no visibility or functional mitigations against it would be a shocking negligence. Point #1 of my pro-PRISM defence is therefore: The internet is now the most 'critical infrastructure' we have. It must be policed, inspected, and protected. As the NSA is funded precisely to do this, that's what they must do, and up until now they have done so without letting the enemy know that we had the capability to see what they were up to. And this is where you have to really stop and appreciate the next point... Point #2: You know there are dreadful people, doing and planning horrendous things on the internet right? They are 'the enemy' to all of us. The web isn't all about the Twitterverse bragging about the perfect latte or how cuddly their cat is in less than 140 characters. There really are terrorists who seek to use the internet to spread violence and propaganda. There really are organised perverts sharing images of child rape for sexual and financial gain. And there really are agents working for foreign governments who use the web to steal intellectual property or uncover our military and intelligence capabilities. Point #3: This process only works when we ('the good guys') have an unknown capability that they ('the bad guys') don't know about. If our enemies think we have a poor capability, or that our laws prevent us from looking at certain traffic or sites, then guess where they are going to hide their malware, propaganda, and stolen data?

Broad NSA authority is key to network access and the future of cyber security.

Goldsmith, Harvard law professor, 2013

(Jack, “We Need an Invasive NSA”, 10-10,
<http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>)

Such cyber-intrusions threaten corporate America and the U.S. government every day.

“Relentless assaults on America’s computer networks by China and other foreign governments, hackers and criminals have created an urgent need for safeguards to protect these vital systems,” the Times editorial page noted last year while supporting legislation encouraging the private sector to share cybersecurity information with the government. It cited General Keith Alexander, the director of the NSA, who had noted a 17-fold increase in cyber-intrusions on critical infrastructure from 2009 to 2011 and who described the losses in the United States from cyber-theft as “the greatest transfer of wealth in history.”

If a “catastrophic cyber-attack occurs,” the Times concluded, “Americans will be justified in asking why their lawmakers ... failed to protect them.” The Times editorial board is quite right about the seriousness of the cyber- threat and the federal government’s responsibility to redress it. What it does not appear to realize is the connection between the domestic NSA surveillance it detests and the governmental assistance with cybersecurity it cherishes. To keep our computer and telecommunication networks secure, the government will eventually need to monitor and collect intelligence on those networks

using techniques similar to ones the Times and many others find reprehensible when done for counterterrorism ends. The fate of domestic surveillance is today being fought around the topic of whether it is needed to stop Al Qaeda from blowing things up. But the fight tomorrow, and the more important fight, will be about whether it is necessary to protect our ways of life embedded in computer networks.

Anyone anywhere with a connection to the Internet can engage in cyber-operations within the United States. Most truly harmful cyber-operations, however, require group effort and significant skill. The attacking group or nation must have clever hackers, significant computing power, and the sophisticated software—known as “malware”—that enables the monitoring, exfiltration, or destruction of information inside a computer. The supply of all of these resources has been growing fast for many years in governmental labs devoted to developing these tools and on sprawling black markets on the Internet. Telecommunication networks are the channels through which malware typically travels, often anonymized or encrypted, and buried in the billions of communications that traverse the globe each day. The targets are the communications networks themselves as well as the computers they connect—things like the Times’ servers, the computer systems that monitor nuclear plants, classified documents on computers in the Pentagon, the nasdaq exchange, your local bank, and your social-network providers.

To keep these computers and networks secure, the government needs powerful intelligence capabilities abroad so that it can learn about planned cyber-intrusions. It also needs to raise defenses at home. An important first step is to correct the market failures that plague cybersecurity. Through law or regulation, the government must improve incentives for individuals to use security software, for private firms to harden their defenses and share information with one another, and for Internet service providers to crack down on the botnets—networks of compromised zombie computers—that underlie many cyber-attacks. More, too, must be done to prevent insider threats like Edward Snowden’s, and to control the stealth introduction of vulnerabilities during the manufacture of computer components—vulnerabilities that can later be used as windows for cyber-attacks. And yet that’s still not enough. The U.S. government can fully monitor air, space, and sea for potential attacks from abroad. But it has limited access to the channels of cyber-attack and cyber-theft, because they are owned by private telecommunication firms, and because Congress strictly limits government access to private communications. “I can’t defend the country until I’m into all the networks,” General Alexander reportedly told senior government officials a few months ago. For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation. It will also allow it to discern patterns of malicious activity in the swarm of communications, even when it doesn’t possess the malware’s signature. And it will better enable the government to trace back an attack’s trajectory so that it can discover the identity and geographical origin of the threat.

PRISM key to Domestic Terrorism

**Key to disrupt homegrown terrorism
Sulmasy, Coast Guard academy law professor, 2013**

(Glenn, "Why we need government surveillance", 6-10,
<http://www.cnn.com/2013/06/10/opinion/sulmasy-nsa-snowden/>)

The current threat by al Qaeda and jihadists is one that requires aggressive intelligence collection and efforts. One has to look no further than the disruption of the New York City subway bombers (the one being touted by DNI Clapper) or the Boston Marathon bombers to know that the war on al Qaeda is coming home to us, to our citizens, to our students, to our streets and our subways. **This 21st century war is different and requires new ways and methods of gathering information.** As technology has increased, so has our ability to gather valuable, often actionable, intelligence. However, **the move toward "home-grown" terror will necessarily require, by accident or purposefully, collections of U.S. citizens' conversations with potential overseas persons of interest.** An open society, such as the United States, ironically needs to use this technology to protect itself. This truth is naturally uncomfortable for a country with a Constitution that prevents the federal government from conducting "unreasonable searches and seizures." American historical resistance towards such activities is a bedrock of our laws, policies and police procedures. **But what might have been reasonable 10 years ago is not the same any longer. The constant armed struggle against the jihadists has adjusted our beliefs on what we think our government can, and must, do in order to protect its citizens.**

PRISM Speed Key

Flexibility is key to quick action and intel Sulmasy, US Coast Guard Academy law faculty, 2009

(Glenn, "Anniversary Contributions: Use of Force: Executive Power: the Last Thirty Year", 30 U. Pa. J. Int'l L. 1355, lexis)

Since the attacks of 9/11, the original concerns noted by Hamilton, Jay, and Madison have been heightened. Never before in the young history of the United States has the need for an energetic executive been more vital to its national security. The need for quick action in this arena requires an executive response, particularly when fighting a shadowy enemy like al Qaeda. not the deliberative bodies opining on what and how to conduct warfare or determining how and when to respond. The threats from non-state actors, such as al Qaeda, make the need for dispatch and rapid response even greater. Jefferson's concerns about the slow and deliberative institution of Congress being prone to informational leaks are even more relevant in the twenty-first century. The advent of the twenty-four hour media only leads to an increased need for retaining enhanced levels of executive [*1362] control of foreign policy. This is particularly true in modern warfare. In the war on international terror, intelligence is vital to ongoing operations and prevention of attacks. Al Qaeda now has both the will and the ability to strike with the equivalent force and might of a nation's armed forces. The need to identify these individuals before they can operationalize an attack is vital. Often international terror cells consist of only a small number of individuals, making intelligence that much more difficult to obtain and even more vital than in previous conflicts. The normal movements of tanks, ships, and aircrafts that, in traditional armed conflict are indicia of a pending attack are not the case in the current "fourth generation" war. Thus, the need for intelligence becomes an even greater concern for the commanders in the field as well as the Commander-in-Chief.[¶] Supporting a strong executive in foreign affairs does not necessarily mean the legislature has no role at all. In fact, their dominance in domestic affairs remains strong. Additionally, besides the traditional roles identified in the Constitution for the legislature in foreign affairs - declaring war, ratifying treaties, overseeing appointments of ambassadors, etc. - this growth of executive power now, more than ever, necessitates an enhanced, professional, and apolitical oversight of the executive. An active, aggressive oversight of foreign affairs, and warfare in particular, by the legislature is now critical. Unfortunately, the United States - particularly over the past decade - has witnessed a legislature unable to muster the political will necessary to adequately oversee, let alone check, the executive branch's growing power. Examples are abundant: lack of enforcement of the War Powers Resolution abound the executive's unchecked invasions of Grenada, Panama, and Kosovo, and such assertions as the Authorization for the Use of Military Forces, the USA Patriot Act, military commissions, and the updated Foreign Intelligence Surveillance Act ("FISA"). There have been numerous grand-standing complaints registered in the media and hearings over most, if not all, of these issues. However, in each case, the legislature has all but abdicated their constitutionally mandated role and allowed the judicial branch to serve as the only real check on alleged excesses of the executive branch. This deference is particularly dangerous and, in the current environment of foreign affairs and warfare, tends to unintentionally politicize the Court.[¶] The Founders clearly intended the political branches to best serve the citizenry by functioning as the dominant forces in [*1363] guiding the nation's foreign affairs. They had anticipated the political branches to struggle over who has primacy in this arena. In doing so, they had hoped neither branch would become too strong. The common theme articulated by Madison: ambition counters ambition, n17 intended foreign affairs to be a "give and take" between the executive and legislative branches. However, inaction by the legislative branch on myriad policy and legal issues surrounding the "war on terror" has forced the judiciary to fulfill the function of questioning, disagreeing, and "checking" the executive in areas such as wartime policy, detentions at Guantanamo Bay, and tactics and strategy of intelligence collection. The unique nature of the conflict against international terror creates many areas where law and policy are mixed. The actions by the Bush administration, in particular, led to outliers from many on the left about his intentions and desire to unconstitutionally increase the power of the Presidency. Yet, the Congress never firmly exercised the "check" on the executive in any formal manner whatsoever.[¶] For example, many policymakers disagreed with the power given to the President within the Authorization to Use Military Force ("AUMF"), n18 Arguably, this legislation was broad in scope, and potentially granted sweeping powers to the President to wage the "war on terror." However, Congress could have amended or withdrawn significant portions of the powers it gave to the executive branch. This lack of withdrawal or amendment may have been understandable when Republicans controlled Congress, but as of November 2006, the Democrats gained control of both houses of the Congress. Still, other than arguing strongly against the President, the legislature did not necessarily or aggressively act on its concerns. Presumably this inaction was out of concern for being labeled "soft on terror" or "weak on national security" and thereby potentially suffering at the ballot box. This virtual paralysis is understandable but again, the political branches were, and remain, the trust voice of the people and provide the means to best represent the country's beliefs, interests, and national will in the arena of foreign affairs. It has been this way in the past but the more recent (certainly over the past thirty years and even more so in the past decade) intrusions of the judicial branch into what [*1364] was intended to be a "tug and pull" between the political branches can properly be labeled as an unintended consequence of the lack of any real legislative oversight of the executive branch.[¶] Unfortunately, now nine unelected, life-tenured justices are deeply involved in wartime policy decision making. Examples of judicial policy involvement in foreign affairs are abundant including *Rasul v. Bush*; n19 *Hamdi v. Rumsfeld*; n20 *Hamdan v. Rumsfeld*; n21 as well as last June's *Boumediene v. Bush* n22 decision by the Supreme Court, all impacting war policy and interpretation of U. S. treaty obligations. Simply, judges should not presumptively impact warfare operations or policies nor should this become acceptable practice. Without question, over the past thirty years, this is the most dramatic change in executive power. It is not necessarily the strength of the Presidency that is the change we should be concerned about - the institutional search for enhanced power was anticipated by the Founders - but they intended for Congress to check this executive tendency whenever appropriate. Unfortunately, this simply is not occurring in twenty-first century politics. Thus, the danger does not necessarily lie with the natural desire for Presidents to increase their power. The real danger is the judicial branch being forced, or compelled, to fulfill the constitutionally mandated role of the Congress in checking the executive.[¶] 4. PRESIDENT OBAMA AND EXECUTIVE POWER[¶] The Bush presidency was, and continues to be, criticized for having a standing agenda of increasing the power of the executive branch during its eight-year tenure. Numerous articles and books have been dedicated to discussing these allegations. n23 However, as argued earlier, the reality is that it is a natural bureaucratic tendency, and one of the Founders presciently anticipated, that each branch would seek greater powers whenever and wherever possible. As the world becomes increasingly interdependent, technology and armament become more sophisticated, and with [*1365] the rise of twenty-first century non-state actors the need for strong executive power is not only preferred, but also necessary. Executive power in the current world dynamic is something, regardless of policy preference or political persuasions, that the new President must maintain in order to best fulfill his constitutional role of providing for the nation's security. This is simply part of the reality of executive power in the twenty-first century. n24

Speed is key to the strategic advantage key to solve global crises and maintain leadership Berkowitz, RAND senior analyst, 2008

(Bruce, Strategic Advantage: Challengers, Competitors, And Threats To America's Future, pg 1-4)

THIS BOOK is intended to help readers better understand the national security issues facing the United States today and offer the general outline of a strategy for dealing with them. National security policy—both making it and debating it—is harder today because the issues that are involved are more numerous and varied. The problem of the day can change at a moment's notice. Yesterday, it might have been proliferation; today, terrorism; tomorrow, hostile regional powers. Threats are also more likely to be intertwined—proliferators use the same networks as narco-traffickers, narco-traffickers support terrorists, and terrorists align themselves with regional powers. Yet, as worrisome as these immediate concerns may be, the long-term challenges are even harder to deal with, and the stakes are higher. Whereas the main Cold War threat—the Soviet Union—was brittle, most of the potential adversaries and challengers America now faces are resilient. In at least one dimension where the Soviets were weak (economic efficiency, public morale, or leadership), the new threats are strong. They are going to be with us for a long time. As a result, we need to reconsider how we think about national security. The most important task for U.S. national security today is simply to retain the strategic advantage. This term, from the world of military doctrine, refers to the overall ability of a nation to control, or at least influence, the course of events.¹ When you hold the strategic advantage, situations unfold in your favor, and each round ends so that you are in an advantageous position for the next. When you do not hold the strategic advantage, they do not. As national goals go, “keeping the strategic advantage” may not have the idealistic ring of “making the world safe for democracy” and does not sound as decisively macho as “maintaining American hegemony.” But keeping the strategic advantage is critical, because it is essential for just about everything else America hopes to achieve—promoting freedom, protecting the homeland, defending its values, preserving peace, and so on. The Changing Threat If one needs proof of this new, dynamic environment, consider the recent record. A search of the media during the past fifteen years suggests that there were at least a dozen or so events that were considered at one time or another the most pressing national security problem facing the United States—and thus the organizing concept for U.S. national security. What is most interesting is how varied and different the issues were, and how many different sets of players they involved—and how each was replaced in turn by a different issue and a cast of characters that seemed, at least for the moment, even more pressing. They included, roughly in chronological order, • regional conflicts—like Desert Storm—involving the threat of war between conventional armies; • stabilizing “failed states” like Somalia, where government broke down in toto; • staying economically competitive with Japan; • integrating Russia into the international community after the fall of communism and controlling the nuclear weapons it inherited from the Soviet Union; • dealing with “rogue states,” unruly nations like North Korea that engage in trafficking and proliferation as a matter of national policy; • combating international crime, like the scandal involving the Bank of Credit and Commerce International, or imports of illegal drugs; • strengthening international institutions for trade as countries in Asia, Eastern Europe, and Latin America adopted market economies; • responding to ethnic conflicts and civil wars triggered by the reemergence of culture as a political force in the “clash of civilizations”; • providing relief to millions of people affected by natural catastrophes like earthquakes, tsunamis, typhoons, droughts, and the spread of HIV/AIDS and malaria; • combating terrorism driven by sectarian or religious extremism; • grassroots activism on a global scale, ranging from the campaign to ban land mines to antiglobalization hoodlums and environmentalist crazies; • border security and illegal immigration; • the worldwide ripple effects of currency fluctuations and the collapse of confidence in complex financial securities; and • for at least one fleeting moment, the safety of toys imported from China. There is some overlap in this list, and one might want to group some of the events differently or add others. The important point, however, is that when you look at these problems and how they evolved during the past fifteen years, you do not see a single lesson or organizing principle on which to base U.S. strategy. Another way to see the dynamic nature of today's national security challenges is to consider the annual threat briefing the U.S. intelligence community has given Congress during the past decade. These briefings are essentially a snapshot of what U.S. officials worry most about. If one briefing is a snapshot, then several put together back to back provide a movie, showing how views have evolved.² Figure 1 summarizes these assessments for every other year between 1996 and 2006. It shows when a particular threat first appeared, its rise and fall in the rankings, and in some cases how it fell off the chart completely. So, in 1995, when the public briefing first became a regular affair, the threat at the very top of the list was North Korea. This likely reflected the crisis that had occurred the preceding year, when Pyongyang seemed determined to develop nuclear weapons, Bill Clinton's administration seemed ready to use military action to prevent this, and the affair was defused by an agreement brokered by Jimmy Carter. Russia and China ranked high as threats in the early years, but by the end of the decade they sometimes did not even make the list. Proliferation has always been high in the listings, although the particular countries of greatest concern have varied. Terrorism made its first appearance in 1998, rose to first place after the September 11, 2001, terrorist attacks, and remains there today. The Balkans appeared and disappeared in the middle to late 1990s. A few of the entries today seem quaint and overstated. Catastrophic threats to information systems like an “electronic Pearl Harbor” and the “Y2K problem” entered the list in 1998 but disappeared after 2001. (Apparently, after people saw an airliner crash into a Manhattan skyscraper, the possible loss of their Quicken files seemed a lot less urgent.) Iraq first appeared in the briefing as a regional threat in 1997 and was still high on the list a decade later—though, of course, the Iraqi problem in the early years (suspected weapons of mass destruction) was very different from the later one (an insurgency and internationalized civil war). All this is why the United States needs agility. It not only must be able to refocus its resources repeatedly; it needs to do this faster than an adversary can focus its own resources.

Speed key to solve terrorism-prefer specific evidence Li, Georgetown JD, 2009

(Zheyao, "NOTE: War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare", Winter, 7 Geo. J.L. & Pub. Pol'y 373, lexis)

By now it should be clear just how different this conflict against the extremist terrorists is from the type of warfare that occupied the minds of the Framers at the time of the Founding. Rather than maintaining the geographical and political isolation desired by the Framers for the new country, today's United States is an international power targeted by individuals and groups that will not rest until seeing her demise. The Global War on Terrorism is not truly a war within the Framers' eighteenth-century conception of the term, and the normal constitutional provisions regulating the division of war powers between Congress and the President do not apply. Instead, this "war" is a struggle for survival and dominance against forces that threaten to destroy the United States and her allies, and the fourth-generational nature of the conflict, highlighted by an indiscernible distinction between wartime and peacetime, necessitates an evolution of America's traditional constitutional warmaking scheme. As first illustrated by the military strategist Colonel John Boyd, constitutional decision-making in the realm of war powers in the fourth generation should [*399] consider the implications of the OODA Loop: Observe, Orient, Decide, and Act. n144 In the era of fourth-generational warfare, quick reactions, proceeding through the OODA Loop rapidly, and disrupting the enemy's OODA loop are the keys to victory. "In order to win," Colonel Boyd suggested, "we should operate at a faster tempo or rhythm than our adversaries" n145 In the words of Professor Creveld, "[b]oth organizationally and in terms of the equipment at their disposal, the armed forces of the world will have to adjust themselves to this situation by changing their doctrine, doing away with much of their heavy equipment and becoming more like police." n146 Unfortunately, the existing constitutional understanding, which diffuses war power between two branches of government, necessarily (by the Framers' design) slows down decision-making. [*400] In circumstances where war is undesirable (which is, admittedly, most of the time, especially against other nation-states), the deliberativeness of the existing decision-making process is a positive attribute. In America's current situation, however, in the midst of the conflict with al-Qaeda and other international terrorist organizations, the existing process of constitutional decision-making in warfare may prove a fatal hindrance to achieving the initiative necessary for victory. As a slow-acting, deliberative body, Congress does not have the ability to adequately deal with fast-emerging situations in fourth-generational warfare. Thus, in order to combat transnational threats such as al-Qaeda, the executive branch must have the ability to operate by taking offensive military action even without congressional authorization, because only the executive branch is capable of the swift decision-making and action necessary to prevail in fourth-generational conflicts against fourth-generational opponents.

Section 702 critical to fight terrorism

Washington Post, June 20, 2013, Reprinted in South China Morning Post, US Defends Surveillance Tactics in War on Terrorism, <http://www.scmp.com/news/world/article/1264602/us-defends-surveillance-tactics-war-terrorism> DOA: 4-1-15

In November 2008, Abid Naseer, a Pakistani student living in Manchester, England, began to e-mail a Yahoo account ultimately traced to his home country. The young man's e-mails appeared to be about four women - Nadia, Huma, Gulnaz and Fozia - and which one would make a "faithful and loving wife". British investigators later determined that the four names were code for types of explosives. And they ascertained that a final April 2009 e-mail announcing a "marriage to Nadia" between the 15th and the 20th was a signal that a terrorist attack was

imminent, according to British court documents. It is unclear exactly how British intelligence linked the Pakistani e-mail address to a senior al-Qaeda operative who communicated in a kind of code to his distant allies. But the intelligence helped stop the plot in England, and the address made its way to the US National Security Agency (NSA). A few months later, the NSA was monitoring the Yahoo user in Pakistan when a peculiar message arrived from a man named Najibullah Zazi, an Afghan American living in Colorado. He asked about "mixing of [flavour and ghee oil] and I do not know the amount, plz right away." Soon after, on September 9, 2009, a second message arrived that echoed the code used in the British plot: "The marriage is ready," Zazi wrote. The e-mails led the NSA to alert the FBI, which obtained a court order to place Zazi under more extensive surveillance. Officials learned that he had visited Pakistan in 2008, the same time as one of the British plotters. In the end, the e-mails and additional surveillance foiled a plot by Zazi and two others to conduct suicide bombings in the New York subway system just days after he sent the "marriage is ready" e-mail. In recent days, US intelligence and law enforcement officials, as well as congressional officials, have pointed to the authority that allowed them to target the Yahoo account - Section 702 of the Foreign Intelligence Surveillance Act (FISA) - as a critical tool in identifying and disrupting terrorist plots in the US and abroad. But some critics of NSA surveillance suggested that the collection of data under a programme called Prism was not essential to Zazi's capture because the British first obtained the critical e-mail address. Still, the case study provides a rare glimpse of how the broad surveillance practices of the United States, often in concert with allies, are deployed. "The 702 programme has been enormously useful in a large number of terrorist cases," said a US official who has access to classified records on NSA programmes. "It's beyond dispute that it is highly effective. It operates exactly as anyone paying attention would have expected it to operate based on floor debate and plain reading of law." Passage of Section 702 as an amendment to FISA in 2008 gave the government the authority to request information from US telecommunications companies on foreign targets located overseas without a court order for each individual case.

The broad authority is reviewed and renewed annually by the FISA court, although the law does not preclude making a specific request for surveillance. "It appears the NSA did not need any of the expanded authorities conferred by Section 702 to monitor the communications at issue," said Elizabeth Goitein, co-director of the Brennan Centre for Justice's Liberty and National Security Programme. "The government easily could have met this standard if it certified that the targets were al-Qaeda terrorists in Pakistan." But US officials argue that, given the flood of leads in today's interconnected world, the system would get bogged down and they could miss plots if they had to go before the court every time they got information about potential foreign suspects. The officials said they used material from multiple sources - allies, agents, informants and other investigations - to provide rolling targeting information for the Prism program.

They also said if the Yahoo address had not been included, Zazi might not have been identified just days before the attacks were set to occur. In testimony before Congress on Tuesday, senior intelligence and law enforcement officials said that recently revealed surveillance programmes have disrupted more than 50 "potential terrorist events", including at least 10 plots with a connection in the US. The Zazi case was one of four that officials used in recent days to defend the effectiveness of the surveillance programmes. One of the others was a planned attack on a Danish newspaper that involved a Pakistani American, David Headley.

Sean Joyce, the deputy director of the FBI, described the other two potential attacks on Tuesday in testimony before the House Intelligence Committee. In one, Joyce said, the NSA was monitoring "a known extremist in Yemen" when it learned that the individual was in contact with a man in Kansas City, Missouri. Joyce said Khalid Ouazzani and two co-conspirators were plotting to bomb the New York Stock Exchange. Ouazzani pleaded guilty in 2010 to supporting a terrorist organisation, bank fraud and overseas money laundering. His co-conspirators also pleaded guilty to terrorism charges. In the other incident, phone records helped identify a San Diego man who was financing a terrorist group overseas, apparently al-Shabab in Somalia.

"Investigating terrorism is not an exact science. It's like a mosaic," Joyce said. "We try to take these disparate pieces and bring them together to form a picture. There are many different pieces of intelligence. "We have assets. We have physical surveillance. We have electronic surveillance through a legal process, phone records through additional legal process, financial records. "Also, these programmes that we're talking about here today, they're all valuable pieces to bring that mosaic together." General Keith Alexander, head of the National Security Agency, said details of the two programmes disclosed by Snowden were not closely held within the secretive agency. Alexander said after the hearing that most of the documents accessed by Snowden, a former systems analyst on contract to the NSA, were on a web forum available to NSA employees. Others were on a site that required a special credential to access. Alexander said investigators were studying how Snowden did that. He told lawmakers Snowden's leaks had caused "irreversible and significant damage to this nation". He also said the internet programme had helped stop 90 per cent of the 50-plus plots he cited. He said more than 10 of the plots thwarted had a link inside the US. Still, little was offered to substantiate claims that the programmes had been successful in stopping acts of terrorism that would not have been caught with narrower surveillance. In the New York subway bombing case, Barack Obama conceded the would-be bomber might have been caught with less sweeping surveillance. Committee chairman Congressman Mike Rogers said the programmes were vital to the intelligence community and blasted Snowden's actions as criminal. "It is at times like these where our enemies within become almost as damaging as our enemies on the outside," Rogers said. Officials acknowledged that intelligence collected from US phone records under a programme authorised by the USA Patriot Act is less compelling and the case for that extensive surveillance is harder to make. The NSA's ability to intercept "the contents of e-mail communications of bad guys overseas provides a more lucrative set of information" about terrorist activity than its access to phone records of millions of Americans, one US official said.

Section 702 programs necessary to defeat terrorism

Sean M. **Joyce**, Deputy Director, Federal Bureau of Investigation (FBI), **July 31**, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hsdl.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

SEN. GRASSLEY: OK.

Mr. Joyce, one part of the balance that we have to strike, protecting privacy of Americans -- the other part, national security. Thankfully, until the Boston bombing, we had prevented large-scale terrorist attacks on American soil. I have a few questions about how valuable the role of Section 215 and 702 programs have played in predicting (sic) our national security. Two questions, and then I'll have to stop and go to our colleagues. Can you describe any specific situations where Section 215 and Section 702 authorities helped disrupt a terrorist attack or identify individuals planning to attack, the number of times? And then secondly, if you didn't have the authority to collect phone records in bulk the way that they are now under Section 215, how would you have affected those investigations?

MR. JOYCE: So to your first question, Senator, as far as a specific example of when we have utilized both of these programs is the one I had first mentioned, the first al-Qaida-directed plot since 9/11, in September of 2009, when Najibullah Zazi and others conspired plot to bomb the New York subway system. We initially found out about Zazi through an NSA 702 coverage, and he was actually talking to an al-Qaida courier who was -- he was asking for his help to perfect an explosives recipe. So but for that, we would not have known about the plot. We followed that up with legal process and then had FISA coverage on him and others as we fully investigated the plot. Business records 215 was also involved, as I had previously mentioned, where we also through legal process were submitting legal process for telephone numbers and other email addresses, other selectors. But NSA also provided another number we are unaware of of a co-conspirator, Adis Medunjanin. So that is an instance where a very serious plot to attack America on U.S. soil that we used both these programs.

But I say, as Chairman Leahy mentioned, there is a difference in the utility of the programs. But what I say to you is that each and every program and tool is valuable. There were gaps prior to 9/11. And what we have collectively tried to do, the members of the committee, other members of the other oversight committees, the executive branch and the intelligence community, is we have tried to close those gaps and close those seams. And the business record 215 is one of those programs that we have closed those seams. So I respectfully say to the chairman that the utility of that specific program initially is not as valuable. I say you are right. But what I say is it plays a crucial role in closing the gaps and seams that we fought hard to gain after the 9/11 attacks.

Section 702 critical to defeat terrorism

Benjamin Wittenberg, Brookings, 2014, Senior Fellow in Governance Studies at the Brookings Institution. I co-founded and am Editor in Chief of *Lawfare*, a website devoted to sober and serious discussion of “Hard National Security Choices.” I am the author or editor of several books on subjects related to law and national security: *Detention and Denial: The Case for Candor After Guantánamo* (2011), *Law and the Long War: The Future of Justice in the Age of Terror* (2008), and *Legislating the War on Terror: An Agenda for Reform* (2009). I have written extensively both on the AUMF and on NSA collection under various provisions of the Foreign Intelligence Surveillance Act (FISA).³ The views I am expressing here are my own, April 8, Prepared Statement, Is Al Qaeda Winning the Administration’s Counterterrorism Policy,”

<http://docs.house.gov/meetings/FA/FA18/20140408/102109/HHRG-113-FA18-Wstate-WittesB-20140408.pdf> DOA: 5-1-15

President Obama has announced that he wants to end the AUMF conflict, raising profound questions both about the plausibility and timeframe of that objective and about what legal instrument—if any—will replace the AUMF. Meanwhile, serial leaks have generated enormous political anxiety about NSA programs and persistent calls for reform in the press, in the general public, among allies, and in this body. Section 702 will sunset in 2017 absent action by Congress to renew this important collection authority.⁴ So major pillars of the legal architecture of America’s conflict with Al Qaeda have been placed—in different ways and for very different reasons—on the table. This body thus cannot avoid the question of how much, if at all, it wants to alter the most fundamental architecture of the conflict.

In my view, as I will lay out, the critical task facing the Congress is different with respect to these two laws. With respect to the AUMF, the Congress should legislate to clearly authorize, and establish proper oversight of, the conflict the United States is likely to continue fighting after its withdrawal from Afghanistan. With respect to Section 702, the task is simpler: to maintain the intelligence community’s capacity to support both the broad national security objectives of the United States and the conflict’s prosecution under whatever legal authorities may succeed the AUMF.

CONTINUES

As I said at the outset of this statement, the question of intelligence collection under Section 702 of the FAA may seem connected to the AUMF’s future in only the most distant fashion. In fact, the connection between intelligence collection authorities and the underlying regime authorizing the conflict itself is a critical one. Good intelligence is key to any armed conflict and good technical intelligence is a huge U.S. strength in the fight against Al Qaeda. Yet ironically, the more one attempts to narrow the conflict, the more important technical intelligence becomes. The fewer boots on the ground we have in Afghanistan, for example, the greater our reliance will become on technical collection. The more we rely on drone strikes, rather than large troop movements, in areas where we lack large human networks, the more we rely on technical intelligence. Particularly if one imagines staying on offense against a metastasizing Al Qaeda in the context of a withdrawal from Afghanistan and a narrowing—or a formal end—of the AUMF conflict, the burden on technical intelligence collection to keep us in the game will be huge even ignoring the many other foreign intelligence and national security interests Section 702 surveillance supports.

Section 702 is a complicated statute, and it is only one part of a far more complicated, larger statutory arrangement. But broadly speaking, it permits the NSA to acquire without an individualized warrant the communications of non-US persons reasonably believed to be overseas when those communications are transiting the United States or stored in the United States. Under these circumstances, the NSA can order production of such communications from telecommunications carriers and internet companies under broad programmatic orders issued by the Foreign Intelligence Surveillance Court (FISC), which reviews both targeting and minimization procedures under which the collection then takes place. Oversight is thick, both within the executive branch, and in reporting requirements to the congressional intelligence committees.

Make no mistake: Section 702 is a very big deal in America's counterterrorism arsenal. It is far more important than the much debated bulk metadata program, which involves a few hundred queries a year. Section 702 collection, by contrast, is vast, a hugely significant component not only of contemporary counterterrorism but of foreign intelligence collection more generally. In 2012, the Senate Select Committee on Intelligence wrote that “[T]he authorities provided [under section 702] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets. . . . [The] failure to reauthorize [section 702] would ‘result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities.’”⁸ The President's Review Group on Intelligence and Communications Technologies, after quoting this language, wrote that “Our own review is not inconsistent with this assessment. . . . [W]e are persuaded that section 702 does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe.”⁹ The *Washington Post* has reported that 702 was in 2012 the single most prolific contributor to the President's Daily Brief.¹⁰

Yet we have seen enormous anxiety about Section 702 collection, along with its close cousin, collection overseas against non-US person targets under Executive Order 12333. Sometimes, these anxieties have been rooted in the supposed effects of this collection on U.S. persons.¹¹ Sometimes, however, the complaints have stemmed from broader concerns about infringement of privacy worldwide. Europeans have expressed shock, for example, that a U.S. spy agency would presume to collect against an allied foreign leader like German Chancellor Angela Merkel¹²—surveillance that now seems forward-thinking and reasonable given later reports that Merkel has been on the phone frequently during the Crimea crisis with Vladimir Putin.¹³ Major news organizations have considered it front-page news that NSA has pursued intelligence targets on online gaming platforms and smartphone apps,¹⁴ that NSA has collected contact lists in large numbers around the world,¹⁵ even that foreign countries *spy on one another*, collect attorney-client communications involving U.S. lawyers along the way, and may share that material with NSA subject to U.S. law and minimization requirements.¹⁶ Whether one considers these stories important journalism or reckless blowing

of valuable surveillance activities, they both reflect and further stoke a deep concern about the scope of U.S. surveillance practices. And that concern is creating inexorable pressures for reforms we may regret in the counterterrorism space.

The legal regime here is one that this body knowingly and deliberatively created in an iterative set of interactions with the intelligence community and the courts. It requires no apology. Rather, it requires an active defense. And while there are certainly areas in which the regime could benefit from reform, the big risk here is that overreaction and panic in the face of exposure will lead to a burdening of the core signals intelligence capacity of the United States with legal processes designed to protect civil liberties domestically. This could happen either because reform efforts go too far or because Congress fails to reauthorize 702 and thus applies the terms of core FISA—which require an individualized warrant based on probable cause—to a wide swath of overseas collection.

Broadly then, the legislative task with respect to Section 702 is something of the opposite of the task with respect to the AUMF. To the extent that members of this committee continue to believe, as I do, in the essential integrity and value of the existing legal authorities for intelligence collection and oversight, the task in the current political environment is to defend that architecture—publicly and energetically—rather than to race to correct imagined deficiencies, or even real structural deficiencies that, however real they may be, bear little relation to the outcomes that disquiet us.

Section 702 and Section 215 programs have prevented terror attacks

Sean M. Joyce, Deputy Director, Federal Bureau of Investigation (FBI), July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"
<https://www.hslc.org/?view&did=741931>

(First joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the deputy chief of the division's public integrity section, went in private practice, sworn in as deputy attorney general on January 3rd, 2011)

SEN. FEINSTEIN: Good.

Now, the NSA has produced and declassified a chart, which I'd like to make available to all members. It has the 54 total events. It includes a Section 702 authority and Section 215 authority, which essentially work together. And it shows the events disrupted based on a combination of these two programs, 13 in the homeland, 25 in Europe, five in Africa and 11 in Asia.

Now, I remember I was on the Intelligence Committee before 9/11, and I remember how little information we have and the great criticism of the government because of those stovepipes, the

inability to share intelligence, the inability to collect intelligence. We had no program that could've possibly caught two people in San Diego before the event took place. I support this program. I think, based on what I know, they will come after us. And I think we need to prevent an attack wherever we can from happening. That doesn't mean that we can't make some changes.

Accessing foreign data stored in the US is crucial to deter terrorism

The Washington Post 13 ("US Defends Surveillance Tactics in War on Terrorism")

A few months later, the NSA was monitoring the Yahoo user in Pakistan when a peculiar message arrived from a man named Najibullah Zazi, an Afghan American living in Colorado. He asked about "mixing of [flavour and ghee oil] and I do not know the amount, plz right away."¶ Soon after, on September 9, 2009, a second message arrived that echoed the code used in the British plot: "The marriage is ready," Zazi wrote.¶ The e-mails led the NSA to alert the FBI, which obtained a court order to place Zazi under more extensive surveillance. Officials learned that he had visited Pakistan in 2008, the same time as one of the British plotters.¶ In the end, the e-mails and additional surveillance foiled a plot by Zazi and two others to conduct suicide bombings in the New York subway system just days after he sent the "marriage is ready" e-mail. In recent days, US intelligence and law enforcement officials, as well as congressional officials, have pointed to the authority that allowed them to target the Yahoo account - Section 702 of the Foreign Intelligence Surveillance Act (FISA) - as a critical tool in identifying and disrupting terrorist plots in the US and abroad.¶ But some critics of NSA surveillance suggested that the collection of data under a programme called Prism was not essential to Zazi's capture because the British first obtained the critical e-mail address.¶ Still, the case study provides a rare glimpse of how the broad surveillance practices of the United States, often in concert with allies, are deployed.¶ "The 702 programme has been enormously useful in a large number of terrorist cases," said a US official who has access to classified records on NSA programmes. "It's beyond dispute that it is highly effective. It operates exactly as anyone paying attention would have expected it to operate based on floor debate and plain reading of law." Passage of Section 702 as an amendment to FISA in 2008 gave the government the authority to request information from US telecommunications companies on foreign targets located overseas without a court order for each individual case.

Authority for PRISM is in section 702

James Carafano, 8-6, 13 Heritage Foundation, The Examiner (Washington, DC)m August 6, 2013, PRISM is essential to U.S. security in war against terrorism (Vice President for Defense and Foreign Policy Studies at The Heritage Foundation, PRISM is Essential to US Security in the War on Terrorism, <http://www.heritage.org/research/commentary/2013/8/prism-is-essential-to-us-security-in-war-against-terrorism> DOA: 2-1-13

"Our intelligence professionals must be able to find out who the terrorists are talking to, what they are saying, and what they're planning," said the president. "The lives of countless Americans depend on our ability to monitor these communications." He added that he would cancel his planned trip to Africa unless assured Congress would support the counterterrorism surveillance program. The president was not , Barack Obama. It was George W. Bush, in 2008, pressing Congress to extend and update reforms to the Foreign Intelligence Surveillance Act

(FISA). He was speaking directly to the American public, in an address broadcast live from the Oval Office. How times have changed. Back then, the President of the United States willingly led the fight for the programs he thought necessary to keep the nation safe. Now, our president sends underlings to make the case. In distancing himself from the debate over PRISM (the foreign intelligence surveillance program made famous by the world- travelling leaker , Edward Snowden), , President Obama followed the precedent he established in May at the National Defense University. There, he spoke disdainfully of drone strikes, the authorization to use military force against terrorists, and the detention facilities at Guantanamo Bay. All three are essential components of his counterterrorism strategy. In distancing himself from his own strategy, , Obama hoped to leave the impression that he is somehow above it all. He has dealt with the Snowden case the same way. When asked while traveling in Africa if he would take a role in going after the leaker, the president replied "I shouldn't have to." The White House's above-it-all attitude sends seriously mixed messages to the American people, who are trying to figure if the government's surveillance programs are legal and appropriate. Congress has not been much better. **The authority for PRISM is in FISA Section 702.** Congress debated these authorities in 2007 and again when the program was reauthorized in 2008. Senate Majority Leader Harry Reid, D-Nev., surely remembers the controversy. He wrote President Bush: "There is no crisis that should lead you to cancel your trip to Africa. But whether or not you cancel your trip, Democrats stand ready to negotiate a final bill, and we remain willing to extend existing law for as short a time or as long a time as is needed to complete work on such a bill." Evidently, Reid must have felt the authorities granted under Section 702 received a full and sufficient hearing. Most current members of Congress were seated under the dome during the 2008 debates. They had every opportunity not just to read the law, but to be briefed on the program by intelligence officials before voting on the bill. For them to act shocked at the scope of the program today rings about as hollow as , Obama's expressed disdain for the operations he oversees. The reality is that Congress and the administration share responsibility for these programs. If they want to change or modify them, who's stopping them? If changes are made, however, they should to be made for the right reason. Leaders must never compromise our security for political expediency. **At least 60 Islamist-inspired terrorist plots have been aimed at the U.S. since the 9/11 attacks. The overwhelming majority have been thwarted thanks to timely, operational intelligence about the threats.** Congress should not go back to a pre-11 set of rules just to appeal to populist sentiment. Congress and the White House have an obligation to protect our liberties and to safeguard our security -- in equal measure. Meeting that mission is more important than winning popularity polls.

NSA mass surveillance is critical – we’re drawing down in every other area of intelligence gathering which means it’s essential to preventing terrorism

Wittes 14 (Benjamin, Senior Fellow @ the Brookings Institute, April 8th 2014, "Is Al Qaeda Winning: Grading the Administration's Counter terrorism Policy, Brookings Institute)

As I said at the outset of this statement, the question of intelligence collection under Section 702 of the FAA may seem connected to the AUMF's future in only the most distant fashion. In fact, the connection between intelligence collection authorities and the underlying regime authorizing the conflict itself is a critical one. Good intelligence is key to any armed conflict and good technical intelligence is a huge U.S. strength in the fight against Al Qaeda. Yet ironically, the more one attempts to narrow the conflict, the more important technical intelligence becomes. The fewer boots on the ground we have in Afghanistan, for example, the greater our reliance will become on technical collection. The more we rely on drone strikes, rather than large troop movements, in areas where we lack large human networks, the more we

rely on technical intelligence. Particularly if one imagines staying on offense against a metastasizing Al Qaeda in the context of a withdrawal from Afghanistan and a narrowing—or a formal end—of the AUMF conflict, the burden on technical intelligence collection to keep us in the game will be huge even ignoring the many other foreign intelligence and national security interests Section 702 surveillance supports.[¶] Section 702 is a complicated statute, and it is only one part of a far more complicated, larger statutory arrangement. But broadly speaking, it permits the NSA to acquire without an individualized warrant the communications of non-US persons reasonably believed to be overseas when those communications are transiting the United States or stored in the United States. Under these circumstances, the NSA can order production of such communications from telecommunications carriers and internet companies under broad programmatic orders issued by the Foreign Intelligence Surveillance Court (FISC), which reviews both targeting and minimization procedures under which the collection then takes place. Oversight is thick, both within the executive branch, and in reporting requirements to the congressional intelligence committees.[¶] Make no mistake: Section 702 is a very big deal in America's counterterrorism arsenal. It is far more important than the much debated bulk metadata program, which involves a few hundred queries a year. Section 702 collection, by contrast, is vast, a hugely significant component not only of contemporary counterterrorism but of foreign intelligence collection more generally. In 2012, the Senate Select Committee on Intelligence wrote that “[T]he authorities provided [under section 702] have greatly increased the government’s ability to collect information and act quickly against important foreign intelligence targets. . . . [The] failure to reauthorize [section 702] would ‘result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities.’”^[8] The President’s Review Group on Intelligence and Communications Technologies, after quoting this language, wrote that “Our own review is not inconsistent with this assessment. . . . [W]e are persuaded that section 702 does in fact play an important role in the nation’s effort to prevent terrorist attacks across the globe.”^[9] The Washington Post has reported that 702 was in 2012 the single most prolific contributor to the President’s Daily Brief.^[10]

PRISM is the most effective way to combat terror domestic *and* abroad — prefer empirics

Mattise 13 — graduate of Syracuse University with a BA in Economics and Newspaper Journalism and a Master's in Magazine, Newspaper and Online Journalism

(Nathan Mattise, 6-16-2013, "PRISM helped stop terrorism in US and 20-plus countries, NSA document argues," <http://arstechnica.com/tech-policy/2013/06/prism-helped-stop-terrorism-in-us-and-20-plus-countries-nsa-document-argues/>, Date Accessed: 6-23-2015) //NM

US intelligence officials sent Congress a new declassified document on Saturday, which the Senate Intelligence Committee then made public. Outlets such as CNN and the Associated Press received the document and revealed a number of interesting statistics related to the government's use of the NSA's controversial PRISM program. However, this document has not yet been published on the Senate Intelligence Committee's website (and does not seem to be easily obtained through basic Internet search). The new document is part of an intelligence official's effort to "show Americans the value of the program," according to the AP. The report's primary supporting stat? Intelligence officials said that information gleaned from these NSA initiatives helped prevent terrorist plots in the US and more than 20 other countries. Additionally, the release stated that phone metadata was searched for less than 300 times within the secretive database last

year. The document also added details to the public's growing picture of the PRISM program. CNN reported that the NSA must delete these records after five years. The AP wrote that the NSA programs are reviewed every 90 days by a secret court authorized by the Foreign Intelligence Surveillance Act (FISA), and that the metadata records (which includes a call's time and length) can only be inspected for "suspected connections to terrorism." Despite all the public attention, the Obama Administration continues to insist that no privacy violations took place. According to White House Chief of Staff Denis McDonough (speaking Sunday on Face The Nation), the president plans to further clarify this "in the days ahead." On Friday, TechDirt also published a set of two documents described as "talking points about scooping up business records (i.e., all data on all phone calls) and on the Internet program known as PRISM." One of the talking points' main arguments is that Section 702 of the Foreign Intelligence Surveillance Act authorizes actions similar to those described above. This is despite the fact that no member of the public has ever been able to see the FISA court's ruling of the government's interpretation. Section 702 is a vital legal tool that Congress reauthorized in December 2012, as part of the FISA Amendments Act Reauthorization Act, after extensive hearings and debate. Under Section 702, the Foreign Intelligence Surveillance Court (FISA Court) certifies foreign intelligence collection. There is no secret program involved—it is strictly authorized by a US statute.

PRISM decimates Al Qaeda's ability to conduct mass attacks

Etzioni 15 [Amitai Etzioni, Director of the Institute for Communitarian Policy Studies at George Washington University, former President of the American Sociological Association, former Professor at Harvard Business School, former Senior Adviser to the White House, “

NSA: National Security vs. Individual Rights,” *Intelligence and National Security*, Volume 30, Issue 1, 2015, pages 100-136]

One telling piece of evidence regarding the effectiveness of the electronic surveillance programs is the way they hobbled bin Laden. He found out that he was unable to use any modern communication device to run his terror organizations that had branches in three continents.⁵⁴ He was reduced to using the same means of communication employed 5000 years ago – a messenger, a very slow, low-volume, cumbersome, and unreliable way of communication and command; in effect, preventing bin Laden from serving as an effective commander-in-chief of Al Qaeda. Moreover, once the CIA deduced that using a messenger was the only way left for him to communicate – tracking the messenger led to bin Laden's downfall.⁵⁵ Additional evidence publicly available that the NSA programs forced terrorists to limit their communications is gleaned from reports that following the revelation that the United States intercepted the communications of Ayman al-Zawahiri, there was a sharp decline in Al Qaeda's electronic communications.⁵⁶ In short, we have seen that there continues to be a serious threat of terrorism to national security; that terrorists cannot be handled like other criminals and to counter them distinct measures are best employed; and that surveillance programs like PRISM and the phone surveillance programs make a significant contribution to curbing terrorism. In short these programs do enhance one core element of the liberal communitarian balance. The next question the article addresses is the extent they undermine the other core element.

PRISM roadblocks terrorists – guts them of the tools necessary to pull off an attack

Arquilla 2013 (John [Professor and Chair Department of Defense Analysis @ Naval postgrad school]; In Defense of PRISM; Jun 7; foreignpolicy.com/2013/06/07/in-defense-of-prism/; kdf)

Prior to TIA, and well before 9/11, there were other ancestors of our current big data efforts. At the National Security Agency, and in other parts of the extensive American intelligence community, search systems known by such evocative names as "Echelon" and "Semantic Forests," among others, were in use, striving relentlessly to detect patterns of communication that might open up golden seams of information from the most secret caches of the world's various malefactors. Often enough, these and other tracking tools did distinguish the pattern from the noise, and national security was well served. And in the early days of the war against al Qaeda, the enemy was still using means of communication that American intelligence had the ability to monitor — including satellite phones and such — leading to several counterterror coups and high-level captures. But the network learned quickly and adjusted, becoming far more elusive, more dispersed, its cells increasingly

attuned to operating independently, its nodes and links ever less visible. It was against this shift that something like PRISM had to be mobilized to improve our ability to find the foe whose best, and only real defense against us is his capacity for concealment. Thus, the tantalizing prospect of PRISM, and of the whole "finding effort," is to deny the terrorists the virtual haven that they enjoy throughout the world's telecommunications spaces — indeed, throughout the whole of the "infosphere," which includes cyberspace. The piercing of this veil would mark a true turning point in the war on terror, for al Qaeda and other networks simply cannot function with any kind of cohesion, or at any sort of reasonable operational tempo if their communications become insecure. Cells and nodes would be ripped up, operatives killed or captured, and each loss would no doubt yield information that imperiled the network further. Even if al Qaeda resorted to the drastic measure of moving messages, training, and financial information by courier, operations would be so slowed as to cripple the organization. And even couriers can be flagged on "no fly" lists or caught boarding tramp steamers and such. So for all the furor caused by the PRISM revelations, my simple recommendation is to take a deep breath before crying out in protest. Think first about how the hider/finder dynamic in the war on terror has driven those responsible for our security to bring to bear the big guns of big data on the problem at hand. Think also about whether a willingness to allow some incursions into our privacy might lead to an improved ability to provide for our security, and where that equilibrium point between privacy and security might be. And last, think about the world as it might be without such a sustained effort to find the hidden — to detect, track, and disrupt the terrorists. That would be a world in which they stay on their feet and fighting, and in which they remain secure enough, for long enough, to acquire true weapons of mass destruction. Those of us in the national security business, who know that networks so armed will be far harder to deter than nations ever were, believe that big data approaches like PRISM and its forebears, have been and remain essential elements in the unrelenting and increasingly urgent effort to find the hidden.

Section 702 has empirically led the NSA to detecting and preventing terror attacks

- Section 702 — PRISM
- Metadata good
- Prevented 50 attacks

Hines 13 — Defense council member of the Truman National Security Project

(Written By, 6-19-2013, "Here's how metadata on billions of phone calls predicts terrorist attacks," <http://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/>, Date Accessed: 6-23-2015) //NM

Yesterday, when NSA Director General Keith Alexander testified before the House Committee on Intelligence, he declared that the NSA's surveillance programs have provided "critical leads to help prevent over 50 potential terrorist events." FBI Deputy Director Sean Boyce elaborated by describing four instances when the NSA's surveillance programs have had an impact: (1) when an intercepted email from a terrorist in Pakistan led to foiling a plan to bomb the New York subway system; (2) when NSA's programs helped prevent a plot to bomb the New York Stock Exchange; (3) when intelligence led to the arrest of a U.S. citizen who planned to bomb the Danish Newspaper office that published cartoon depictions of the Prophet Muhammad; and (4) when the NSA's programs triggered reopening the 9/11 investigation. So what are the practical applications of internet and phone records gathered from two NSA programs? And how can "metadata" actually prevent terrorist attacks? Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted. Section 215 of the Patriot Act provides the legal authority to obtain "business records" from phone companies. Meanwhile, the NSA uses

Section 702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According to the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases. One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists' planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat. Even more useful than hindsight is a crystal ball that gives the intelligence community a look into the future. Simply knowing how many individuals are in a chat room, how many individuals have contacted a particular phone user, or how many individuals are on an email chain could serve as an indicator of how many terrorists are involved in a plot. Furthermore, knowing when a suspect communicates can help identify his patterns of behavior. For instance, metadata can help establish whether a suspect communicates sporadically or on a set pattern (e.g., making a call every Saturday at 2 p.m.). Any deviation from that pattern could indicate that the plan changed at a certain point; any phone number or email address used consistently and then not at all could indicate that a suspect has stopped communicating with an associate. Additionally, a rapid increase in communication could indicate that an attack is about to happen. Metadata can provide all of this information without ever exposing the content of a phone call or email. If the metadata reveals the suspect is engaged in terrorist activities, then obtaining a warrant would allow intelligence officials to actually monitor the content of the suspect's communication. In Gen. Alexander's words, "These programs have protected our country and allies . . . [t]hese programs have been approved by the administration, Congress, and the courts." Now, Americans will have to decide whether they agree.

Prism necessary to get to emails to counter threats

Michael Hayden, former director of the NSA and the CIA, May 5, 2014, "Michael Hayden's Unwitting Case Against Secret Surveillance,"
<http://www.theatlantic.com/politics/archive/2014/05/michael-haydens-unwitting-case-against-secret-surveillance/361689/> DOA: 2-19-15

Actually, you need to go back and look at the whole movie. You need to see what went on before. Because if you know what went on before you may have a different interpretation of what you think the butler is guilty of. There are three or four things that happen that NSA and all these organizations have tried to solve. Enormous volume. How do you conduct signals intelligence to keep you safe in a tsunami of global communications? Well, the answer to that is bulk collection of metadata. Another issue that's out there prominently is NSA is mucking about in those global telecommunication grids that have your emails. No one complained when NSA was doing Soviet strategic microwave rocket signals. Well, the equivalent of those Soviet microwave signals are proliferator, terrorist, narco-trafficker, money-launderer emails, coexisting with yours and mine, out there in Gmail. And if you want NSA to continue to do what it was doing, or CSEC to continue to do what it's doing, what it had been doing to keep you safe, it's got to be in the stream where your data is. There's a couple other things too. After 9/11, the enemy was inside my country. That's the 215 program, metadata. Who might be affiliated with terrorists inside the United States? And finally, when the enemy wasn't in my country his communications were. It's an accident of history, but it's a fact, most emails reside on servers in the United States. They should not deserve constitutional protection if the email's from a bad man in Pakistan

communicating to a bad man in Yemen. And the Prism program is what allowed us to get those emails to keep everyone safe. There's a lot more to talk about but you're going to start clapping in about nine seconds. So I'm going to go back to the podium.

PRISM has contributed to actionable intelligence in the fight against terrorism

Stuart Taylor, April 29, 2014, The Big Snoop: Life, Liberty, and the Pursuit of Terrorists, <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.)

The **PRISM** program poses an even trickier version of the cost/benefit question: it is easier to justify its efficacy, but because it goes after the contents of messages, not just their origin and destination, it is more intrusive on the liberties of the people whose communications it scoops up. Moreover, while PRISM is more restrictive in its formal mandate (i.e., it is targeted only at foreign bad actors), in practice it does pry “incidentally” into the Internet traffic of many law-abiding U.S. citizens.

Yet there's no denying that PRISM's mining of emails and other Internet messages has produced a mother lode of useful information. An internal NSA document leaked by Snowden described the program as “the most prolific contributor to the President's Daily Brief” and the NSA's “leading source of raw material, accounting for nearly one in seven [of all the intelligence community's secret] reports.” More to the point, PRISM has often contributed to the collection of actionable intelligence used in the fight against terrorism. Even Wyden, the NSA's strongest congressional critic, acknowledges as much. He and his ally on the surveillance issue, Senator Mark Udall (D-Colo.), said in a joint statement last summer that “multiple terrorist plots have been disrupted at least in part because of information obtained under Section 702.”

PRISM important method of data collection – easy to find potential threats

Thompson, Ph.D., '13 (Loren B. [prof at Harvard and Georgetown University]; “Why NSA's PRISM Program Makes Sense”, Forbes, <http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/>)

President Obama's firm defense of the National Security Agency's “domestic” surveillance program on Friday should calm some of the more extravagant fears provoked by public disclosure of its existence. I put the word “domestic” in quotes because the effort to monitor Internet and other communications traffic isn't really about listening in on Americans, or even foreign nationals living here, but rather intercepting suspicious transmissions originating overseas that just happen to be passing through the United States. That is an eminently sensible way of keeping up with terrorists, because it is so much easier than tapping into network conduits in other countries or under the seas (not that we don't do that). In order to grasp the logic of the NSA program, which is code-named PRISM, you have to understand how the Internet evolved. It was a purely American innovation at its inception, with most of the infrastructure concentrated in a few places like Northern Virginia. I live a few miles from where the Internet's first big East Coast access point was located in the parking garage of an office building near

the intersection of Virginia's Routes 7 and 123, an area that some people refer to as Internet Alley. Because the Worldwide Web grew so haphazardly in its early days, it was common until recently for Internet traffic between two European countries to pass through my neighborhood. There were only a few major nodes in the system, and packet-switching sends messages through whatever pathway is available. The Washington Post story on PRISM today has a graphic illustrating my point about how bandwidth tends to be allocated globally. Like a modern version of ancient Rome's Appian Way, all digital roads lead to America. It isn't hard to see why Director of National Intelligence James R. Clapper could say on Thursday that "information collected under this program is among the most important and valuable foreign intelligence information we collect." No kidding: PRISM generated an average of four items per day for the President's daily intelligence briefing in 2012.

Reducing surveillance would make us blind to terrorists; keeping the efficiency of the program is necessary

Yoo '13, law professor ("Ending NSA Surveillance Is Not the Answer", 8-16-2013, National Review Online, <http://www.nationalreview.com/corner/356027/ending-nsa-surveillance-not-answer-john-yoo>)

We should be careful not to put the NSA in an impossible position. Of course, we should be vigilant against the administrative state in all of its tangled tendrils, especially its collection of taxes (the IRS scandal) and enforcement of the laws (Obama's refusal to enforce Obamacare and immigration law). The problem here, however, is that we are placing these kinds of domestic law-enforcement standards on a foreign intelligence function. With domestic law enforcement, we want the Justice Department to monitor one identified target (identified because other evidence gives probable cause that he or she has already committed a crime) and to carefully minimize any surveillance so as not to intrude on privacy interests. Once we impose those standards on the military and intelligence agencies, however, we are either guaranteeing failure or we must accept a certain level of error. If the military and intelligence agencies had to follow law-enforcement standards, their mission would fail because they would not give us any improvement over what the FBI could achieve anyway. If the intelligence community is to detect future terrorist attacks through analyzing electronic communications, we are asking them to search through a vast sea of e-mails and phone-call patterns to find those few which, on the surface, look innocent but are actually covert terrorist messages. If we give them broader authority, we would have to accept a level of error that is inherent in any human activity. No intelligence agency could perform its mission of protecting the nation's security without making a few of these kinds of mistakes. The question is whether there are too many, not whether there will be any at all. Domestic law enforcement makes these errors too. Police seek warrants for the wrong guy, execute a search in the wrong house, arrest the wrong suspect, and even shoot unarmed suspects. We accept these mistakes because we understand that no law-enforcement system can successfully protect our communities from crime with perfection. The question is the error rate, how much it would cost to reduce it, the impact on the effectiveness of the program, and the remedies we have for mistakes. Consider those questions in the context of the NSA surveillance program. The more important question is not the top of the fraction but the bottom — not just how many mistakes occurred, but how many records were searched overall. If there were 2,000 or so mistakes, as the Washington Post suggests, but involving billions of communications, the error rate is well less than 1 percent. Without looking at the latest figures, I suspect that is a far lower error rate than those turned in by domestic police on searches and arrests. To end the NSA's efforts to intercept terrorist communications would be to willfully blind ourselves to the most valuable intelligence sources on al-Qaeda (now that the president won't allow the capture and interrogation of al-Qaeda leaders). The more useful question is whether there is a cost-effective way to reduce the error rate without detracting from the effectiveness of the program, which, by General Keith Alexander's accounting, has been high.

PRISM is necessary and effective – newer electronic communication requires a wider net for surveillance, different from before.

Kempa '13 (Darcy Kempa, political writer and ex-Marine Corps, "NSA PRISM Program: Big Brother is Watching, and That's a Good Thing", 7-2-2013, <http://mic.com/articles/52379/nsa-prism-program-big-brother-is-watching-and-that-s-a-good-thing>)

Publicized information on the U.S. government's PRISM program has created a new debate on security. The debate is broadly one between national security and individual security, specifically a right to privacy. While Americans want terrorist acts prevented, they also want the government not to collect information on them. The biggest question is, if programs like PRISM work then why stop them? Early in 2013, a Gallup poll revealed that the majority of respondents (67%) felt satisfied with the nation's security from terrorism. That number increased from 53% noted in 2007, the year that PRISM started. A recent Gallup poll shows that a majority of Americans disapprove of government surveillance programs. This poll was taken after reports of the PRISM program were published. Former President George W. Bush defended PRISM and stated that "civil liberties were guaranteed" in the program. President Obama also defended the program as necessary to combat terrorism. National Security Agency Director Keith Alexander stated that PRISM prevented 11 terrorist attacks in the U.S. and over 50 "potential terrorist events" abroad. While these statements support the idea that the surveillance program is legal and effective, most Americans still reject them. Why? One reason is that Americans do not understand how the internet and cellular phones have changed the nature of surveillance activities. The old protocols of following people, tapping into phone lines, and taking pictures have changed. Today, terrorists can communicate instantaneously through email or cellular phones. The accounts can be created, changed, or closed just as quickly as the information is transmitted. Governments need to modify their methods since the criminals and terrorists have changed theirs. Another reason is that Americans prefer to be "people-savvy" and not "tech-savvy." The idea that America can negotiate with terrorists by finding common ground doesn't make sense. Terrorists, and criminals for that matter, don't care about building rapport. Instead, they care about winning whether that is destroying an ideology or emptying a bank account. Maybe the Transportation Security Administration can create a "terrorists only" line at airports to help identify people who should be monitored. Until that happens or works, technological surveillance can help protect this nation. A third reason may be that Americans do not trust their government. Almost 50% of Americans disapprove of President Obama's performance. The disapproval rate for Congress is even worse at 78% of those polled. Americans may be fed up with Obama and his "trust me" rhetoric, or may be tired of a dysfunctional Congress. While testimony about PRISM may be factual, Americans may not believe nor care that it works. The final analysis is that most Americans are more worried about their privacy than national security. Those concerns are not as important as protecting the nation from terrorism. If "Big Brother" is watching then it is a good thing. Preventing terrorism in the U.S. is more important than wondering if anyone cares about your internet or cellular phone activities.

The NSA needs current surveillance capabilities to fight terrorism, not further restrictions

Thiessen et al. '13 (Bill Harlow, an author specializing in the legality of the NSA; Diana West, author of "New America"; Marc Thiessen, an associate at the American Enterprise Institute; DR. EMANUELE OTTOLENGHI, member of the Foundation for Defense of Democracies, "Experts Explain Why the NSA Program Is Necessary", 6-13-2013, Center for Security Policy, <http://www.centerforsecuritypolicy.org/2013/06/13/arguing-for-the-nsa/>)

Thiessen also stressed how vital the PRISM program and the phone-data collection programs are to national security. "I think we should be celebrating the fact that the NSA is doing this...The fact is we are still facing a terrorist enemy who is trying to attack us. They don't have armies, navies, and air

forces that we can track with satellites. They send 19 men with box cutters to hijack planes and fly them into buildings. So there are only three ways we can find out what their plans are, and in each case they have to tell us. The first case is interrogation. Getting them to tell us their plans. Thanks to Barack Obama we don't do that any more. Second way to do it is penetration—which is incredibly hard to do—by infiltrating Al Qaeda, either just recruiting double agents or getting someone placed in there....When we have done it we've been fooled....So that leaves signaled intelligence. The only way that we have to find out what the terrorists are planning and disrupt their plans is to listen to their communications, monitor their e-mails, monitor them electronically. So if we get rid of this program, if this were to disappear, we would be flying blind. On the initial outcry over the programs made public by the leaks, Harlow says that "Just six weeks ago when the Boston bombings happened many people were saying 'Why were we let down by the intelligence community? Why didn't they collect the information that would allow us to stop incidences like that?" And now just six weeks later we have people crying 'Why are you trying to connect so many dots? Why are you trying to get information?' I think people can be genuinely concerned about the potential invasion of privacy, but you have to also understand that the only way to collect much of this potential information about threats from overseas is to have access to information which may pass through US servers."

ONLY PRISM bulk collection can provide access to necessary communications – empirics

Schmitt, Sanger, and Savage, B.A. in Political Sciences, Pulitzer Winning NYT globalization specialist, Master's from Yale Law School, 2013 (Eric, David, Charlie, "Administration Says Mining of Data Is Crucial to Fight Terror" New York Times, http://www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?_r=0)

To defenders of the N.S.A., the Zazi case underscores how the agency's Internet surveillance system, called Prism, which was set up over the past decade to collect data from online providers of e-mail and chat services, has yielded concrete results. "We were able to glean critical information," said a senior intelligence official, who spoke on the condition of anonymity. "It was through an e-mail correspondence that we had access to only through Prism." John Miller, a former senior intelligence official who now works for CBS News, said on "CBS This Morning," "That's how a program like this is supposed to work." Veterans of the Obama intelligence agencies say the large collections of digital data are vital in the search for terrorists. "If you're looking for a needle in the haystack, you need a haystack." Jeremy Bash, chief of staff to Leon E. Panetta, the former C.I.A. director and defense secretary, said on MSNBC on Friday. Under the program, intelligence officials must present Internet companies with specific requests for information on a case-by-case basis, showing that the target is a foreigner and located outside the United States, a senior law enforcement official said Friday. If the N.S.A. comes across information about an American citizen during the search, it turns over that material to the F.B.I. for an assessment, the official said. An administration official said Friday that agencies were evaluating whether they could publicly identify particular terrorism cases that came to the government's attention through the telephone or Internet programs. Representative Mike Rogers, the Michigan Republican who is chairman of the House intelligence committee, said Thursday that the phone program "was used to stop a terrorist attack." He did not identify the plot, or explain whether the call logs in the case would have been unavailable by ordinary subpoenas. Two Democratic senators on the Intelligence Committee who have been warning about the bulk collection of records under the Patriot Act, Ron Wyden of Oregon and Mark Udall of Colorado, said Friday that their study of the calling log program has convinced them that it was not worth its cost to privacy. "As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans," they said. In contrast to the call log program, there appears to be greater public evidence that programs like Prism have led to specific useful information. The Prism program relies on a 2008 law, the FISA Amendments Act, that allows surveillance without individualized warrants if it is targeted at foreigners abroad, even if it takes place on domestic soil. Last December, when Congress was preparing to vote on extending the law, Senator Dianne Feinstein, Democrat of California, who is chairwoman of the Senate Intelligence Committee, linked the law to eight recent terrorism-related cases, saying, "these cases show the program has worked." The cases included plots to bomb the New York Federal Reserve Bank,

the United States Capitol, locations in Tampa, Fla., and New York City and troops returning from combat overseas. She also listed a plot to assassinate the Saudi ambassador in the United States; plans by three men to travel to Afghanistan “to attend terrorist training and commit violent jihad”; and a conspiracy to provide support to a terrorist group in Uzbekistan called the Islamic Jihad Union. While most of those accused in those cases pleaded guilty — and therefore much of the evidence against them was not publicly disclosed — a case involving two Pakistani-American brothers in Florida accused of planning to set off a bomb in New York is still active, as is one involving a Chicago-area teenager accused of planning to bomb a bar.

PRISM has successfully curbed global terrorist threats because of intensive surveillance and extraordinary oversight.

Gernstein '13, a specialist in national security (Josh Gernstein, White House reporter, specialist in national legal and security issues, "NSA: PRISM stopped NYSE attack", 6-18-2013, POLITICO, <http://www.politico.com/story/2013/06/nsa-leak-keith-alexander-92971.html>)

Recently leaked communication surveillance programs have helped thwart more than 50 “potential terrorist events” around the world since the Sept. 11 attacks, National Security Agency Director Keith Alexander said Tuesday. Alexander said at least 10 of the attacks were set to take place in the United States, suggesting that most of the terrorism disrupted by the program had been set to occur abroad. The NSA also disclosed that counterterrorism officials targeted fewer than 300 phone numbers or other “identifiers” last year in the massive call-tracking database secretly assembled by the U.S. government. Alexander said the programs were subject to “extraordinary oversight.” “This isn’t some rogue operation that a group of guys up at NSA are running,” the spy agency’s chief added. The data on use of the call-tracking data came in a fact sheet released to reporters in connection with a public House Intelligence Committee hearing exploring the recently leaked telephone data mining program and another surveillance effort focused on Web traffic generated by foreigners. Alexander said 90 percent of the potential terrorist incidents were disrupted by the Web traffic program known as PRISM. He was less clear about how many incidents the call-tracking effort had helped to avert. Deputy FBI Director Sean Joyce said the Web traffic program had contributed to arrests averting a plot to bomb the New York Stock Exchange that resulted in criminal charges in 2008. Joyce also indicated that the PRISM program was essential to disrupting a plot to bomb the New York City subways in 2009. “Without the [Section] 702 tool, we would not have identified Najibullah Zazi,” Joyce said. However, President Barack Obama acknowledged in an interview aired Monday that it is impossible to know whether the subway plot might have been foiled by other methods. ”

PRISM has shut down multiple terrorist plots

Ackerman, National Security writer for Guardian U.S., 6/19/13 (Spencer, (2012 National Magazine Award for Digital Awarding) “NSA chief claims “focused” surveillance disrupted more than 50 terror plots”, The Guardian, <http://www.theguardian.com/world/2013/jun/18/nsa-surveillance-limited-focused-hearing>)

Some of the most senior intelligence and law enforcement officials in the United States strongly defended the National Security Agency's broad surveillance efforts on Tuesday, saying they had disrupted more than 50 terrorist plots around the world. General Keith Alexander, the director of the NSA, told a rare public hearing of the House intelligence committee in Washington that the programs were "critical" to the ability of the intelligence community to protect the US. Offering the most extensive defence yet on the efficacy of secret surveillance programs reported by the Guardian and the Washington Post, Alexander said they were “limited, focused and subject to rigorous oversight”. During the hearing, members of Congress criticised the source of the leaks, Edward Snowden, who remains free in Hong Kong. On Tuesday, Iceland said it had received an informal approach from an intermediary claiming that Snowden, a 29-year-old former NSA contractor, wanted to seek asylum there. Asked at the congressional hearing about what was next for Snowden, Alexander said: “justice”. Flanked by senior officials from the FBI, Justice Department and

the Office of the Director of National Intelligence, Alexander said that two surveillance programs revealed by the Guardian and the Washington Post had "helped prevent more than 50" terrorist attacks in over 20 countries. Most of those prevention efforts, Alexander said, came from the NSA's monitoring of foreigners' internet communications under a program known as Prism. He conceded that only 10 related to domestic terror plots. The Obama administration officials gave more details about four cases in which information taken from the NSA's databases of foreign internet communications and millions of Americans' phone records had contributed to stopping attacks. Two of them have been previously disclosed, especially that of the 2009 arrest of would-be New York subway bomber Najibullah Zazi. That case has been sharply challenged thanks to court records as more attributable to traditional police surveillance. Referring to the statutory authority for Prism, known as Section 702 of the 2008 Fisa Amendments Act, FBI deputy director Sean Joyce said: "Without the 702 tool, we would not have identified Najibullah Zazi." Joyce identified two previously unknown cases that he said the surveillance efforts helped unravel. In one, a Kansas City, Missouri, man named Khalid Ouazzani was found communicating with a "known extremist" in Yemen, information that helped detect what Joyce called "nascent plotting" to bomb the New York Stock Exchange. The other, described more vaguely, allowed the US government, using the NSA's phone-records database of Americans, to revisit a case closed shortly after 9/11 for lack of evidence. Ouazzani, however, was never convicted of plotting to bomb the stock exchange. Andrew Ames, a Justice Department spokesman, later clarified that he was convicted of "sending funds" to al-Qaida. The other case, Joyce said, involved an American who provided "financial support" to extremists in Somalia.

PRISM has prevented multiple terrorist attacks

Mattise, Staff Editor at Ars Technica, 6/16/13 (Nathan, (B.A. in Economics and Newspaper Journalism and a Master's in Magazine, Newspaper and Online Journalism), "Prism helped stop terrorism in US and 20-plus countries, NSA document argues". Ars Technica, <http://arstechnica.com/tech-policy/2013/06/prism-helped-stop-terrorism-in-us-and-20-plus-countries-nsa-document-argues/>)

[Intelligence officials said that information gleaned from these NSA initiatives helped prevent terrorist plots in the US and more than 20 other countries. Additionally, the release stated that phone metadata was searched for less than 300 times within the secretive database last year. The document also added details to the public's growing picture of the PRISM program. CNN reported that the NSA must delete these records after five years. The AP wrote that the NSA programs are reviewed every 90 days by a secret court authorized by the Foreign Intelligence Surveillance Act (FISA), and that the metadata records (which includes a call's time and length) can only be inspected for "suspected connections to terrorism." Despite all the public attention, the Obama Administration continues to insist that no privacy violations took place. According to White House Chief of Staff Denis McDonough (speaking Sunday on Face The Nation), the president plans to further clarify this "in the days ahead." On Friday, TechDirt also published a set of two documents described as "talking points about scooping up business records (i.e., all data on all phone calls) and on the Internet program known as PRISM." One of the talking points' main arguments is that Section 702 of the Foreign Intelligence Surveillance Act authorizes actions similar to those described above. This is despite the fact that no member of the public has ever been able to see the FISA court's ruling of the government's interpretation.]

NSA bulk data collection stopped a number of potentially deadly attacks.

Simeone, American Forces Press Service, 2013 (Nick, "NSA Chief: Surveillance Stopped More Than 50 Terror Plots", U.S. Department of Defense News, <http://www.defense.gov/news/newsarticle.aspx?id=120318>)

WASHINGTON, June 18, 2013 – The director of the National Security Agency told Congress today more than 50 terrorist plots worldwide have been prevented since the 9/11 attacks through the classified surveillance programs the government uses to gather phone and Internet data, programs he said are legal and do not compromise the privacy and civil liberties of Americans. Army Gen. Keith B. Alexander, who also commands U.S. Cyber Command,

told the House Intelligence Committee he plans as early as tomorrow to provide lawmakers with classified details about the plots that were foiled in an effort to show how valuable the programs are to national security. Alexander and other senior U.S. officials were called to testify in response to unauthorized disclosures to the media by former NSA contractor Edward Snowden, who revealed details about the agency's gathering of telephone numbers and the monitoring of Internet activity by foreigners overseas, leaks that Alexander said have caused irreversible and significant damage to the security of the United States and its allies. Testifying alongside Alexander, Deputy FBI Director Sean Joyce discussed two terrorist plots that he said the surveillance programs helped to prevent. In one, emails intercepted from a terrorist in Pakistan helped to stop a plot to bomb New York City's subway system. Another involved a failed attempt by a known extremist in Yemen who conspired with a suspect in the United States to target the New York Stock Exchange. Both cases led to arrests and convictions, Joyce said. "These programs are immensely valuable for protecting our nation and the security of our allies," Alexander said, and added that they may have helped to prevent the 9/11 attacks themselves if the government had the legal authority, as granted by the Patriot Act, to use them at the time. The disclosure of the NSA programs has generated a nationwide debate over what techniques the government can legally use to monitor phone and Internet data to prevent terrorism without violating the privacy and civil liberties of Americans. Alexander and other senior U.S. officials emphasized that the gathering of phone numbers that already are being collected by service providers as well as the tracking of U.S.-based Internet servers used by foreigners are legal and repeatedly have been approved by the courts and Congress. "These programs are limited, focused and subject to rigorous oversight," and their disciplined operation "protects the privacy and civil liberties of the American people," Alexander said.

The PRISM program is necessary to prevent terrorist attacks globally – empirics prove

Kelly, reporter for CNN, 8/1/13 – (Heather, CNN, August 1, 2013, "NSA chief: Snooping is crucial to fighting terrorism" <http://www.cnn.com/2013/07/31/tech/web/nsa-alexander-black-hat/>, accessed 7/15/15 JH @ DDI)

The National Security Agency's controversial intelligence-gathering programs have prevented 54 terrorist attacks around the world, including 13 in the United States, according to Gen. Keith Alexander, NSA director. Speaking before a capacity crowd of hackers and security experts Wednesday at the Black Hat computer-security conference, Alexander defended the NSA's embattled programs, which collect phone metadata and online communications in an effort to root out potential terrorists. The secret programs have come under fire since their existence was revealed in June by former CIA contractor Edward Snowden, who leaked details about them to several newspapers. "I promise you the truth -- what we know, what we're doing, and what I cannot tell you because we don't want to jeopardize our future defense," Alexander told the audience, which included a few hecklers who shouted profanities and accused him of lying. He then gave a partial recap, using PowerPoint slides, of how the two intelligence programs work. Alexander said the NSA can collect metadata on phone calls in the United States, including the date and time of the call, the numbers involved and the length of the conversations. He made a special point of saying the NSA does not have access to the content of citizens' calls or text messages. Alexander said the NSA's PRISM surveillance program, which probes digital activity such as e-mail, instant messaging and Web searches, focuses on foreign actors and does not apply to people in the United States. He said the phone and Internet data is necessary to "connect the dots" and identify potential terrorists before they act. Alexander attempted to reassure the audience that NSA officials are not abusing access to the databases to intrude on Americans' privacy. "The assumption is that people are out there just wheeling and dealing (users' information), and nothing could be further from the truth," he said. "We have tremendous oversight and compliance in these programs." Congress and courts make sure the programs operate within the bounds of the Foreign Intelligence Surveillance Act, and internal auditing systems are in place to prevent any abuse by employees, Alexander said. He added that only 35 analysts are authorized to run queries on the phone metadata.

Data gathered by PRISM is some of the most useful foreign intelligence gathered and is essential to prevent terror attacks

Thompson, contributor to Forbes on National Security and Business, 6/7/13 – (Loren, Forbes, June 7, 2013, "Why NSA's PRISM Program Makes Sense" <http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/>, accessed 7/15/15)

President Obama's firm defense of the National Security Agency's "domestic" surveillance program on Friday should calm some of the more extravagant fears provoked by public disclosure of its existence. I put the word "domestic" in quotes because the effort to monitor Internet and other communications traffic isn't really about listening in on Americans, or even foreign nationals living here, but rather intercepting suspicious transmissions originating overseas that just happen to be passing through the United States. That is an eminently sensible way of keeping up with terrorists, because it is so much easier than tapping into network conduits in other countries or under the seas (not that we don't do that). In order to grasp the logic of the NSA program, which is code-named PRISM, you have to understand how the Internet evolved. It was a purely American innovation at its inception, with most of the infrastructure concentrated in a few places like Northern Virginia. I live a few miles from where the Internet's first big East Coast access point was located in the parking garage of an office building near the intersection of Virginia's Routes 7 and 123, an area that some people refer to as Internet Alley. Because the Worldwide Web grew so haphazardly in its early days, it was common until recently for Internet traffic between two European countries to pass through my neighborhood. There were only a few major nodes in the system, and packet-switching sends messages through whatever pathway is available. The Washington Post story on PRISM today has a graphic illustrating my point about how bandwidth tends to be allocated globally. Like a modern version of ancient Rome's Appian Way, all digital roads lead to America. It isn't hard to see why Director of National Intelligence James R. Clapper could say on Thursday that "information collected under this program is among the most important and valuable foreign intelligence information we collect." No kidding: PRISM generated an average of four items per day for the President's daily intelligence briefing in 2012. The key point to recognize, though, is that this really is foreign intelligence. The architecture of the Internet enables NSA to collect it within U.S. borders, but there is no intention to spy on U.S. citizens. A few elementary algorithms used in narrowing the analysis of traffic should be sufficient to assure that the privacy of American citizens is seldom compromised. President Obama stressed in his comments today that safeguards have been put in place to prevent the scope of NSA surveillance from expanding beyond its original purpose.

Materiality requirement

A materiality requirement for a connection to a foreign power wrecks counter-terrorism investigations

Cordero, 13 – professor of law at Georgetown (Carrie, “Continued Oversight of U.S. Government Surveillance Authorities : Hearing Before the S. Committee on the Judiciary, 113th Cong., December 11, 2013 (Statement by Professor Carrie F. Cordero, Geo. U. L. Center)”
<http://scholarship.law.georgetown.edu/cong/118>

I would next like to highlight four components of S.1599. The first three would, in my view, significantly limit the effectiveness of the U.S. Government to conduct foreign intelligence activities to protect the nation from the national security threats of today, and, tomorrow. The fourth is a brief comment on competing proposals to add an adversarial component to the FISA process.

First, sections 101 and 201 would change the legal standards to obtain business records and implement pen register/trap and trace devices by requiring a connection to an agent of a foreign power. The sections also add a “materiality” requirement in addition to relevance. The likely intended effect of these provisions is to eliminate the utility of these provisions for large scale collection, such as the 215 telephony metadata program. But the proposed changes would likely have far more dramatic, and harmful, consequences to more traditional, day-to-day, national security investigations. The standards are currently aligned with investigative authorities in the criminal investigative context, such as subpoenas and pen register/trap and trace surveillance conducted under Title 18. Both of those criminal authorities operate on a relevance standard. By raising the standard to requiring a connection to an agent of a foreign power, these sections would render these investigative techniques nearly useless in the early stages of an investigation, which is precisely when they are most useful. Investigators may never get to determine whether a target rises to the agent of a foreign power standard, if they cannot conduct the less intrusive records request or pen register/trap and trace surveillance as part of an investigation. These changes, if made law, would return us to the days prior to September 11, 2001, when it was harder for an investigator to request records or conduct pen register/trap and trace surveillance in an international terrorism case than it was in an everyday drug or fraud case.

Third Party Doctrine: FISA

Third Party Doctrine justifies warrantless searches and is key to clarify legal application issues

Peikoff, philosophy prof. @ Texas , 14 (Amy L., St. John's Law Review, "Of Third-Party Bathwater: How to Throw out the Third-Party Doctrine While Preserving Government's Ability to Use Secret Agents," HeinOnline, p. 355-7)/ES

Without the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection. A criminal could plot and execute his entire crime from home knowing that the police could not send in undercover agents, record the fact of his phone calls, or watch any aspect of his Internet usage without first obtaining a warrant. He could use third parties to create a bubble of Fourth Amendment protection around the entirety of his criminal activity.³⁴

With no third-party doctrine, Kerr argues, it would be nearly impossible for the police to gain enough evidence to support a search warrant, particularly when a criminal is clever at substituting private, third-party-assisted actions and transactions for those that were once, of necessity, amenable to public viewing.³⁵ The doctrine, therefore, in Kerr's terms, avoids the "substitution effect" and thereby preserves the "technological neutrality" intended by the Court in Katz.³⁶ Just as the new technologies can bring 'intimate occurrences of the home' out in the open, so can technological change and the use of third parties take transactions that were out in the open and bring them inside.³⁷

If it is right to understand the Fourth Amendment from this perspective of technological neutrality, Kerr argues, then "it must be a two-way street."³⁸ So, just as the "reasonable expectation of privacy" test of Katz addresses the problem of technology exposing intimate details of one's life, the third-party doctrine addresses the problem of criminals substituting private, third-party transactions for actions conducted out in the open. Kerr notes that the doctrine thus provides another type of neutrality, in that a criminal enjoys "roughly the same degree of privacy protection regardless of whether [the] criminal commits crimes on his own or uses third parties."³⁹

Kerr's second argument in defense of the third-party doctrine is that it helps to ensure the clarity of Fourth Amendment rules.⁴⁰ The need for clarity, says Kerr, comes from the exclusionary rule's evidence-suppression remedy:

The severe costs of the exclusionary rule require ex ante clarity in the rules for when a reasonable expectation of privacy exists. The police need to know when their conduct triggers Fourth Amendment protection. Uncertainty can both overdeter police from acting when no protection exists and can lead them to inadvertently trample on Fourth Amendment rights.⁴¹

The third-party doctrine achieves the necessary clarity, says Kerr, by "guarantee [ing] that once information is present in a location it is treated just like everything else located there."⁴² So, for example:

[A] letter that arrives in the mail, is opened, and sits on the recipient's desk at home[It] is treated just like all the other papers on the desk [T]he Fourth Amendment rules [that the

police] must follow will be set by the usual rules of home searches rather than special rules for each piece of paper defined by the history of each page.⁴³

**Third Party Doctrine is used by FISC to justify it's activities
Ombres 15 (Devon, JD from Stetson, "NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform," Seton Hall Legislative Journal, HeinOnline, p. 33-4)//ES**

There is little doubt that the collection of content data, absent probable cause, violates the Fourth Amendment as an unreasonable search.^{2'} However, whether the mass collection of domestic metadata violates the Fourth Amendment is a question that is still being wrestled with due to the historical approval of the Third Party Doctrine ("TPD") arising from the seminal opinion of Smith v. Maryland²

In Smith, a PR was used to assist in a conviction of a burglary.³⁰ The Supreme Court held that using a PR did not constitute an unreasonable search because individuals are aware that phone companies maintain permanent records of dialed phone numbers, thereby abrogating any expectation of privacy." As Smith has not been overruled, it maintains its standing as a guiding principle under stare decisis and is being utilized, at least in part, as a basis for conducting domestic surveillance as discussed below.

The FISC cites directly to the Smith reasoning, in a heavily redacted opinion/order, in noting that there is no reasonable expectation of privacy in the collection of metadata.³² The FISC notes that Congress relaxed requirements to collect "non-content addressing information through [PR] and [TT] devices" through the PATRIOT Act and FISA Amendments and that "such information is not protected by the Fourth Amendment."³³ Like phone calls under Smith, the FISC held that email users, due to the same reasoning, also do not have an expectation of privacy. ³⁴ The FISC recognized the need for only a relevance standard, rather than reasonable suspicion, in approving the government's requests for widespread surveillance.

Third Party Doctrine: Undercover Informant

Thompson, Legislative Attorney, 14 (Richard M., written for the Congressional Research Service, June 5 2014, "The Fourth Amendment Third-Party Doctrine," p. 7-8)//ES

In a series of five cases throughout the 20th century, the Supreme Court assessed the constitutionality of the use of undercover agents or informants under the Fourth Amendment. In On Lee v. United States, the government wired an "undercover agent" with a microphone and sent him into On Lee's laundromat to engage him in incriminating conversation.⁴⁹ An agent of the Bureau of Narcotics sat outside with a receiving set to hear the conversation. In the course of these conversations, On Lee made incriminating statements, which the agent later testified to at On Lee's trial. On Lee argued that this evidence was obtained in violation of the Fourth Amendment. In an opinion authored by Justice Jackson, the Court disagreed, noting that On Lee was "talking confidentially and indiscreetly with one he trusted" and that the agent was let into his shop "with the consent, if not implied invitation" of On Lee.⁵⁰

In a similar case, Lopez v. United States, the defendant attempted to bribe an internal revenue agent, who during some of these conversations was wearing a recording device." At trial, Lopez moved to suppress evidence of the wire recordings as fruits of an unlawful search. Relying on the On Lee decision, the Court rejected this argument on the grounds that the defendant consented to the agent being in his office and "knew full well" that the statements he made to the agent could be used against him.⁵¹ Further, the Court noted that the listening device was not used to intercept conversations the agent could not have otherwise heard, but "instead, the device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose.,⁵²

In Lewis v. United States, the government sent an undercover federal narcotics agent to the defendant's home several times to purchase marijuana.⁵³ Over the defendant's objections, the agent was permitted to recount the conversations at trial. Upon review, the Supreme Court held that the conversations were not protected under the Fourth Amendment as the defendant had invited the federal agent into his home and that the statements were "willingly" made to the agent.⁵⁴

Finally, in Hoffa v. United States, a government informant relayed to federal law enforcement agents the many conversations he had with Jimmy Hoffa about Hoffa's attempt to tamper with a jury.⁵⁵ Because the informant did not enter Hoffa's hotel room by force, was invited to participate in the conversations by Hoffa, and was not a "surreptitious eavesdropper," the Court concluded that the Fourth Amendment had not been violated.

Katz didn't change the precedent, White said this is still permissible, but overturning the third party doctrine would cause a shift in justified action
Thompson, Legislative Attorney, 14 (Richard M., written for the Congressional Research Service, June 5 2014, "The Fourth Amendment Third-Party Doctrine," p. 9)//ES

Note that these cases came before Katz shifted the Fourth Amendment focus from property to privacy. Whether Katz would disturb this line of cases was a matter of "considerable speculation" 62 until the Court decided United States v. White four years later. In White, an undercover informant wearing a radio transmitter engaged the defendant in several incriminating conversations, four of which took place at the informant's house, and several other conversations took place in the defendant's home, a restaurant, and in the informant's car.⁶³ The court of appeals in White interpreted Katz as implicitly overruling this line of cases as it was based on a trespass doctrine that was "squarely discarded" in Katz.⁶⁴ The Supreme Court disagreed, however, and upheld the surreptitious surveillance. The opinion accepted that the trespass rationale could not survive after Katz, but that the undercover informant cases were also supported by a "second and independent ground"-that the informant was not an uninvited eavesdropper, but a party to the conversation who was free to report what he heard to the authorities.⁶⁵ For the Court, White had assumed the risk that information he shared with the informant could be shared with the police⁶⁶

Third Party Doctrine: Bank Records

Third Party doctrine justifies tracking of financial records – *Miller* decision proves

Thompson, Legislative Attorney, 14 (Richard M., written for the Congressional Research Service, June 5 2014, “The Fourth Amendment Third-Party Doctrine,” p. 9-10)//ES

In 1976, the Court took up its first major third-party doctrine case to deal with transactional documents in *Miller v. United States*. In that case, agents of the Treasury Department's Alcohol, Tobacco, and Firearms Bureau were investigating Mitch Miller for his participation in an illegal whiskey distillery.⁶⁹ The agents subpoenaed the presidents of several banks in which Miller had an account to produce all records of accounts including savings, checking accounts, and any loans he may have had. The banks never informed Miller that the subpoenas had been served, but ordered their employees to comply with the subpoenas. At one bank, an agent was shown microfilm of Miller's account and provided copies of "one deposit slip and one or two checks."⁷⁰ At the other bank, the agent was shown similar records and was given copies of "all checks, deposit slips, two financial statements, and three monthly statements.",⁷¹ Copies of the checks were later introduced into evidence at Miller's trial.

The lower court held that the government had unlawfully circumvented the Fourth Amendment by first requiring the banks to maintain the customer's records for a certain period of time and second by using insufficient legal process to obtain those records from the bank. In a 7-2 ruling, the Supreme Court reversed and held that subpoenaing the bank records without a warrant did not violate the Fourth Amendment. The opinion by Justice Powell discarded the first argument by noting that previous case law held that merely requiring the bank to retain its customers' records did not constitute a Fourth Amendment search.⁷² That previous case, however, did not resolve whether a subpoena was sufficient to access those documents.⁷³ Miller argued that the bank kept copies of personal records that he gave to the bank for a limited purpose and in which he retained a reasonable expectation of privacy under Katz. The Court, applying language from Katz, noted that "[w]hat a person knowingly exposes to the public ..is not a subject of Fourth Amendment protection.⁷⁴ The Court concluded that banking documents were not "confidential communications," but rather negotiable instruments that were required to transact business between the customer and the bank. All of the documents contained information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.,⁷⁵ As with the undercover agent cases, once documents were shared with the bank, they could then be given to the government without requiring a search warrant. Citing to White, Justice Powell instructed that a bank customer "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government.,⁷⁶ Looking to both this assumption of the risk theory and the secrecy model, the Court then included the following sentence which would come to encapsulate the third-party doctrine:

This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.⁷⁷

Third Party Doctrine: Telephone Calls

Wiretaps are justified by the third party doctrine – latest precedent Thompson, Legislative Attorney, 14 (Richard M., written for the Congressional Research Service, June 5 2014, “The Fourth Amendment Third-Party Doctrine,” p. 11-2)//ES

Several years later, the Court took up the second major third-party doctrine case, Smith v. Maryland,⁷ which would have major implications for government collection of transactional records, especially those held by third-party companies.

In Smith, the police were investigating the robbery of a young woman, who gave the police a description of her assailant and the vehicle seen near the scene of the crime.⁷⁹ The police later spotted a man matching the victim's description driving an identical vehicle in her neighborhood, which they traced back to Michael Smith. Upon police request, the telephone company installed a pen register at its central office to record the telephone numbers dialed from Smith's home. The device was installed without a warrant or court order. Through the pen register, the police learned that a call was placed from Smith's home to the victim's phone, which would eventually connect Smith to the robbery. At trial, Smith claimed that any evidence obtained from the pen register violated his Fourth Amendment rights as the police failed to obtain a warrant before installing it. This motion was denied, Smith was later convicted of robbery, and the appeals court affirmed his conviction, holding that the installation of the pen register was not a Fourth Amendment search.⁸⁰

In line with Justice Harlan's formulation of the Katz privacy test, the Supreme Court asked the following questions: first, whether Smith had a subjective expectation of privacy in the numbers he dialed, and second, whether that expectation was reasonable.⁸¹ As to the former, the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial."⁸² The Court assumed that people, in the main, know and understand that they must convey the dialed numbers to the company to complete the call; that the company has a process of recording those numbers; and that the company actually does record those numbers for various business reasons. It deduced this partially from the fact that phone books inform consumers that the telephone companies "can frequently help in identifying to authorities the origin of unwelcome and untroublesome calls" and that customers see a list of their calls recorded on their monthly phone bills.⁸³

Even if Smith did harbor a subjective expectation of privacy, the Court found that "this expectation is not 'one society is prepared to recognize as 'reasonable.'⁸⁴ Justice Blackmun cited to Miller, White, Hoffa, and Lopez for the proposition that "a person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties.⁸⁵ Because Smith "voluntarily conveyed" the telephone numbers to the company in the process of making the call, he had "exposed" that information to the company's equipment in the "ordinary course of business" and thus could not reasonably expect privacy in that information.⁶ Moreover, the Court found that Smith "assumed the risk" that the telephone company would reveal to the police the numbers he dialed.⁸⁷

Although Smith was the Court's last significant pronouncement on the parameters of the thirdparty doctrine, the lower federal courts have applied it in various contexts, with a significant number of these cases dealing with the transfer of electronic information.

Third Party Doctrine: Metadata

The Third Party Doctrine justifies metadata collection through the *Smith* decision

Yoo 14 (John, UC Berkeley law prof, Harvard Journal of Law and Public Policy, “The Legality of the National Security Agency’s Bulk Data Surveillance Programs,” HeinOnline, 37(3), p. 916)//ES

The NSA's first program, which collects metadata on domestic phone calls, poses the fewest constitutional difficulties. Under existing judicial doctrine, individuals have Fourth Amendment rights in the content of communications, but not in their addressing information.⁶¹ Privacy does not extend to the writing on the outside of envelopes deposited in the mail because the sender has voluntarily revealed the addresses to the post office for delivery.⁶² An identical principle applies to telecommunications. In *Smith v. Maryland*, the Supreme Court found calling information, such as the phone number dialed, beyond Fourth Amendment protection because the consumer had voluntarily turned over the information to a third party namely, the phone company-for connection and billing purposes.⁶³ Under the rubric of *Katz v. United States*, no one can have an expectation of privacy in records that they have handed over to someone else."

Administrative Search Doctrine: FISA

Administrative Search Doctrine key to justify FISA surveillance

Birkenstock 92 (Gregory E., "The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis," Georgetown Law Journal, 80(3), p. 858-60)

Based on the administrative search doctrine, the essential constitutional argument for accepting the diminished probable cause standards of FISA is that the primary purpose of the search is not to gather evidence for criminal prosecutions. 14 When the government has a special need for the information, the Fourth Amendment should allow the government more latitude in justifying its need to conduct a search. This is especially true for foreign intelligence, where the emphasis of the FISA search is on gathering information needed to defend against a threat to national security. The use of that information as criminal evidence is merely a legitimate byproduct of the search for foreign intelligence information, much as uncovering of evidence of criminal activity during an administrative search is allowable under Burger.

In Camara and See, the Court acknowledged that the Fourth Amendment does protect the individual's privacy even in the context of civil searches.¹¹⁵ According to the Camara Court, administrative searches are reasonable when the government's need for regulatory enforcement outweighs the limited intrusiveness of the noncriminal search.¹¹⁶ As in the "special governmental needs" cases discussed below,¹⁷ the Court attached great significance to the fact that administrative searches are not conducted primarily for penal law enforcement. While FISA searches may often be expected to discover incriminating evidence, FISA's main purpose of gathering information for protection of national security interests, "I rather than prosecuting criminals, supports the analogies suggested in this note.

As a preliminary matter, the focus on administrative searches' noncriminal purpose in Camara requires further clarification. That portion of the Camara opinion that relied on the "limited" invasion of privacy resulting from the administrative inspection¹⁹ is sufficiently ambiguous to obscure the Court's reasoning. The reference may be interpreted in at least two ways: (1) a lesser quantum of evidence is constitutionally required when the goal of the search is not furtherance of criminal prosecution; or (2) a lesser quantum of evidence is constitutionally required when the search is less intensive than that generally permitted in a criminal investigation. Although the Court has never resolved this debate, the former interpretation is a more logical one. In Abel v. United States,²⁰ a pre-Camarad decision, an administrative search was upheld because its purpose was not to search for evidence of crime, even though "a more exhaustive search is hardly to be found in the records of the Supreme Court."²¹ Thus, while FISA searches are necessarily more intrusive than administrative searches, the proposed analogy can still be instructive. Furthermore, while the applicability of Camara's other factors—the history of judicial and popular acceptance and the requirement that the search be the most effective means—are also problematic, the proposed analogy would still provide a superior model of judicial decisionmaking in the national security area than the present deferential approach.

Analyzing FISA searches under the administrative search doctrine can illuminate the potential utility of a similar national security jurisprudence. The usefulness of this approach is underscored by the fact that the Senate Judiciary Committee, in considering the wisdom of a lower standard of probable cause, referred to the administrative search doctrine in coming to its conclusion that the

FISA probable cause standard was constitutionally acceptable.'²² By using principles from an analogous area of the law, rather than creating a separate sphere of jurisprudence for foreign intelligence, progress can be made in assessing the wisdom of relaxing the probable cause standards for national security searches.

The administrative search doctrine is key to justify FISA activities

Birkenstock 92 (Gregory E., "The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis," **Georgetown Law Journal**, 80(3), p. 865-6)//ES

Although the analogy is not a perfect one, the tests developed in the administrative search context are instructive in exploring the legitimacy of FISA searches. For this analysis, the relevant test is that articulated in Camara: to weigh the interests served by the search against the intrusion into privacy that the search entails. 161

The government has a strong interest in gaining the information that FISA surveillance gathers. 162 It is an "elementary truth" that "unless the Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered."⁶³ FISA limits the "foreign intelligence information" that may be sought to information relevant to the nation's ability to protect against an act of war, international terrorism, or clandestine intelligence activities. 164 FISA searches may also seek information that relates to or is necessary to "the national defense or the security of the United States; or... the conduct of the foreign affairs of the United States."¹⁶⁵ While it is possible to overstate and thus manipulate these interests, they are nonetheless at the very core of the government's constitutional mandate to "provide for the common defense."¹⁶⁶

The intrusion authorized under a FISA search order is intensive, but in most cases not sufficiently intensive to outweigh the interest supporting the search. Generally, wiretapping is a highly intrusive investigatory technique. 167 But FISA includes several provisions designed to ensure that the intrusion will be no greater than is absolutely necessary. 168 FISA's web of definitions helps to ensure that the search will not be overly intrusive by limiting searches to the most important national security information.¹⁶⁹ When intelligence gathering and criminal investigation overlap, however, the courts must ensure that FISA searches are not abused. When this is accomplished, FISA searches represent a legitimate tool to promote national security. While certainly not perfect, the administrative search analogy helps to place FISA searches in their proper constitutional context.

The Supreme Court has taken the view that the evidentiary requirement of the Fourth Amendment is not a rigid standard that requires precisely the same quantum of evidence in all cases.¹⁷⁰ It is instead a flexible standard, permitting consideration of the public and individual interests as they are reflected in the facts of a particular case.⁷¹ This is an important and meaningful concept, which has proved useful in defining Fourth Amendment limits upon certain "special" enforcement procedures that are unlike the usual arrest and search. Viewed as a part of this framework, FISA surveillance is constitutionally permissible, and courts need not invoke the catch phrase "national security" to uphold such searches.

Administrative Search Doctrine necessary to avoid a warrant – allows quick and flexible responses

Birkenstock 92 (Gregory E., “The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis,” Georgetown Law Journal, 80(3), p. 868) //ES

The administrative search doctrine symbolizes the Supreme Court's turn away from the proscriptions of the Fourth Amendment's Warrant Clause toward a more flexible reasonableness analysis.¹⁸⁷ This note demonstrates that the doctrine serves as an appropriate jurisprudential model for FISA searches. In a variety of contexts, the Court has used a balancing approach to justify even full-scale searches without a warrant, probable cause, or even individualized suspicion, when the governmental need is especially acute. This Part of the note briefly examines the "special governmental needs" cases and further demonstrates how FISA surveillance can be assimilated into modern Fourth Amendment jurisprudence.

Administrative search doctrine allows investigations without warrants

Birkenstock 92 (Gregory E., “The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis,” Georgetown Law Journal, 80(3), p. 869) //ES

Thus, where the governmental interest is particularly acute, the Court shuns the specific commands of the Warrant Clause and uses a balancing test under a general reasonableness standard. Significantly, none of these searches involved attempts by the police to locate evidence of crime. In each, the Court referred to the government's special needs as those beyond the normal need for law enforcement.¹⁹⁷

In both the administrative search and special governmental needs cases, then, the Court has been persuaded that probable cause and individualized suspicion are not always Fourth Amendment requirements. In an expanding line of cases, the Court has held that certain governmental interests outweigh individual privacy interests. In each case, the Court has been careful to stress the difference between the search at issue and the traditional criminal search.

Administrative Search justifies FISA – Supreme Court precedent

Birkenstock 92 (Gregory E., “The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis,” Georgetown Law Journal, 80(3), p. 870) //ES

In sum, while some have questioned FISA's diminished probable cause standard over the years, an examination of Supreme Court precedent demonstrates that the standard is less problematic than it may first appear. While the courts have uniformly upheld FISA under Fourth Amendment challenges, they have been reluctant to assimilate FISA surveillance into Fourth Amendment doctrine. The administrative search and special governmental needs doctrines provide constitutional justification for the diminished probable cause standard in FISA. By analyzing FISA surveillance in this manner, courts can avoid the pitfall of assigning national security matters to a separate sphere of the law.

Administrative Search Doctrine: TSA

**Administrative search doctrine justifies to TSA security checks
Sanford 93 (Don L., Summer 1993, "Airport Security, Terrorism, and the
Fourth Amendment: A Look Back and a Step Forward," Journal of Air Law
and Commerce, 58(4), p. 1176-7)//ES**

A second approach taken to justify airport searches is the administrative search. The Supreme Court has addressed searches conducted for purposes other than criminal law enforcement that might invade areas protected by the Fourth Amendment. In 1967, the Supreme Court enunciated the administrative search doctrine in a pair of companion cases: Camara v. Municipal Court 329 and See v. City of Seattle.¹³⁰ In Camara, the Court reasoned that an administrative search was permissible under the Fourth Amendment "by balancing the need to search against the invasion which the search entails."¹³¹ In articulating the new administrative search doctrine, the Court redefined the traditional probable cause standard. Individualized suspicion was replaced with a more expansive concept of reasonableness, cast in the form of a balancing test.¹³² This reasonableness "must be as limited in its intrusiveness as is consistent with satisfaction of the administrative need that justifies it."¹³³ Administrative searches generally satisfy the Fourth Amendment's reasonableness requirements because the searches are not personal in nature, are not directed toward discovering evidence of a crime,¹³⁴ and thus involve a relatively limited invasion of privacy.¹³⁵

Airport security screenings have consistently been upheld as a consensual regulatory search to further an administratively directed program whose goal is to ensure air safety.¹³⁶ In the seminal case of United States v. Davis¹³⁷ the Ninth Circuit Court of Appeals approved warrantless airport security checks of all passengers and their carry-on luggage as administrative searches.¹³⁸ According to the court, administrative searches are constitutionally permissible without a warrant if the intrusion is consistent with satisfying the administrative need.¹³⁹ A warrantless administrative search is also legitimate when requiring a search warrant would frustrate the governmental purpose behind the search.¹⁴⁰

**Administrative Search Doctrine is used to justify TSA screenings – case law
Israelson 13 (Gregory R., Summer 2013, "Applying the Fourth Amendment's National-Security Exception to Airport Security and the TSA," Journal of Air Law and Commerce, 78(3), p. 512-3)//ES**

As courts turned away from the earlier frameworks, they began to apply the administrative-search exception. In recent years, the administrative-search framework has been the doctrine of choice for courts analyzing Fourth Amendment concerns related to airport security."

At the core of the administrative-search exception is a balancing of the government's legitimate interests and the individual's right to be free from government intrusion. Beyond this basic test, however, courts have differed in their application of the administrative-search exception to airport security cases.

Most circuits view airport security screening as an "administrative search,"¹⁴⁷ which allows for a balancing of "the individual's privacy expectations against the [g]overnment's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion

in the particular context."⁷⁵ In the context of "blanket suspicionless searches," the Supreme Court explained that a reasonable search must be "calibrated to the risk" and referred to airport security as it existed in 1997 as one example of such a search.⁷⁶ But the Court added the caveat that "where . . . public safety is not genuinely in jeopardy, the Fourth Amendment precludes the suspicionless search, no matter how conveniently arranged."⁷⁷ In sum, determining the constitutionality of a suspicionless checkpoint search requires balancing the "gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.'⁷⁸

Airport Security Links

Surveillance by TSA, Border and Customs agents key to security --- internal safe guards will protect civil rights

Horwitz, 14 --- covers the Justice Department and criminal justice issues nationwide for The Washington Post (12/8/2014, Sari, "Justice Dept. announces new rules to curb racial profiling by federal law enforcement," http://www.washingtonpost.com/world/national-security/justice-dept-to-announce-new-rules-to-curb-racial-profiling-by-federal-law-enforcement/2014/12/07/e00eca18-7e79-11e4-9f38-95a187e4c1f7_story.html)

A fact sheet on the policy said that some DHS activity is not covered by the policy because of the “unique nature of DHS’s mission.” “This does not mean that officers and agents are free to profile,” according to the DHS fact sheet. “To the contrary, DHS’s existing policies make it categorically clear that profiling is prohibited, while articulating limited circumstances where it is permissible to rely in part on these characteristics, because of the unique nature of border and transportation security as compared to traditional law enforcement.” President George W. Bush banned racial profiling in 2003, but the prohibition did not apply to national security investigations and covered only race — not religion, national origin, gender or sexual orientation and gender identity. Civil rights groups and Democratic lawmakers have pushed for expanded anti-profiling protections since President Obama was elected in 2008. Holder began the process to revamp the rules in 2009 and considers the new policy one of the signature accomplishments of his tenure. About six months ago, the Justice Department delivered the rules to the White House. But they applied only to the department, and White House officials wanted the policies to cover additional agencies. The rules have been delayed in part because DHS officials pushed the White House and the Justice Department to allow major exclusions for agencies such as the Transportation Security Administration, Immigration and Customs Enforcement, and Customs and Border Protection. In several high-level meetings, DHS Secretary Jeh Johnson argued that immigration and customs agents and airport screeners needed to consider a variety of factors to keep the nation safe, according to officials familiar with his personal efforts. TSA officials argued that the rules should not apply to them because the TSA is not a law enforcement agency. In its fact sheet, DHS officials said that they will review activities not directly covered by the guidance to ensure that “we are including every appropriate safeguard and civil rights protection in the execution of those important security activities, and to enhance our policies where necessary.”

TSA suffers hypocritical persecution-IS actually really good-SL

Reed 8/9/-12(Ted, Transportation Journalist for over 20 years, "Surprise Gallup Poll: People Think TSA Does A Good Job", Forbes,<http://www.forbes.com/sites/tedreed/2012/08/09/surprise-gallup-poll-people-think-tsa-does-a-good-job/>)

Surprisingly, despite all of the negative Internet commentary and Congressional complaining about the Transportation Security Administration, the majority of U.S. travelers have a positive opinion of the agency. Not only that, but people who fly, and who are exposed to TSA screening, have an even more positive opinion than people who rarely or never fly. According to a Gallup poll released Wednesday, 54% of Americans think the TSA is doing either an excellent or a good job of handling security screening at airports. Moreover, among Americans who have flown at least once in the past year, 57% have an excellent or good opinion of the agency. As far as TSA effectiveness at preventing acts of terrorism on U.S. airplanes, 41% think the screening procedures are extremely or very effective. Another 44% think the procedures are somewhat effective. That number varies little for people who fly somewhat regularly and people who rarely or never fly. The poll was conducted with telephone interviews July 9th through July 12. Gallup interviewed 1,014 adults living in all 50 states and the District of Columbia. Interestingly, younger Americans “have significantly more positive opinions of the TSA

than those who are older," Gallup said, noting that 67% of people between 18 and 29 rate the agency as excellent or good. This may be because young people fly more frequently, or it may be because that for young people TSA screening, first implemented in 2001, has been part of their flying experience for the majority of their lives. Criticism of the TSA seems to come primarily from two sources. One is Internet sites, where reporting standards are generally not at the same level as newspapers, where reporters are taught to consider what is told to them with skepticism and to seek responses to charges. On Wednesday, some sites were repeating charges by a man who said that his wife was admitted to the emergency room for treatment after TSA agents at Fort Lauderdale-Hollywood International Airport harassed her and subjected her to closed door screening after metal in her bra set off an alarm. The man said his wife was subject to a brutal rape three years ago and is still recovering from the psychological impact. Without denigrating the man or his wife in any way, it is possible to say that the **TSA is put into a difficult situation when such charges are posted with little or no fact checking by reporters.** As for Congress, the House Homeland Security Committee's Transportation Security Subcommittee recently convened a hearing on the topic: "Breach of Trust: Addressing Misconduct Among TSA Screeners." According to About.com, "It didn't take (committee chairman) Rep. Mike Rogers (R-Alabama) long to set the tone for the day, saying in his opening statement: "Stealing from checked luggage; accepting bribes from drug smugglers; sleeping or drinking while on duty — this kind of criminal behavior and negligence has contributed significantly to TSA's shattered public image." Now there is a poll to show that in fact, TSA does not have actually have a bad public image. And here, it is worth mentioning that **the public image of Congress is not so good, perhaps reflecting a tendency to be excessively critical of perceived enemies rather than to seek compromise and solve problems.**

Without NSA current Procedures we're susceptible to Terrorism-SL

Herridge 12/17/-14(Catherine Catherine Herridge is an award-winning Chief Intelligence correspondent for FOX News Channel, "TSA head: Threat from terrorism worse now but US better able to combat it", FNC, "<http://www.foxnews.com/politics/2014/12/17/tsa-head-threat-from-terrorism-worse-now-but-us-better-able-to-combat-it/>)

Khorasan contains long-time associates of Usama bin Laden, including Sanafi al-Nasr and Muhsin al-Fadhli, as well as a handful of operatives trained by the Yemeni bomb maker Ibrahim al-Asiri, who specializes in non-metallic bombs that traditional airport screening can miss. "Without going into details about what that may look like from a classified intelligence perspective, we do remain concerned that there is active plotting going on," Pistole said. And with new information that the French bomb maker David Drugeon likely survived a U.S. air strike last month, Pistole added, "there is concern that there are still individuals out there who have not only the ability to do that, but also the intent to use that on a flight to Europe or the US." The TSA administrator also described classified procedures that track foreign fighters, based on their travel history, before they check in at overseas airports for U.S.-bound flights. "There are individuals we are concerned about and we are again looking at if they make travel reservations, then they of course receive proper scrutiny," Pistole said. The continued threat from groups like Khorasan explains why procedures, implemented in July, requiring passengers to turn on their phone and computers at some airports, remain in place. As the holiday travel season begins, TSA officials say they are not expecting big changes at the checkpoints, but if there are changes, they will be driven by new and specific intelligence.

TSA Prevents Terrorist Attacks- SL

Reed 10/23/-12(Ted, Transportation Journalist for over 20 years, "Remember 9/11? TSA finally gets its gloves off", Forbes," <http://www.forbes.com/sites/tedreed/2012/10/23/remember-911-tsa-finally-takes-off-the-gloves-reminds-critics-of-reality/>"

The Transportation Security Administration has taken off the gloves and started to respond more aggressively to the constant barrage of criticism – as well it should. Last week, in an opinion piece in the Rockland County Times, published in a close-in New York City suburb, TSA spokeswoman Lisa Farbstein responded to a critical column by area resident Diane Dimond, a syndicated

columnist. "Perhaps the next time Diane and her family fly out of a New York-area airport to a fun vacation spot, they'll look out the car window at the New York skyline minus the Twin Towers and remember some of the true facts about TSA and why it exists," Farbstein wrote. Dimond "criticized the very security measures that were designed to keep passengers safe — to help ensure that there is not another 9/11 in her back yard," said Farbstein, who answered about a dozen criticisms, point-by-point. Among them: it is inconvenient, undignified and an invasion of your privacy to be forced to remove your shoes, jackets and belts, take off your belt and take your computer from its case. TSA agents "treat all of us like we're new arrivals at a prison camp." The lines are too long and some agents seem to stand around doing nothing. While the criticisms are familiar, the aggressive response is new. In fact, the TSA responds to multiple daily attacks, most far less coherent than Dimond's. Critics include travelers who make up stories; members of Congress who seek political gain and bloggers, tweeters and other self-promoters aware that the best way to be noticed and collect Internet hits is to express outrage. The outrage business, it must be said, is a growth business, thriving in the age of new media. Last week, radio talk show host Dana Loesch tweeted about an incident at the Phoenix airport. Loesch claimed she was sexually molested after a sensor showed traces of explosives on her. She was upset that the incident took place in private: she had requested a public screening. Earlier, in June, Loesch and her husband were detained by the TSA in Providence, R.I., after he allegedly underwent intrusive screenings because sensors detected traces of explosives on him. Perhaps we should conclude that TSA agents are engaged in a nationwide plot to harass the couple whenever possible. Or perhaps explosive pixie dust suddenly finds them whenever they head to the airport. Clearly, they are outliers among the 650 million people TSA screens annually. Last year, about one tenth of one percent of those filed complaints. The truth is that, for all of the complaints, most U.S. travelers have a positive opinion of the TSA. According to a Gallup poll released in August, 54% of Americans think TSA is doing either an excellent or a good job of handling airport screening. Among Americans who have flown at least once in the past year, 57% have an excellent or good opinion of the agency. In other words, the more you see them, the better you like them. Of course, TSA is not perfect. It employs 62,000 people, a few of whom have stolen from the luggage they are paid to inspect. The annual \$8.1 billion budget seems high: the same work was done for far less by private firms before Sept. 11. The firms followed federal guidelines, which sadly did not prevent box cutters on airplanes. The TSA is very visible to millions of travelers, some of whom have had a bad day by the time they get to the airport. And of course the agency is overseen by a dysfunctional Congress, whose 535 members bring a love of the limelight, vastly differing agendas and an inability to compromise. Probably the biggest problem is that, unfortunately, we really don't know how much screening is enough and how much is too much. Eleven years later, that is something we are still learning.

Recent revelations ensure TSA security is effective- high spending and increased surveillance

SCHOLTES 7/15— Transportation Reporter. (Jennifer, "TSA's response to criticism: Longer airport lines," Politico, 7/15/15, <http://www.politico.com/story/2015/07/longer-airport-lines-likely-as-tsa-tries-to-plug-security-holes-120117.html>). WM

The Transportation Security Administration has a new strategy for improving its woeful performance in catching airport security threats — and it will likely mean longer lines and more government bucks. A month after the TSA was embarrassed by its almost-total failure in a covert security audit, Homeland Security Secretary Jeh Johnson has ordered the agency to pursue an improvement plan that will require more hand-wanding of passengers, more use of bomb-sniffing dogs and more random testing of luggage and travelers for traces of explosives. It will also consider reducing travelers' chances of being sent through the expedited PreCheck lines at airports. Increased reliance on PreCheck is just one strategy TSA has used to become slimmer and swifter in the past few years, drawing buckets of praise from a Congress that's otherwise largely criticized the agency. It has also relied more on technology like body-scanners and analyses of specific travelers' risks while leaning less on labor-intensive methods like pat-downs, allowing the TSA to save manpower costs and shrink its workforce. But then came the leak of a still-classified inspector general report in June, which found that TSA agents had failed to find fake explosives and weapons 67 out of 70 times during covert testing — and that the screening technology often just doesn't work. The 96-percent failure rate drew sharp rebukes from Capitol Hill, led to the immediate ouster of then-acting Administrator Melvin Carraway and caused much shuttle diplomacy between lawmakers and the agency's top brass. Now the response threatens to gum up airport checkpoints. "In light of the 96 percent failure, they're probably going to slow things down," House Homeland Security Chairman Mike McCaul (R-Texas) acknowledged in an interview. He added that "the technology failure was a big part of the problem" and that the DHS inspector general pointed to the agency's policy of funneling travelers from regular security lines through the less-intensive PreCheck queues as one of the "big weaknesses." Kevin Mitchell, chairman of the Business Travel Coalition, agreed that air passengers will probably feel the impact of the latest changes. "Things are going to slow down, and consumers are going to

get increasingly frustrated." he said. Johnson said this month that he had ordered TSA to start doing more manual screening, such as using handheld metal detectors and doing more random tests for trace explosives, and to take a second look at the agency's policy of selectively diverting non-vetted travelers into the PreCheck lanes. "Some of those things he's talking about are going to slow the lines down," the House Homeland Security Committee's ranking Democrat, Rep. Bennie Thompson of Mississippi, told POLITICO. "So the question is: What's this going to do to throughput?" While Thompson says he supports adding more manual screening and being more selective about which travelers get expedited treatment, he's concerned about how this shift reflects on all the work the agency has done to move away from slower procedures. "If walking back allows us to identify more vulnerabilities, then that's good. But what does that say for all the tens of millions of dollars that we've spent on technology that was supposed to move us forward?" Thompson said. "It's clear that our technology that's being deployed — either because of the machines or the operators — failed us." Johnson also said this month that he has directed the TSA to rethink performance standards for the screening equipment implicated in the inspector general's report. He noted that the CEO of the company that manufactures the machines has said he will help make the technology more effective. Although Johnson didn't directly pin the blame on the scanning machines, McCaul and Rep. Kathleen Rice (D-N.Y.) say the IG's report noted that the body imaging technology has an unacceptable failure rate and that the manufacturer guarantees threat detection accuracy at well under 100 percent. Because the report is still classified, the agency hasn't disclosed exactly which types of equipment were involved or how they failed. But McCaul and Rice identified them as the millimeter-wave body scanners, made by L-3 Communications Corp., that force passengers to pose inside a booth with their arms raised. The machines are supposed to find both "metallic and nonmetallic" objects hidden under passengers' clothing, including guns and explosives, and "can detect a wide range of threats to transportation security in a matter of seconds," TSA boasts on its website. McCaul said his panel is looking into how much of the failure rate can be attributed to technology issues versus human error. He plans a hearing on the issue this month with testimony from new TSA Administrator Peter Neffenger, who assumed his post July 6 after being confirmed by the Senate. The current plan, McCaul said, is for DHS to update the imaging machines' software. "Jeh Johnson's a smart guy," the chairman said. "He and I talk a lot. And he knows that updating that software is probably going to reduce the failure rate." What's less clear is how the department is going to handle vulnerabilities in its PreCheck program, which allows travelers to pass through security checkpoints with their shoes and belts on, and without removing laptops and liquids from bags. The main problem, many lawmakers say, is TSA's "managed inclusion" policy of giving that special treatment to travelers who haven't gone through the program's vetting process. To enroll in PreCheck, passengers must provide fingerprints, undergo a background check and pay an \$85 fee. One purpose of steering non-enrolled passengers into the PreCheck lanes has been to give travelers a taste of what life could be like if they signed up for the expedited screening program, said David Inserra, a homeland security policy analyst at the Heritage Foundation. It also makes more efficient use of TSA's screeners when the speedier lines are drastically shorter than the regular queues. "You've got these people working these lines, and sometimes they're going to be doing nothing, or we can use them for something," Inserra said. "But that's not really a good security mindset. That's really an efficiency mindset." Patricia Rojas Ungár, vice president of government relations at the U.S. Travel Association, says the "managed inclusion" program "really has run its course." Now, she said, it's important for TSA "to double down in getting people enrolled in the actual program." The agency's standard security policies were born of credible threats and real terrorism plots, such as Richard Reid's attempt to detonate explosives packed in his shoes on a flight from Paris to Miami just three months after the Sept. 11, 2001, terrorist attacks. Lawmakers first started to challenge the "managed inclusion" policy after learning this spring that TSA screeners had allowed a known former domestic terrorist through a PreCheck line last year. And the issue has only gotten more attention since the IG's report was leaked. "The inspector general highlighted that one of the big weaknesses was managed inclusion," said McCaul, whose committee approved a bill last month that would bar the agency from allowing most non-vetted travelers into PreCheck lines. "Do we want to be kicking in people who may be a threat? I don't know. Obviously we're not going to target the grandmother and the baby. ... It has to be risk-based, but with security in mind, because the terrorists — unfortunately — they still want to blow up airplanes." In his 10-point plan for the TSA, Johnson has also directed the agency to reassess whether it should allow non-vetted travelers into PreCheck. But Thompson, who wrote the bill that would prohibit the policy, says there's no doubt the practice is weakening security and should already be changed. "If you know a system you have deployed creates a vulnerability, you fix it," Thompson said. "If throughput is one of the objectives, it should not be the sole objective." Homeland Security officials often reiterate that individual aspects of physical security screening, or even the whole checkpoint process, are only layers of a vast aviation security system that includes behavior detection officers, bomb-sniffing canine teams, federal air marshals and reinforced cockpit doors. And it's the strength of those layers in combination that will ultimately thwart terrorist attacks, says Senate Homeland Security and Governmental Affairs Chairman Ron Johnson (R-Wis.). The Senate chairman said he views the new steps the TSA is taking as "kind of Band-Aids" to try to provide some interim security improvements while Congress and the department consider bigger changes, such as expanding the role of air marshals to give them more law enforcement and investigative power. "We're obviously far from 100 percent secure. I mean, far from 100 percent secure. So we really need to look at a layered approach, think outside the box," he told POLITICO. "There's so many different facets of this problem that we need to look at, but I think security's got to be multi-layered — some visible, some invisible."

The TSA “Playbook” Strategy is backed up by decades of crime prevention practices

Lum et. Al. 11— Ph.D., Criminology and Criminal Justice, (Cynthia Lum; Charlotte Gill, Ph.D. in Criminology; Breanne Cave Ph.D. Criminology, Law, and Society; Julie Hibdon, Ph.D., Criminology, Law and Society; David Weisburd, Ph.D, Criminality, Law, and Society; “Translational Criminology: Using Existing Evidence for Assessing TSA’s Comprehensive Security Strategy at Airports,” Evidence-Based Counterterrorism Policy,

19 Aug 2011, Springer: http://link.springer.com/chapter/10.1007/978-1-4614-0953-3_10). WM Conclusion

This chapter describes the first systematic, evidence-based review and assessment

of TSA’s Playbook strategy to prevent and deter crime and terrorist activity at our nation’s airports using a translational criminological approach. As we have seen, there are very few evaluations of counterterrorism measures or airport security compared to other law enforcement sectors. Given the massive amount of money spent on such measures since 9/11, evaluation of the efficiency and outcome effectiveness of such measures is imperative. However, many of the crime-prevention measures at airports mirror a broader criminological literature on situational crime-prevention, deterrence, and interagency cooperation. Here, we have used these parallels in our preliminary assessment and evaluation of the TSA Playbook. In classifying the Playbook using an “Airport Security Matrix,” we found that most plays are immediate and tactical in nature, and few are strategic. Further, the vast majority of plays do not require cooperative deployment. Thus, much of our analysis focuses on immediate and tactical plays that are primarily carried out by TSA personnel. For these plays, we discovered four general tendencies. The first is that these plays more often involve mechanisms of prevention that aim to harden targets, deter and prevent offenders by increasing their perceived effort, rather than increase guardianship, or reduce vulnerabilities of passengers or other targets. Second, most of these plays focus on the public and employee screening areas; there is definitely a focus in the Playbook on employees rather than passengers. Third, plays occurring in public areas outside or directly inside of the airport entrance tend to be guardianship-oriented rather than specifically focused on deterring offenders. Finally, in the Playbook tends to focus on reducing passenger and target vulnerability largely at the final “layer of security” located at gates and airplanes. When we examined the immediate/tactical plays within each of the sub-books, we found additional concentrations of plays in both mechanism type and location of play. For instance, FSD plays primarily occur in screening and secure areas (both passenger and employee) and mainly involve approaches designed to increase offender efforts. HQ plays are also designed to deter offenders, but unlike the FSD plays, they are typically designed for public areas. The HQ Playbook also contains a significant majority of the plays that require cooperation between TSA and other non-TSA agencies. NR plays typically occur at secure passenger areas and gate locations and tend to use increased guardianship as their main mechanism of prevention. A small minority of the plays was strategic in nature, and most focus on long-term management activities that incorporate the use of general watchfulness and increased guardianship. It is expectedly in the strategic plays where requirements for cooperation are found. When comparing more general descriptions of plays at intersecting Matrix dimensions, we found that the Playbook generally and loosely incorporates many evidence-based practices for prevention and deterrence, although this evidence base varies across studies by design rigor as well as applicability to airport security and counterterrorism. Of course, how and which plays are implemented at any given time ultimately tempers the Playbook’s effectiveness. The majority of plays within the Playbook use situational crime-prevention mechanisms (e.g., blocking offender access and target hardening), which have been supported in other crime-prevention evaluations. Additionally, studies confirm and support the use of tailored, place-specific interventions for crime prevention and deterrence. The Playbook illustrates some compliance with this evidence-based mechanism through the location focus of many of the plays. However, how places are chosen for play implementation is not clear. More importantly, exactly how such studies translate to the context of terroristic violence within a confined location (airports) is still unknown. With regard to the notion of randomization as a deterrence mechanism, the research indicates that randomly allocating patrol at selected high-risk places can increase crime-prevention effects. However, whether the locations in which the plays are implemented are indeed the highest-risk locations in the airport is unknown. Further, although the Playbook has a built-in randomization component with regard to selection of the set of plays used at any particular time, this element of the Playbook may be manipulated in such a way that reduces randomization. However, whether this is a negative or positive change with regards to increasing security is also unknown in the absence of evaluation. Reducing random deployment of plays may not be problematic depending on whether such randomization increases or decreases deterrence. This is not clearly understood in criminological research and is not researched at all in counterterrorism studies. Further, although there is research supporting some of the prevention mechanisms that are found in both

situational crime-prevention measures and airport security (which itself needs to be more closely scrutinized for comparison), there are some types of airport security measures for which we could not easily identify parallel evidence in the crime-prevention literature. Ultimately, the determination of effectiveness must be supported by evaluations, through experimentation and simulation, of the actual interventions within airports. Finally, we think the Playbook, which uses plays that involve interagency cooperation, can actually serve as a means of facilitating and fostering working relationships between the TSA and other agencies that operate in and around the airport. It might be worthwhile to explore how these interagency relationships and efforts could benefit from involvement in additional plays beyond public airport areas and areas external to the airport. The Playbook attempts a broad range of prevention and deterrence tactics across multiple contexts. Understanding the prospects and challenges of implementing

such a strategy and identifying ways in which measures of success might be derived are imperative in accurately judging this method of airport security

TSA behavioral monitoring solves- Israeli Airline empirics prove

Adams, NORDHAUS and SHELLENBERGE 11— leading global thinkers on energy, environment, climate, human development, and politics. All work for the Breakthrough Institute. Norhaus is chairman, Shellenberg is cofounder (NICK ADAMS, TED NORDHAUS AND MICHAEL SHELLENBERGE, “COUNTERTERRORISM SINCE 9/11 Evaluating the Efficacy of

Controversial Tactics,” THE SCIENCE OF SECURITY- a project of the Breakthrough Institute, SPRING 2011, http://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf). WM

The TSA also employs behavioral profiling, whereby agents seek to discover passenger nervousness, irritability, or other suspicious signs that might indicate their intentions to commit terrorism. The methods are reputed to be highly effective in Israel, where the national airline, El Al, despite receiving almost daily terror threats, has not experienced a major attack in over three decades. TSA’s use of behavioral profiling is much less intensive than El Al’s. The latter approach submits every passenger to a battery of open-ended questions and psychological evaluations. By contrast, TSA’s Screening Passengers by Observation Techniques (SPOT) program only closely questions the rare passengers that agents deem suspicious. In practice, probably owing to the human tendency to interpret the behaviors of poorly understood out-group members as ‘exotic’ (Tajfel 1982), TSA agents, according to multiple anecdotal accounts, have been prone to apply greater scrutiny to Muslim, Arab, Sikh, and SouthAsian air passengers

TSA Screening methods effectively combat terrorism

Adams, NORDHAUS and SHELLENBERGE 11— leading global thinkers on energy, environment, climate, human development, and politics. All work for the Breakthrough Institute. Norhaus is chairman, Shellenberg is cofounder (NICK ADAMS, TED NORDHAUS AND MICHAEL SHELLENBERGE, “COUNTERTERRORISM SINCE 9/11 Evaluating the Efficacy of

Controversial Tactics,” THE SCIENCE OF SECURITY- a project of the Breakthrough Institute, SPRING 2011, http://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf). WM

MORE UNIVERSAL SCREENING METHODS SHOULD BE IMPLEMENTED IN AIRPORTS, GIVEN THEIR

EFFECTIVENESS SINCE 9/11 IN PREVENTING ATTACKS. Given that terrorist groups have avoided

heightened airport screening by recruiting new members who do not fit CAPPs (or ‘Secure Flight’) profiles, DHS and the TSA need to universally apply the highest available levels of screening to all passengers. Universal screening for liquids and metal have already made it more difficult for terrorists to either bring, or effectively detonate, bombs on planes, as the botched bombing attempts of the shoe bomber and the Christmas Day bomber demonstrate. Minimally invasive full body scanners can pose an even more effective barrier. TSA should install these scanners as quickly as possible and also consider greater implementation of randomized and unseen screening methods – which cannot be reverse-engineered by terrorists – if they continue to distinguish passengers for secondary screening

The TSA has 20 checks against terrorism, making threats very unlikely

Dillon and Thomas 15— Ph.D., Professor of Computer Information Systems,

and Professorship of Business Administration, both at James Madison University (Thomas W. Dillon, Daphyne S. Thomas, “Exploring the acceptance of body searches, body scans and TSA trust,” Journal of Transportation Security, May 2015, Springer: <http://link.springer.com/article/10.1007/s12198-015-0157-7>). WM

In response to this heightened level of concern, the Transportation Security Administration (TSA) has established a system of “20 Layers of Security.” Strengthening security through a layered approach is designed to provide defense-in-depth protection of the traveling public and the United States transportation system. Of these 20 layers, 14 are pre-boarding security designed to deter and apprehend terrorists prior to boarding aircraft (Stewart and Mueller 2008). Both pat-down body searches and full-body scanning fall under “pre-screening” measures found within the Pre-Boarding Security category. There are important issues surrounding the need for a better and more effective screening process, and a higher level of acceptance by flyer. These include designing more agile screening operations, balancing technology and human approaches to security, and focusing the appropriate levels of security resource on both stopping terrorist and meeting privacy concerns (Jacobson et al. 2009).

TSA machinery deters terrorists

Frimpong 11— PhD in public affairs (Agyemang, “Introduction of full body image scanners at the airports: a delicate balance of protecting privacy and ensuring national security,” Texas Southern University, Houston, TX, USA, 1 April 2011, Springer: <http://link.springer.com/article/10.1007/s12198-011-0068-1/fulltext.html>). WM

There has been a challenge for governments around the world balancing the security of aviation travel while protecting civil liberties and privacy of the people. In America any form of encroachment on civil liberties and personal privacy is highly resisted no matter where it comes from. The introduction of the new full body image scanners at some of the nation’s airports have stoked high passions from private citizens alleging that TSA officials would be spying on their naked bodies. The federal government counteracts these complaints by saying that the new machines could go a long way to deter potential terrorists from sneaking contrabands and weapons through the old security system. So far scholars and experts have not been able to come up with a possible solution as to how to avoid invasion of privacy while ensuring security of air travel.

Airplane security is effective- Multiple checks and deterrence

Abend 15— captain for a major airline and aviation analyst(Les, “Pilot: Is TSA security a complete failure?,” CNN, June 4, 2015, <http://www.cnn.com/2015/06/03/opinions/abend-tsa-screening-failure/>). WM

The process we all have come to know and love involves technology like magnetometers and full body scanners. But while it seems that the process starts with the smashing of your roller bag onto the security belt, trained personnel are observing behaviors. Profiling is politically incorrect, but all aspects of passenger dress and demeanor are considered part of threat assessment. If a nervous twenty-something male is wearing a winter coat in Miami rather than carrying it, an alert TSA agent will most likely apply extra scrutiny. During boarding, flight attendants perform their own screening. Over my 31 years with the airline, I have found no better people watchers than flight attendants. Passengers are their captive audience. All flight attendants are trained in defensive tactics, too, with the ability to use creative resources you could never imagine. And finally, the buck stops in the cockpit. Pilots are also trained in defensive tactics. In some cases, an unknowing terrorist who breaks into the flight deck may find himself facing the business end of a very loud and lethal semiautomatic weapon. So what's up with the Grandma screening or the child-in-the-stroller wanding? A lot of security procedures involve deterrent logic. In other words, an individual with nefarious intentions might conclude that his evil plot carries a high risk of detection, especially if everyone is a suspect. And don't underestimate the evil sickness of terrorists. It is indeed possible that Grandma or a toddler could be used to transport something

threatening. Another aspect of deterrence is randomness: not maintaining a routine during the security process, or not having the same routine at every airport. That said, my experiences at various airports around the world make me question the rationale behind procedures. At one very civilized and busy international destination, crew members are corralled through specifically designated screening areas away from passenger traffic. Almost every other crew member sets off the magnetometer alarm and then receives a thorough wanding and pat-down. In other countries, it's the opposite -- screeners are just going through the motions. Although crew members pass through the same magnetometers as passengers, everyone appears to receive the same indifferent treatment, uniform or not.

Terrorism may be increasing but the TSA has accounted for it

Herridge 14— award-winning Chief Intelligence correspondent (Catherine Herridge, “TSA head: Threat from terrorism worse now but US better able to combat it,” Fox News, December 17, 2014, <http://www.foxnews.com/politics/2014/12/17/tsa-head-threat-from-terrorism-worse-now-but-us-better-able-to-combat-it/>). WM

The outgoing and longest-serving head of the Transportation Security Administration says the threat from terrorism is worse now than when he took the job four years ago, but the U.S. is better positioned to combat foreign plots. "The threat today is unfortunately more expansive than what it was four-and-a-half years ago," John Pistole told Fox News during an interview before he leaves at the end of the month, concluding 31 years of government service -- including 27 at the FBI, where he rose to the rank of deputy director. "With that being said, we also have better insights into who the potential bombers are," he added. From Pistole's unique position at the TSA and FBI, he watched Al Qaeda's strategy evolve from the 9/11 attacks that murdered nearly 3,000 Americans, to the failed underwear bomb plot to bring down a jet on Christmas Day 2009 and the non-metallic explosive devices buried in cargo a year later. Although Al Qaeda experimented in 2012 with surgically implanted bombs before apparently abandoning the idea as impractical, Pistole suggested they are now focused on devices held close or strapped to the body. "That is one of things that concerns us, how well do they design, construct and then conceal," he said. Pistole will become president of his alma mater, Anderson University in Anderson, Ind., this spring. Fox News asked Pistole whether the threat to American aviation had diminished since August, when the U.S. launched a bombing campaign against ISIS in Syria and Iraq, and the Al Qaeda-led "Khorasan" group. Khorasan contains long-time associates of Usama bin Laden, including Sanafi al-Nasr and Muhsin al-Fadhli, as well as a handful of operatives trained by the Yemeni bomb maker Ibrahim al-Asiri, who specializes in non-metallic bombs that traditional airport screening can miss. "Without going into details about what that may look like from a classified intelligence perspective, we do remain concerned that there is active plotting going on," Pistole said. And with new information that the French bomb maker David Drugeon likely survived a U.S. air strike last month, Pistole added, "there is concern that there are still individuals out there who have not only the ability to do that, but also the intent to use that on a flight to Europe or the US." The TSA administrator also described classified procedures that track foreign fighters, based on their travel history, before they check in at overseas airports for U.S.-

bound flights. "There are individuals we are concerned about and we are again looking at if they make travel reservations, then they of course receive proper scrutiny," Pistole said.

Empirics and other countries prove the TSA is the best option

Maxa 7/14— travel expert(Rudy, host and executive producer of “Rudy Maxa’s World,” the Emmy Award-winning, travel series, “Travel Minute — A Word In Defense of the TSA,” Rudy Maxa’s World, JUL 14TH, 2015, <http://rudymaxa.com/2015/07/travel-minute-a-word-in-defense-of-the-tsa/>). WM

I and others often take the TSA to task for sloppy work, rudeness, or plain, old lack of common sense. I thought it might be nice to note that since 9/11, not a single US airline has been a victim of terrorism. Oh, folks have tried. Remember the failed effort of the so-called “Christmas underwear bomber” who tried to blow up a Northwest Airline flight from Amsterdam to Detroit in 2009? And let us keep in mind that terrorism targeting airliners is older than most know. Way back in 1933, a bomb blew up a United Airlines Boeing 247—a Chicago gangland murder was suspected—but the case was never solved. The first in-flight bombing of a jet liner was in 1962 when a Continental Airlines flight was blown up over Iowa while flying from Chicago to Kansas City, MO. An investigation determined a passenger had brought a bomb aboard in order to commit suicide as part of an insurance fraud scheme. And while Islamist terrorists have attacked Russian aircrafts—two in 2004—and a Chinese carrier was brought down in 2002 in another insurance scam, US carriers have been blessedly free of a successful terrorist action in the last 14 years. I don’t know that the TSA can take full credit, but I am certain that security curtain has caused some terrorists to re-think strategies.

TSA is key to protect against dangerous weapons, explosives, and innovate in security technologies.

John S. Pistole, 3-5-2012, "Counterterrorism, Risk-Based Security and TSA's Vision for the Future of Aviation Security," Transportation Security Administration,
<https://www.tsa.gov/press/speeches/counterterrorism-risk-based-security-and-tsa%20%99s-vision-future-aviation-security>

Remember that before September 11, 2001, there was:
¶ No cohesive system in place to check passenger names against terrorist watch lists in advance of flying;
¶ Only limited technologies in place for uncovering a wide array of threats to passengers or aircraft;
¶ No comprehensive federal requirements to screen checked or carry-on baggage;
¶ Minimal in-flight security on most flights; and,
¶ From a coordination standpoint, before 9/11 there was a lack of timely intelligence-sharing, in both directions — from the federal level down to the individual airports, as well as from an individual airport up to the national level.
¶ I came to TSA more than a year and a half ago, having worked the previous 26 years in a variety of positions within the FBI. That experience with a range of partners inside the law enforcement and intelligence communities helped shape my approach to solidifying TSA's place within the national counterterrorism continuum.
¶ Every day, we strive to ensure our operational planning and decision making process is timely, efficient and as coordinated as possible — and critically, based on intelligence. We work to share critical information with key industry stakeholders whenever appropriate, and we are constantly

communicating with our frontline officers through shift briefings held several times a day.[¶] Thanks to the effective partnerships we've forged with industry stakeholders, with our airline and airport partners, and with law enforcement colleagues at every level, TSA has achieved a number of significant milestones during its first 10 years of service.[¶] These include matching 100 percent of all passengers flying into, out of, and within the United States against government watch lists through the Secure Flight program.[¶] It includes screening all air cargo transported on passenger planes domestically and, as you know, we work closely with our international partners every day to screen 100% of high-risk inbound cargo on passenger planes. We're also working hard with these same partners to screen 100% of all international inbound cargo on passenger planes by the end of this year.[¶] And it also includes improving aviation security through innovative technology that provides advanced baggage screening for explosives.[¶] Since their inception in 2005 through February 2012, we have also conducted more than 26,000 Visible Intermodal Prevention and Response or VIPR operations. We have 25 multi-modal VIPR teams working in transportation sectors across the country to prevent or disrupt potential terrorist planning activities.[¶] Additionally, since 2006, TSA has completed more than 190 Baseline Assessments for Security Enhancement for transit, which provides a comprehensive assessment of security programs in critical transit systems.[¶] We are seeing the benefits of how these important steps — combined with our multiple layers of security including cutting-edge technology — keep America safe every day.[¶] Since our standup in 2002, we have screened nearly six billion passengers. Our front line officers have detected thousands of firearms and countless other prohibited items and we have prevented those weapons from entering the cabin of an aircraft.[¶] In fact, more than 10 years after 9/11, TSA officers still detect, on-average, between three and four firearms every day in carry-on bags at security checkpoints around the country.[¶] Deploying advanced, state-of-the-art technologies continue to factor significantly into our multi-layered approach to transportation security. In particular, we continue to see the efficacy of Advanced Imaging Technology, or AIT, machines at hundreds of passenger security checkpoints around the United States.[¶] From February 2011 to June 2011, the Office of the Inspector General (OIG) assessed the manner in which TSA inspects, maintains and operates backscatter units used in passenger screening.[¶] The OIG found that TSA was in compliance with standards regarding radiation exposure limits and safety requirements. As a result of intensive research, analysis, and testing, TSA concludes that potential health risks from screening with backscatter X-ray security systems are minuscule.[¶] While there is still no perfect technology, AIT gives our officers the best opportunity to detect both metallic and non-metallic threats including improvised explosive devices such as the device Umar Farouk Abdulmutallab attempted to detonate on Christmas Day, 2009.[¶] As manufacturers continue enhancing the detection capability and strengthening the privacy features of their machines, we maintain the ability to upgrade the software used on them to stay ahead of the rapidly shifting threat landscape. Maintaining a high level of adaptability enables us to keep an important technological advantage.[¶] Throughout 2011, this and other technologies helped our officers detect hundreds of prohibited, dangerous, or illegal items on passengers.[¶] These "good catches" as we call them, illustrate how effective our people, process and technology are at finding concealed metallic and non-metallic items concealed on a passenger or in their bags.[¶] In an ongoing effort to help educate the traveling public, we highlight many of these good catches every week in blog posts uploaded to TSA.gov. I hope some of you have seen these. They have included incidents of items concealed in shoes, to weapons hidden in a hollowed out book, to ceramic knives, to exotic snakes strapped to a passenger's leg. As strange as some of these tales may be, they are a stark reminder that now — more than 10 years after the September 11, 2001, attacks — people are still trying to bring deadly weapons onto aircraft. And our officers are detecting numerous weapons

every day and keeping them off of planes.[¶] Less than one month ago in fact, over Presidents Day weekend in February, our officers detected 19 guns in carry-on bags at various checkpoints around the country. In total, 1,306 guns were detected at airport checkpoints in 2011.

Threat to national security greater than ever, TSA is key to solve

Fox News 12-17-2014, ("TSA head: Threat from terrorism worse now but US better able to combat it," <http://www.foxnews.com/politics/2014/12/17/tsa-head-threat-from-terrorism-worse-now-but-us-better-able-to-combat-it/>)

The outgoing and longest-serving head of the Transportation Security Administration says the threat from terrorism is worse now than when he took the job four years ago, but the U.S. is better positioned to combat foreign plots.[¶] "The threat today is unfortunately more expansive than what it was four-and-a-half years ago," John Pistole told Fox News during an interview before he leaves at the end of the month, concluding 31 years of government service -- including 27 at the FBI, where he rose to the rank of deputy director.[¶] "With that being said, we also have better insights into who the potential bombers are," he added.[¶] From Pistole's unique position at the TSA and FBI, he watched Al Qaeda's strategy evolve from the 9/11 attacks that murdered nearly 3,000 Americans, to the failed underwear bomb plot to bring down a jet on Christmas Day 2009 and the non-metallic explosive devices buried in cargo a year later.[¶] Although Al Qaeda experimented in 2012 with surgically implanted bombs before apparently abandoning the idea as impractical, Pistole suggested they are now focused on devices held close or strapped to the body.[¶] "That is one of things that concerns us, how well do they design, construct and then conceal," he said.[¶] Pistole will become president of his alma mater, Anderson University in Anderson, Ind., this spring.[¶] Fox News asked Pistole whether the threat to American aviation had diminished since August, when the U.S. launched a bombing campaign against ISIS in Syria and Iraq, and the Al Qaeda-led "Khorasan" group.[¶] Khorasan contains long-time associates of Osama bin Laden, including Sanafi al-Nasr and Muhsin al-Fadhli, as well as a handful of operatives trained by the Yemeni bomb maker Ibrahim al-Asiri, who specializes in non-metallic bombs that traditional airport screening can miss.[¶] "Without going into details about what that may look like from a classified intelligence perspective, we do remain concerned that there is active plotting going on," Pistole said.[¶] And with new information that the French bomb maker David Drugeon likely survived a U.S. air strike last month, Pistole added, "there is concern that there are still individuals out there who have not only the ability to do that, but also the intent to use that on a flight to Europe or the US."[¶] The TSA administrator also described classified procedures that track foreign fighters, based on their travel history, before they check in at overseas airports for U.S.-bound flights.[¶] "There are individuals we are concerned about and we are again looking at if they make travel reservations, then they of course receive proper scrutiny," Pistole said.[¶] The continued threat from groups like Khorasan explains why procedures, implemented in July, requiring passengers to turn on their phone and computers at some airports, remain in place. As the holiday travel season begins, TSA officials say they are not expecting big changes at the checkpoints, but if there are changes, they will be driven by new and specific intelligence.[¶] Pistole said the transition from a one-size-fits-all approach after 9/11 to a risk-based strategy -- driven by

intelligence -- is one of the TSA workforce's accomplishments.¶ "I think that's been one of the biggest changes. ...We're more efficient. Complaints are down. Wait times are down," he said.¶ Data provided by the TSA showed that over Thanksgiving, more than 12.5 million passengers were screened, a 1.3 percent increase from 2013, with nearly 50 percent of these passengers getting expedited screening.¶ Nationwide, TSA said 99.6 percent of passengers waited in a line for less than 20 minutes.¶ Pistole was in Australia days before the hostage situation unfolded in Sydney last weekend, telling Fox it fit the profile of a classic lone wolf attack. "I am not aware of any intelligence about it as of last week, there was no talk about something like that," he said.¶ But it's not that kind of attack that keeps Pistole up at night.¶ "My greater concern, rather than just a lone wolf, is simultaneous attacks such as you saw on 9/11 ... with that being said, we also have better insights into who the potential bombers are," he said.

Airport -- Airline attacks coming

Security expert indicates airline attack coming now

Page 15— Washington Bureau chief of USA TODAY (Susan, “CIA veteran Morell: ISIS' next test could be a 9/11-style attack,” USA Today, May 11, 2015, <http://www.usatoday.com/story/news/politics/2015/05/10/michael-morell-cia-the-great-war/27063655/>). WM

WASHINGTON – The Islamic State simply inspired the deadly assault by two men on an exhibit of cartoons depicting the prophet Mohammed near Dallas last week, CIA veteran Michael Morell says. But it's only a matter of time before the jihadist group is likely to be in a position to direct more elaborate attacks on American soil that could result in mass casualties. "If we don't get ISIS under control, we're going to see that kind of attack," the kind of attack al-Qaeda launched on 9/11, Morell told USA TODAY. So far, U.S. efforts haven't been effective in countering the Islamic State's success in recruiting hundreds of American converts, he says, "and we're not effective at it because it's very hard to do." Morell was by President George W. Bush's side at a Florida elementary school in 2001 when the president was told hijacked airliners had crashed into the World Trade Center, and he was in the White House Situation Room with President Obama nearly a decade later when the first word was relayed that Navy Seal Team Six had killed Osama bin Laden. After 33 years in the CIA, including two stints as acting director, Morell has written an account of his experiences, published Tuesday by Twelve, titled The Great War of Our Time: The CIA's Fight Against Terrorism From Al Qa'ida to ISIS. His central point: This "great war," which already has tested the nation's national security and its politics, is likely to stretch for decades more. "For as far as I can see," he says. Just last Friday, the threat level at U.S. military bases was raised to the highest level since the 10th anniversary of 9/11, in part because of concern about the Texas attack that left the two assailants dead. "We're very definitely in a new phase in the global terrorist threat," Homeland Security Secretary Jeh Johnson warned Sunday on ABC's This Week. On Fox News Sunday, House Homeland Security Chairman Mike McCaul, R-Texas, said the groups' sophisticated use of the Internet means that "really, terrorism has gone viral." "It was a mistake to think that al-Qaeda died along with bin Laden in Abbottabad," Morell says, an assumption made by some relieved Americans that he says wasn't shared by intelligence agencies. While al-Qaeda's leadership in Afghanistan and Pakistan has been decimated, other branches of the group have thrived, including al-Qaeda in the Arabian Peninsula, based in Yemen. "They today have the ability to bring down an airliner in the United States," Morell says. "If that happened tomorrow, I would not be surprised."

ISIS will attempt 9/11 style attacks soon- masterminds currently on their side and experts see the most dangerous combination of events

Kaplan 14—political reporter (Rebecca, “Will ISIS plan a 9/11-style terror plot against the U.S.?,” CBS News, June 16, 2014, <http://www.cbsnews.com/news/will-isis-plan-a-911-style-terror-plot-against-the-u-s/>). WM

Republicans are sounding the warning that the next 9/11-like terror plot could emerge from the regions of Iraq and Syria that are currently dominated by an extremist group bearing down on Baghdad. As the Islamic State of Iraq and Syria (ISIS) - which has already captured the cities of Tikrit and Mosul and is threatening to take the capital city as well - grows in strength and

numbers, will it pose an immediate threat to the United States homeland as well? Experts say the group's increasing power and reach is concerning, though it's not entirely clear when they might be able to threaten the U.S. "You've got motivation mixed with opportunity, ideology and foreign fighters and all of that looks like a very extreme version of Afghanistan in the '90s, plus what was happening in Iraq after the Iraq war," said CBS News National Security Analyst Juan Zarate. "This is a cauldron of future terrorist threats to the west." The bigger danger, Zarate said, is that the U.S. does not yet know exactly what the group will look like once it evolves. While ISIS might not launch an attack on U.S. soil tomorrow, he said, "I think the grave threat here is that you have the seeds of a new terrorist movement emerging very aggressively." Sen. Lindsey Graham, R-S.C., said on CBS' "Face the Nation" Sunday that U.S. officials have warned the next major attack on U.S. soil could emanate from the region. "**The seeds of 9/11s are being planted** all over Iraq and Syria," Graham said. "They want an Islamic caliphate that runs through Syria and Iraq...and they plan to drive us out of the Mideast by attacking us here at home." Graham's concerns were echoed on ABC's "This Week" by Ret. Gen. Peter Chiarelli, who said that "all Americans should be concerned" by ISIS' quick rise and success in Iraq. And on "Fox News Sunday," House Intelligence Committee Chairman Mike Rogers, R-Mich., said, "I guarantee you: this is a problem that we will have to face and we're either going to face it in New York City or we're going to face it here." "These are not monkey bar terrorists out in the desert somewhere planning some very low-level attack. These are sophisticated, command and controlled, seasoned combat veterans who understand the value of terrorism operations external to the region, meaning Europe and the United States. That is about as dangerous a recipe as you can put together," he said. There have been some indications this might be the group's intent. Army Col. Kenneth King, who was the commanding officer of a U.S. detention camp in Iraq, told the Daily Beast recently that when current ISIS head Abu Bakr al-Baghdadi was released in 2009, he said, "I'll see you guys in New York." But Michael Morell, the former acting CIA director and a CBS News analyst on intelligence, national security and counterterrorism issues, predicted it's at least a year before ISIS might pose more of a serious threat to the U.S. The current major threats to the homeland still come from al Qaeda groups in Pakistan and Yemen, he said. But, Morell added, if it looks like the U.S. influence in Iraq is increasing once again, the threat from ISIS could also rise. "That's one of the downsides of U.S. involvement," he told CBS News. "The more we visibly get involved in helping the [Iraqi Prime Minister Nouri al-Maliki] government fight these guys, the more we become a target."

Terrorists ultimate targets are airlines- first strike and experience

Flintoff 12— (Corey, "Why Do Terrorists So Often Go For Planes?", NPR, MAY 15, 2012, <http://www.npr.org/2012/05/15/152750767/why-do-terrorists-so-often-go-for-planes>). WM

Ever since the Sept. 11 attacks, airports have probably been the most heavily guarded sites when it comes to preventing terrorist attacks. And yet the most recent terrorism plot in Yemen involved an attempt to blow up a U.S. airliner with a bomber wearing a difficult-to-detect explosive bomb in his underwear, according to U.S. officials. Why do terrorist groups keep trying to defeat the multiple layers of security at airports when there are so many soft targets? For one, a plane heading into the U.S. represents the first available target to strike against a large number of Americans. It doesn't require reaching the U.S. first, and then acquiring a weapon and launching an attack from U.S. soil. Also, terrorist groups have learned from previous attacks on planes.

"Terrorists like to do what they know how to do," says terrorism analyst Jessica Stern. But the difficulty of breaching airport security does appear to be generating other approaches. Two Different Types Of Plots Stern says she sees two trends. One involves developing new and more sophisticated techniques for evading security measures and attacking airplanes. The other involves "looking for low-tech ways to attack softer targets," she says. This is a way of encouraging "leaderless resistance," says Stern, the author of *Terror in the Name of God*. For example, the latest issue of *Inspire*, the jihadi magazine produced by the Yemen-based group al-Qaida in the Arabian Peninsula, includes an eight-page feature that encourages readers to start wildfires in Australia and the United States. It recommends that would-be saboteurs in the U.S. study weather patterns in order to determine when vegetation will be dry and winds favorable for a wildfire. It specifically suggests Montana as a good site for practicing pyro-terrorism, because of the residential housing that is in wooded areas. Stern says the aim of terrorism is to frighten the public and push governments into over-reacting — so spectacular, random-seeming attacks like airplane bombings work well. "Terrorists do really aim for what we call symbolic targets," she says. "Terrorism is a form of theater, so they're going to hit targets that will make us maximally afraid, and inflict the maximum amount of humiliation."

The structure and goals of terrorism make airplanes the best and only target

Kydd and Walter 10— associate professor of political science at the University of Wisconsin and professor of political science at UC San Diego's Graduate School of International Relations and Pacific Studies (Andrew H. and Barbara F., "By focusing on planes, terrorists take a calculated risk," Los Angeles Times, January 24, 2010,
<http://articles.latimes.com/2010/jan/24/opinion/la-oe-walter24-2010jan24>). WM

Targeting civilian aircraft still makes sense, from the terrorists' point of view, for at least five reasons. First, nature is working with them. People don't naturally fly 30,000 feet above the ground at 300 mph; it takes a very special machine. These machines are much more vulnerable than trains or ships. One person can easily carry enough explosives to blow a hole in the side of a pressurized aircraft, which may be enough to bring it down and kill everyone aboard. The same explosive on a train or ship would likely only cause minor damage. Second, the costs of reduced air travel, or slower air travel, are borne by business travelers and those with money -- exactly those people who are most likely to influence policymakers and government decisions. Terrorists aren't attacking for the fun of it; they want to have an impact on government policy, and the way to do that is to target those who have clout. Third, it is difficult for these travelers to switch to another mode of transportation, given the distances involved. Much as the folks at Cunard might wish otherwise, almost no amount of terrorism is going to persuade most people to take a passenger ship across the Atlantic for seven days rather than fly in seven hours. This means that demand for air travel is inelastic; travelers have little option but to bear the costs of increasing security, lost time and risks. Fourth, people are already afraid of flying. Despite statistics showing that flying is safer than driving, people are still more afraid of hurtling through the air in a large aluminum tube than sliding behind the wheel for a trip to the grocery store. It's easy to play on these fears, even with incompetent attacks that fail. Finally, our political system is structured to overreact to attacks on aircraft and to underreact to other kinds of attacks, particularly shooting sprees. In reaction to the "shoe bomber," we now all take off our shoes at security checkpoints.

Because of the "underwear bomber," we now may be subject to thorough body scans before boarding a flight. The 2006 plot to blow up seven transatlantic flights out of London cursed us with the inability to bring a bottle of water on board. Security agencies feel duty-bound to do something, and politicians wring their hands about whether they are doing enough. In comparison, there appears to be no limit to the number of fatalities that can be inflicted by automatic weapons fire in the United States without generating a political reaction. Politicians limit themselves to expressions of sorrow for the victims and the families, and then the matter is quietly dropped. One might think this provides an opportunity for Al Qaeda to easily kill large numbers of Americans, but that misses the point of terrorism. Killing large numbers in a way that is quickly forgotten is much less useful than killing a few or even none in a way that causes profound ripples of fear and costly overreactions on the part of the target group. Al Qaeda has no need to organize gun rampages against Americans if the occasional low-budget aircraft attack does the trick.

Airport -- 9/11 style attacks lead to war

The psychology of 9/11 attacks makes a public overreact and leads to war

Gander 15— (KASHMIRA GANDER, “US overreacted to 9/11 attacks says terror expert and next vice-chancellor of the University of Oxford, Louise Richardson,” The Independent, 03 June 2015, <http://www.independent.co.uk/news/world/politics/us-overreacted-over-911-says-terror-expert-and-next-vicechancellor-of-the-university-of-oxford-louise-richardson-10295014.html>). WM

The United States overreacted to the 9/11 attacks on the Twin Towers, according to the incoming vice-chancellor of the University of Oxford. The panic that ensued following the September 11 attacks played a part in the US launching the so-called War on Terror. Louise Richardson, an expert in terrorism, said the US' response was a symptom of the fact that such attacks are a “new experience” for the country. Speaking at a higher education conference in London, the principal of the University of St Andrews went on to argue that the UK is more resilient when it comes to terrorist attacks, due to the troubles in Northern Ireland. Exploring the psychological impact of terrorism, she went on to argue that random attacks have such an impact on the public because “if nobody is chosen, nobody is safe”, the Daily Mail reported. Professor Richardson went on to tell the audience, according to The Times: “Central to any terrorism campaign should be a resilient population and, I have to say, the British population in the course of the Troubles and violence in Northern Ireland proved really quite resilient. “Far more so than the United States. And the scale of the reaction - I would say over-reaction - in the United States to the 9/11 atrocity was reflective of the fact that it was such a new experience for the United States,” she added. An internationally respected scholar and author of the study ‘What Terrorist Want: Understanding the Enemy Containing the Threat’, Professor Richardson often advises policy makers on the topics of terrorism and security. Professor Richardson will become Oxford’s first female vice-chancellor when she adopts the position in January, after she was put forward by a nominating committee led by Oxford’s chancellor, Lord Patten of Barnes.

9/11 attacks eliminate party lines and make the population permit, an even support, invasions

Fournier 14— Senior Political Columnist at NJ (Ron, “Would We Rally Behind Obama After the Next 9/11?,” National Journal, August 11, 2014, <http://www.nationaljournal.com/white-house/would-we-rally-behind-obama-after-the-next-9-11-20140811>). WM

But I can't shake another, darker, question. What if we get hit again with a 9/11-sized attack? More to the point, hypothetically, would a crisis pull us together or drive us apart? It's a morbid question worth asking before the worst happens, because there's reason to worry about the durability of what Lincoln called "the better angels of our nature." What can we learn from the Bush era? Well, the nation immediately rallied behind the fledgling president (Bush had been in office only about seven months). Members of Congress famously locked arms on the East Front steps of the Capitol and sang "God Bless America." Bush's approval ratings soared to 90 percent, as he ordered U.S. troops into Afghanistan to defeat the Taliban and hunt for Osama bin Laden.

Symbolic 9/11 style attacks reinforce the war on terror mindset that we need to invade any country that harbors terrorists, making interventions inevitable

Giannella 12— University of Kent, Political Strategy and Communication (Margherita, “US: did 9/11 attacks provide a moral and legal justification to enter the war against Afghanistan?,” Acadmia, 2012, http://www.academia.edu/2626532/US_did_9_11_attacks_provide_a_moral_and_legal_justification_to_enter_the_war_against_Afghanistan). WM

INTRODUCTION The morning of 11 th September 2001, the American soil was subjected to a series of air attacks destined to remain stamped in world people's memory. Four planes were hijacked to strike the economic and military nerve centers. The first two, American Airlines Flight 11 and United Airlines Flight 175, crashed into the Twin Towers of the World Trade Center complex in New York City; the third one, American Airlines Flight 77, into the Pentagon in Washington D.C. while the last one, United Airlines Flight 93, missed the expected target falling into Pennsylvania. Nearly 3 thousand people died in the attacks. The official governmental version ascribed the attacks to 19 terrorists. In fact, in the first presidential speech released to the Nation on the evening of 9/11, Bush did not clarify who were responsible for the attacks since he mostly centred his speech on the bravery and altruism of 4 American citizens and on the government solidity and strength. Only 9 days after, President Bush, by addressing to a Joint Session of Congress and the American people, would link the 19 hijackers to Al Qaeda and in particular to its leader, Osama bin Laden. Thus, he condemned the Taliban regime accused of sponsoring shelter and supply to terrorists. However, Bush said “Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated”. So the logic apparently relies on the assumption that the US could destroy the terrorism and all of Al-Qaeda, which has hundreds of cells throughout the world, by finding and eliminating bin Laden, who resided in Afghanistan even if terrorists appeared to have had their headquarters, funding and religious roots in Saudi Arabia. Therefore, President Bush declared a global war on terror which, by starting from Afghanistan, would have stricken all those countries linked to terrorist cells 1 . However Bush and his government would not ask questions about why the attack occurred, what the terrorists might have wanted or even the ideology which inspired them to kill themselves. Instead, the President simply stated they "hate us because we are free". Thus , according to Bush, terrorists had struck America because the nation represented freedom.

Domestic Surveillance

Domestic surveillance stops terrorism

AFP 5/31/15 [“CIA Chief: Ending NSA Spying Would Boost Terror Threat”, Security Week, <http://www.securityweek.com/cia-chief-ending-nsa-spying-would-boost-terror-threat>] Schuler 39

CIA chief John Brennan warned Sunday that allowing vital surveillance programs to expire could increase terror threats, as the US Senate convened for a crunch debate on whether to renew the controversial provisions. With key counterterrorism programs set to expire at midnight Sunday, the top intelligence official made a final pitch to senators, arguing that the bulk data collection of telephone records of millions of Americans unconnected to terrorism has not abused civil liberties and only serves to safeguard citizens. "This is something that we can't afford to do right now," Brennan said of allowing the expiration of counterterrorism provisions, which "sunset" at the end of May 31. Because if you look at the horrific terrorist attacks and violence being perpetrated around the globe, we need to keep our country safe, and our oceans are not keeping us safe the way they did century ago," he said CBS' "Face the Nation" talk show. Brennan added that groups like Islamic State have followed the developments "very carefully" and are "looking for the seams to operate." The House has already passed a reform bill, the USA Freedom Act, that would end the telephone data dragnet by the National Security Agency and require a court order for the NSA to access specific records from the vast data base retained by telecommunications companies. If no action is taken by the Senate Sunday, authorities will be forced to shut down the bulk collection program and two other provisions, which allow roving wiretaps of terror suspects who change their mobile phone numbers and the tracking of lone-wolf suspects. Senator Rand Paul, a Republican 2016 presidential candidate adamantly opposed to reauthorizing the surveillance, is threatening to delay votes on the reform bill or an extension of the original USA Patriot Act. That would force the counterterrorism provisions to lapse until at least Wednesday. Former NSA chief Michael Hayden, who is also a former CIA director, equated such a temporary lapse as "giving up threads" in a broader protective fabric. "It may not make a difference for a while. Then again, it might," he told CNN's State of the Union. "Over the longer term, I'm willing to wager, it will indeed make a difference."

Domestic surveillance is vital to the *intelligence* necessary to deter and disrupt terrorism

Sims, 7 (Jessica Sims, Senior Fellow in National Intelligence at the Chicago Council on Foreign Affairs, “Intelligence to counter terror: The importance of allsource fusion”, Intelligence and National Security Volume 22, Issue 1. 3/15/7.

<http://www.tandfonline.com/doi/abs/10.1080/02684520701200772>) KW

This is the story of MASK – the codename for MI-5’s penetration of the Communist Party of Great Britain during the period between the two world wars. Although the details of the story are worth rereading in the post-9/11 political context, just the facts summarized above suggest three truths about counterintelligence operations directed against networks: they involve intrusive domestic operations, often against domestically based groups designed to ‘disappear’ within the societies in which they operate; they require patient accumulation of data over a lengthy period of time; and they depend on information fused from a variety of widely differing sources. These three ingredients, essential for such operations almost a century ago, are still important in the age of global, digitalized information flows and transnational threats. In fact, the new, digital environment has made transnational crimes vastly easier to coordinate on a worldwide scale than was possible before World War II. It has also exacerbated a most serious

challenge: governments attempting to stop terrorists – particularly democracies – are expected to do so without undermining the laws, representative principles and informal confidences upon which a culture of democracy depends. Unfortunately, what Britain succeeded in doing against its domestic threat – to the satisfaction of the British public – was done even ‘better’ within the militarized German state by Hitler’s Gestapo and Waffen SS (Schutzstaffel). If, as President Truman once promised the American people, we are not in the business of creating a Gestapo in this country, what are the proper limits of our counterintelligence business?¹ The purpose of this article is to examine the modern intelligence requirements for countering terror in order to appreciate this challenge in greater depth and to develop a reasoned basis for balancing counterintelligence capabilities with civil liberties. What is meant by all-source data fusion in intelligence work and how necessary is it against terrorists? How necessary are government-wide databases of digitalized information and why does the idea of connecting them worry civil libertarians? If, as the post-9/11 commissions have suggested, one of the US government’s worst intelligence failures during this tragedy was the lack of adequate data fusion and analysis, what has been done about it and can we do more without intolerable risks to our social and moral fabric?² To explore these questions, this article will begin by considering the nature of the terrorists we face and the requirements for good intelligence operations against them. Historical examples will illustrate that there are lessons to be learned from the defeat of similar threats in the past, including the recurring ways in which challenges to civil liberties arise as democracies optimize intelligence in the name of security. Second, we will run through the special opportunities and challenges modern technology presents. Third, we will discuss an essential next step for democracies threatened by terrorists in their midst.³ As has been repeatedly pointed out, terrorism is a tool, not an adversary. Yet adversaries who use this tool reveal much about themselves. They are ruthless, have strategies and tactics that require operational access to their victims, and they are able to organize in pursuit of their goals. Moreover, unless psychopathic, they use terror because they have no alternative that offers as much opportunity to win battles as this method does. Public access to national treasures and freedom to organize are integral to western democracies’ most vital interests. Democracies intent on fighting adversaries that exploit openness to kill massively risk undermining themselves. To counter such adversaries at the strategic level may require understanding their larger purposes in order to deflect, overcome or undermine them. But to defeat them at the tactical level, one must deny them access, disrupt their ability to organize, or deny them their ‘victories’ even if their tactics succeed. One must know what they are doing and either catch them at it or refuse to flinch – ideally both. Intelligence, in any case, is essential.⁴ The Role of Intelligence⁵ ‘Intelligence’ is best understood as the collection, analysis and dissemination of information by parties in conflict or competition. What turns the simple pursuit of information into the business of intelligence is its purpose: gaining competitive advantage over adversaries.⁶ This goal fuels the desire for specific, urgent and often secret knowledge as well as a systematic way of obtaining it in time to win the contest. Given that the context is competition, such ‘decision advantages’ can be acquired in two ways: by getting better information for one’s strategy than one’s opponents gain for theirs, or by degrading the competitors’ decision-making through denial, disruption, deception, or surprise.⁴ This latter category of activity is called counterintelligence. More than just security, counterintelligence involves discovering what opponents think they need to know and then using this information to block, disorient, confuse and ultimately beat them. In virulent or hostile competitions, increasing the speed of one’s own decision-making and the mobility of the decision-makers, may unbalance the opponent more than trying to discern and defend all the information believed to be critical to that opponent’s strategy – a process that can actually slow decision-making down and cripple one’s offensive. Of course, the best way to protect an intelligence system is to own the adversary’s intelligence system through the use of moles, double agents and the like.⁴ Gangs, bureaucrats and football teams all use a form of intelligence to gain advantages over their competitors.⁵ The more intense and lawless the competition, such as in international politics, the more secretive intelligence operations tend to become and the more decisive the potential advantages they offer. In fact, for states, intelligence can be more than a life or death enterprise; it can entail the end of nations and cultures.⁶ For these reasons, secrecy is often viewed as a necessary component of national or transnational intelligence efforts. It is more accurate, however, to think of secrecy as an attribute of a relatively good intelligence effort – not an essential requirement for it. Some contestants’ counterintelligence capabilities are so poor that they are not aware of what information they need to protect in order to beat their adversaries. Or they believe their relative agility makes such protection unnecessary. To try to defeat such opponents by only looking for the secrets they protect would lead to failure. Intelligence must

instead work to collect the information that provides the competitor with a decision advantage over opponents – whether that information is secret or not – and to assume adversaries are doing likewise.

Domestic surveillance stops terrorism by maximizing the effectiveness of the US technological advantage

Posner, 8 (Richard Allen Posner is an American jurist and economist, who is a judge on the United States Court of Appeals for the Seventh Circuit in Chicago and a Senior Lecturer at the University of Chicago Law School. 2008. University of Chicago Law School; Chicago Unbound. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2808&context=journal_articles) KW

We should be playing to our strengths, and one of the greatest of them is technology. **We may not be able to prevail against terrorism with one hand tied behind our back.** Critics of surveillance argue that since our enemies know that we monitor electronic communications, they will foil us by simply ceasing to use such communications. That is wrong. We know it is wrong because we do intercept terrorist communications.²⁴ But if it were true that our monitoring caused the terrorists to abandon the telephone and the internet, **that would be an enormous victory for counterterrorism, as it is extremely difficult to coordinate and execute a major terrorist attack if all communications among the plotters must be face to face to avoid detection.** The greater danger is that encryption and other relatively cheap and simple countermeasures will defeat our surveillance. **Opponents of efforts to amend FISA point out that the Foreign Intelligence Surveillance Court has almost never turned down an application for a warrant. In 2005, for example, although more than 2,000 applications were filed, not a single one was denied in whole or in part.**⁵ The inference the critics wish drawn is that FISA is not inhibiting surveillance. **The correct inference is that the Justice Department is too conservative in seeking warrants. The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time. The effect of our legalistic culture is to cause law enforcement agencies, notably the FBI, to avoid not only violating the law but also steering so close to the wind that they might be accused, albeit groundlessly, of violating the law or of being "insensitive" to values that inform the law, even when those values have not been enacted into law.**

Surveillance need more than ever

Inserra 6/29 [David - specializes in homeland security and cybersecurity issues at the Allison Center for Foreign and National Security Policy at The Heritage Foundation. “Turning the tide on terrorism”, The Heritage Foundation, 6/29/15, <http://www.heritage.org/research/commentary/2015/6/turning-tide-on-terrorism>] Schuler 48

Their surveillance operation blown, the police moved in and arrested Saleh and the other conspirator who ran at the police vehicle. **After questioning Saleh, the FBI learned that the group had planned to use a bomb, run over law enforcement that responded with a car, and then take their weapons to attack others. Saleh pledged full allegiance to Islamic State and claimed that his co-conspirators had also.** When the FBI went to arrest Mumuni on June 17, he stabbed an FBI agent multiple times, but the agent's vest prevented the knife from doing any serious injury. **The Saleh case, one of three foiled attacks in June alone, shows why law enforcement and intelligence officials need more tools to stop terrorists before they strike - not fewer, as some lawmakers have suggested.** Legitimate government surveillance programs, for example, are a

vital component of our national security and should be allowed to continue. Greater cyber-investigation capabilities in the higher-risk urban areas are also essential. **With so much terrorism-related activity occurring on the Internet, local law enforcement should be able to monitor and track violent extremist activity on the Web** when reasonable suspicion exists to do so. Greater intelligence and law enforcement cooperation is also needed to uncover and neutralize terrorist plots, curtail the flow of foreign fighters to Syria, and monitor the activities of foreign fighters who have returned to the U.S. and other countries. This doesn't mean we allow anything in the name of national security. Far from it. The government has an obligation to follow the law and respect individual privacy and liberty. **But within those necessary strictures, we should give our law enforcement and intelligence officials all the tools they need - to ensure that any future aspiring terrorists remain as unknown as Munther Omar Selah.**

Spies/DITU

DITU key to intelligence and counterterrorism efforts.

Harris, 13 (Shane Harris is a senior staff writer at Foreign Policy, covering intelligence and cyber security. He is the author of *The Watchers: The Rise of America's Surveillance State*, which chronicles the creation of a vast national security apparatus and the rise of surveillance in America, 11/23/13, Foreign Policy, "Meet the Spies Doing the NSA's Dirty Work", <http://foreignpolicy.com/2013/11/21/meet-the-spies-doing-the-nsas-dirty-work/>) KW

With every fresh leak, the world learns more about the U.S. National Security Agency's massive and controversial surveillance apparatus. Lost in the commotion has been the story of the NSA's indispensable partner in its global spying operations: an obscure, clandestine unit of the Federal Bureau of Investigation that, even for a surveillance agency, keeps a low profile.

When the media and members of Congress say the NSA spies on Americans, what they really mean is that the FBI helps the NSA do it, providing a technical and legal infrastructure that permits the NSA, which by law collects foreign intelligence, to operate on U.S. soil. It's the FBI, a domestic U.S. law enforcement agency, that collects digital information from at least nine American technology companies as part of the NSA's Prism system. It was the FBI that petitioned the Foreign Intelligence Surveillance Court to order Verizon Business Network Services, one of the United States' biggest telecom carriers for corporations, to hand over the call records of millions of its customers to the NSA.[¶] But the FBI is no mere errand boy for the United States' biggest intelligence agency. It carries out its own signals intelligence operations and is trying to collect huge amounts of email and Internet data from U.S. companies — an operation that the NSA once conducted, was reprimanded for, and says it abandoned.[¶] The heart of the FBI's signals intelligence activities is an obscure organization called the Data Intercept Technology Unit, or DITU (pronounced DEE-too). The handful of news articles that mentioned it prior to revelations of NSA surveillance this summer did so mostly in passing. It has barely been discussed in congressional testimony. An NSA PowerPoint presentation given to journalists by former NSA contractor Edward Snowden hints at DITU's pivotal role in the NSA's Prism system — it appears as a nondescript box on a flowchart showing how the NSA "task[s]" information to be collected, which is then gathered and delivered by the DITU.[¶] But interviews with current and former law enforcement officials, as well as technology industry representatives, reveal that the unit is the FBI's equivalent of the National Security Agency and the primary liaison between the spy agency and many of America's most important technology companies, including Google, Facebook, YouTube, and Apple.[¶] The DITU is located in a sprawling compound at Marine Corps Base Quantico in Virginia, home of the FBI's training academy and the bureau's Operational Technology Division, which runs all the FBI's technical intelligence collection, processing, and reporting. Its motto: "Vigilance Through Technology." The DITU is responsible for intercepting telephone calls and emails of terrorists and foreign intelligence targets inside the United States. According to a senior Justice Department official, the NSA could not do its job without the DITU's help. The unit works closely with the "big three" U.S. telecommunications companies — AT&T, Verizon, and Sprint — to ensure its ability to intercept the telephone and Internet communications of its domestic targets, as well as the NSA's ability to intercept electronic communications transiting through the United States on fiber-optic cables.[¶] For Prism, the DITU maintains the surveillance equipment that captures what the NSA wants from U.S. technology companies, including archived emails, chat-room sessions, social media posts, and Internet phone calls. The unit then transmits that information to the NSA, where it's routed into other parts of the agency for analysis and used in reports.[¶] After Prism was disclosed in the Washington Post and the Guardian, some technology company

executives claimed they knew nothing about a collection program run by the NSA. And that may have been true. The companies would likely have interacted only with officials from the DITU and others in the FBI and the Justice Department, said sources who have worked with the unit to implement surveillance orders.¶ "The DITU is the main interface with providers on the national security side," said a technology industry representative who has worked with the unit on many occasions. It ensures that phone companies as well as Internet service and email providers are complying with surveillance law and delivering the information that the government has demanded and in the format that it wants. And if companies aren't complying or are experiencing technical difficulties, they can expect a visit from the DITU's technical experts to address the problem.¶ * * * Recently, the DITU has helped construct data-filtering software that the FBI wants telecom carriers and Internet service providers to install on their networks so that the government can collect large volumes of data about emails and Internet traffic.¶ The software, known as a port reader, makes copies of emails as they flow through a network. Then, in practically an instant, the port reader dissects them, removing only the metadata that has been approved by a court.¶ The FBI has built metadata collection systems before. In the late 1990s, it deployed the Carnivore system, which the DITU helped manage, to pull header information out of emails. But the FBI today is after much more than just traditional metadata — who sent a message and who received it. The FBI wants as many as 13 individual fields of information, according to the industry representative. The data include the route a message took over a network, Internet protocol addresses, and port numbers, which are used to handle different kinds of incoming and outgoing communications. Those last two pieces of information can reveal where a computer is physically located — perhaps along with its user — as well as what types of applications and operating system it's running. That information could be useful for government hackers who want to install spyware on a suspect's computer — a secret task that the DITU also helps carry out.¶ The DITU devised the port reader after law enforcement officials complained that they weren't getting enough information from emails and Internet traffic. The FBI has argued that under the Patriot Act, it has the authority to capture metadata and doesn't need a warrant to get them. Some federal prosecutors have gone to court to compel port reader adoption, the industry representative said. If a company failed to comply with a court order, it could be held in contempt.¶ The FBI's pursuit of Internet metadata bears striking similarities to the NSA's efforts to obtain the same information. After the 9/11 terrorist attacks, the agency began collecting the information under a secret order signed by President George W. Bush. Documents that were declassified Nov. 18 by Barack Obama's administration show that the agency ran afoul of the Foreign Intelligence Surveillance Court after it discovered that the NSA was collecting more metadata than the court had allowed. The NSA abandoned the Internet metadata collection program in 2011, according to administration officials.¶ But the FBI has been moving ahead with its own efforts, collecting more metadata than it has in the past. It's not clear how many companies have installed the port reader, but at least two firms are pushing back, arguing that because it captures an entire email, including content, the government needs a warrant to get the information. The government counters that the emails are only copied for a fraction of a second and that no content is passed along to the government, only metadata. The port reader is designed also to collect information about the size of communications packets and traffic flows, which can help analysts better understand how communications are moving on a network. It's unclear whether this data is considered metadata or content; it appears to fall within a legal gray zone, experts said.¶ * * * The DITU also runs a bespoke surveillance service, devising or building technology capable of intercepting information when the companies can't do it themselves. In the early days of social media, when companies like LinkedIn and Facebook were starting out, the unit worked with companies on a technical solution for capturing information about a specific target without also capturing information related to other people to whom the target was connected, such as comments on posts, shared photographs, and personal data from other people's profiles, according to a technology expert who was involved in the negotiations.¶ The technicians and engineers who work at the DITU have to stay up to date on the latest trends and developments in technology so that the government doesn't find itself unable to tap into a new system. Many DITU employees used to work for the telecom companies that have to implement government surveillance orders, according to the industry representative. "There are a lot of people with inside knowledge about how telecommunications work. It's probably more intellectual property than the carriers are comfortable with the FBI knowing."¶ The DITU has also intervened to ensure that the government maintains uninterrupted access to the latest commercial technology. According to the Guardian, the unit worked with Microsoft to "understand" potential obstacles to surveillance in a new feature of Outlook.com that let users create email aliases. At the time, the NSA wanted to make sure that it could circumvent Microsoft's encryption and maintain access to Outlook messages. In a statement to the Guardian, Microsoft said, "When we upgrade or update products we aren't absolved from the need to comply with existing or future lawful demands." It's the DITU's job to help keep companies in compliance. In other instances, the unit will go to companies that manufacture surveillance software and ask them to build in particular capabilities, the industry representative said.¶ The DITU falls under the FBI's Operational Technology Division, home to agents, engineers, electronic technicians, computer forensics

examiners, and analysts who "support our most significant investigations and national security operations with advanced electronic surveillance, digital forensics, technical surveillance, tactical operations, and communications capabilities," according to the FBI's website. Among its publicly disclosed capabilities are surveillance of "wireline, wireless, and data network communication technologies"; collection of digital evidence from computers, including audio files, video, and images; "counter-encryption" support to help break codes; and operation of what the FBI claims is "the largest fixed land mobile radio system in the U.S."¶ The Operational Technology Division also specializes in so-called black-bag jobs to install surveillance equipment, as well as computer hacking, referred to on the website as "covert entry/search capability," which is carried out under law enforcement and intelligence warrants.¶ The tech experts at Quantico are the FBI's silent cybersleuths. "While [the division's] work doesn't typically make the news, the fruits of its labor are evident in the busted child pornography ring, the exposed computer hacker, the prevented bombing, the averted terrorist plot, and the prosecuted corrupt official," according to the website.¶ According to former law enforcement officials and technology industry experts, the DITU is among the most secretive and sophisticated outfits at Quantico. The FBI declined Foreign Policy's request for an interview about the unit. But in a written statement, an FBI spokesperson said it "plays a key role in providing technical expertise, services, policy guidance, and support to the FBI and the intelligence community in collecting evidence and intelligence through the use of lawfully authorized electronic surveillance."

Increasing Transparency Links

Increasing transparency increases terrorism risks because terrorists can take advantage of the information

SENATOR CHARLES GRASSLEY (R-IA), July 31, 2013, Hearing of the Senate Judiciary Committee Subject: "Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs"

<https://www.hsl.org/?view&did=741931>

Finally, increased transparency is a worthy goal in general. And as I suggested before, whenever we can talk about these programs, I think there's less questions out there in the minds of people, and we probably created some public relations problems for us and for this program and for our national security community because maybe we haven't made enough information available. I say that understanding that we can't tell our enemies what we -- what tools we use. But if we consider any reform that may bring more transparency to the FISA process, we should keep in mind, then, that every piece of information we make available to the public will be read by a determined adversary, and that adversary has already demonstrated the capacity to kill thousands of Americans, even on our own soil.

Domestic Anti-Terrorism Key

DOMESTIC ANTITERRORISM IS KEY- IT'S THE LINCHPIN TO ALL OTHER STRATEGIES

Michael Massing, Journalist, 2001

[The American Prospect, " Home-Court Advantage: What the War on Drugs Teaches Us about the War on Terrorism, 12/3, 12: 21, <http://prospect.org/article/home-court-advantage>]

Might not the same be true with terrorism? There is no treatment analogy, of course. But if our main goal is to prevent future terrorist attacks, wouldn't it be more effective to concentrate our enforcement efforts here, in the United States, instead of operating on the hostile terrain of the Middle East? In all the talk about unleashing the CIA, it's often overlooked that the perpetrators of September 11 had been living in this country for years. In detecting and rooting out terrorists, shouldn't we tend primarily to our own backyard? The Home Team Emphasizing prevention at home would offer a number of advantages. First, it's much easier to carry out undercover work here than abroad. Agents face fewer hazards in San Diego, Trenton, and Boca Raton than they do in Beirut, Cairo, or Peshawar. And we have many more resources here. In addition to the FBI and other federal agencies, thousands of local police officers are working on terrorism in cities across the country. In the drug war, the local police have led the way in dismantling drug gangs, and they could make a similar contribution toward uprooting terrorist networks. Furthermore, when it comes to obtaining "HUMINT"--the critical "human intelligence" collected by investigative agencies--the millions of loyal American Muslims living in this country would seem a far more fruitful source than Islamic fundamentalists in the Middle East. Finally, concentrating on domestic law enforcement would avoid the types of covert actions that have proved so costly and embarrassing in the past.

Counterterrorism Generally Effective

Efforts to track-down and arrest terrorists are effective

Heritage Foundation, August 2011, Homeland Security 2010,
<http://www.heritage.org/Events/2011/08/Terror-Trends?query=Terrorism+by+the+Numbers:+Understanding+U.S.+and+Global+Trends>

A decade after the 9/11 terrorist attacks and after the demise of Osama bin Laden, looking back is as important as looking forward, in order to learn from the past and to examine the current and future threats facing the United States. Domestically, **since the terrorist attacks of September 11, 2001, at least 40 terror plots against the U.S. have been foiled thanks to domestic and international cooperation, as well as efforts to track down terror leads in local communities.** Likewise, on a global scale, from 1969 to 2009, there were a staggering 38,345 terrorist incidents around the world, with nearly 3,000 targeted at the United States alone. These numbers serve as a reminder that **terrorists have not relented in their desire to harm the United States and its people – America needs to remain vigilant.** Join us as our panelists discuss the nature of the terrorist threat to the United States and U.S. counterterrorism policy since 9/11.

Existing US counterterrorism efforts effective

Bergen, et al, September 2013, Jihadist Terrorism: A Threat Assessment,
http://bipartisanpolicy.org/sites/default/files/Jihadist%20Terrorism-A%20Threat%20Assesment_0.pdf

Peter Bergen is the author of four books about al-Qaeda, three of which were *New York Times* best sellers. The books have been translated into 20 languages. He is the director of the National Security Program at the New America Foundation in Washington, D.C.; a fellow at Fordham University's Center on National Security; and CNN's national security analyst. He has held teaching positions at the Kennedy School of Government at Harvard University and at the School of Advanced International Studies at Johns Hopkins University.[¶] Bruce Hoffman is a professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where he is also the director of both the Center for Security Studies and the Security Studies Program. He previously held the corporate chair in counterterrorism and counterinsurgency at the RAND Corporation and was the scholar-in-residence for counterterrorism at the CIA between 2004 and 2006.[¶] Michael Hurley is the president of Team 3i LLC, an international strategy company, and advises the Bipartisan Policy Center's Homeland Security Project. He led the 9/11 Commission's counterterrorism policy investigation, as well as CIA personnel in Afghanistan immediately after the 9/11 attacks. He retired from the CIA following a 25-year career and has served as director on the National Security Council staff.[¶] Erroll Morris is the associate director of research transition at the Department of Homeland Security's National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California, where he is an adjunct professor in the Sol Price School[¶] of Public Policy. He is a former FBI special agent and was President Barack Obama's nominee for the Transportation Security Administration, as well as Governor Arnold Schwarzenegger's deputy director for the California Office of Homeland Security and the chief of homeland security and intelligence for the LAX Police Department. He is the author of *Homegrown Violent Extremism*.)

As detailed above, **al-Qaeda has weakened considerably over the past few years, while U.S. defenses have been strengthened.** Just consider the following changes since the 9/11 attacks:

- **On 9/11, there were 16 people on the “no fly” list. Now there are more than 20,000.**
- **In 2001, there were 32 Joint Terrorism Task Force “fusion centers”** where multiple law enforcement agencies work together to chase down leads to build terrorism cases. **Now there are 103.**
- A decade ago, **the Department of Homeland Security, National Counterterrorism Center, Transportation Security Administration, U.S. Northern Command, and U.S. Cyber Command** didn't exist. All of these new institutions **currently make it much harder for terrorists to operate in the United States.**
- **Before 9/11, Special Operations Forces were rarely deployed against al-Qaeda and allied groups. Now they perform nearly a dozen operations every day in Afghanistan,** as well as missions in other countries such as Yemen and Somalia.
- At the beginning of the 21st century, the American public didn't comprehend the threat posed by jihadist terrorists,

but that changed dramatically after 9/11. In December 2001, it was passengers who disabled Richard Reid, “the shoe bomber.” Similarly, it was fellow passengers who tackled Umar Farouk Abdulmutallab, the “underwear bomber,” eight years later. And the following year, it was a street vendor who spotted the bomb-laden SUV Faisal Shahzad had parked in Times Square.

□□ Before 9/11, the CIA and the FBI barely communicated about their respective investigations of terrorist groups. Now they work together quite closely.

□□ The U.S. intelligence budget grew dramatically after 9/11, giving the government large resources with which to improve its counterterrorism capabilities. In 2010, the United States spent more than \$80 billion on intelligence collection and other covert activities, a total more than three times what it spent in 1998.

OCOs

OCO's are vital to target ISIS use of the internet – prevents cyber attacks and disrupts command and control

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” The American Interest, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

Going on Cyber Offense

At the moment, the web presence of Islamist extremists is a sort of “gateway drug” into the cyber world. If the United States and its allies do not address it now, they may have to accept extremist cyber activity of increasing breadth and sophistication, with greater cyberspace consequences. Terrorist use of cyberspace also works to internationalize the Islamist fight. In a sense, the “cyber jihad” world is flat, connecting individuals worldwide who might not otherwise have been connected.

If Islamist extremists turn their attention to disruption and destruction through the web, they are likely to conduct distributed denial of service (DDOS) attacks and threaten the controls for electric power grids, oil pipelines, and water systems. Should social media accounts become useful for disseminating cyber weapons, Islamists would gain additional capacity.

Threat is a function of expertise and access. Fortunately, the Islamic State’s cyber expertise overall is low, as is its access to high-quality advice or tutelage. But unlike with the development of WMD, both expertise in and access to cyber capabilities can change overnight, particularly should a capable revisionist state or individual decide to assist the Islamic State. With WMD, a research-and-development phase exists during which U.S. and other intelligence services can discern, evaluate, and plan accordingly. With cyber weapons, space, time, and geography offer up no comparable advantages. Delivery methods for cyber weapons are much easier to devise and disseminate, and have little to no lead-time (no lengthy research and development phase). In short, the targets would likely not see it coming.

There is reason for concern. A 2013 edition of Inspire called upon jihadists to burn parked cars, make oil slicks to cause car accidents, and puncture tires with nails hammered into blocks of wood. It used to be that al-Qaeda wanted a spectacular follow-on attack to 9/11 and desired to take on the West as a whole. It did not want just any attack; it wanted a good one. Today, al-Qaeda affiliates seem to be calling for any attack, even those as comparatively minor as an individual picking up an AK-47 or using a private vehicle to run over people. The Islamic State’s online magazine, Dabiq, has called for its supporters living in Western countries to rise up individually and attack law enforcement and government officials. It seems to have abandoned the long-sought “spectacular” follow-up to 9/11. It is reasonable to think al-Qaeda’s attitude toward cyber weapons may change too.

Should just the right expert hacker join the Islamic State or al-Qaeda, whether for money or out of sympathy, either group could move overnight from a cyber nuisance to a serious cyber power. It is not inconceivable that rivals to the United States, Israel, or the cultural West in general such as Iran might provide such cyber weapons to al-Qaeda, or even to its enemy the Islamic State.

Tehran might do so as a means to fight the United States asymmetrically, divert U.S. attention from its nuclear weapons program or its support for Shi'a terrorists worldwide, or simply create a deeply distracting economic drain for the United States.

Further, the forensic attribution problem for the United States and its allies, should a cyber weapon be used against it, would be horrendous. The cyber weapon might appear to be Russian- or Chinese- or Iranian-made if its code were originally written in one of those countries, but that will not mean the weapon was delivered by that state. Regardless of whether al-Qaeda or the Islamic State took credit for the attack, the United States might be confused as to who created such a cyber weapon, who sent it and why, and how to defend against a repeat attack.

So far, the Islamic State has not been too interested in cyber weapons for three probable reasons: cyber weapons are not spectacular enough in their destruction (messing with websites and infrastructure is not as powerful an image as a beheading video); it lacks the technical ability to create such weapons; and “cyber jihad 2.0” has served it well thus far. Despite some setbacks, the Islamic State is currently flushed with success—why change anything?

One of those successes is of a particularly unusual and alarming nature. Most Islamic State supporters today were teenagers when 9/11 occurred and are children of the internet and social media. Their radicalization is very recent; it is a post-bin Laden phenomenon. Their motivation for joining the Islamic State has more to do with the dynamics of a social network that provides direction, identity, and excitement than it does with religious understanding. The Islamic State dangles the opportunity to join something new and exciting in front of bored and disaffected teens.¹⁹ This social media strategy is aimed purposefully at youth worldwide. How does this work?

Islamic State videos take the traditional Western narrative, that Islamist extremists kill Muslims and are wanton, heretical murderers, and stand it on its head. It has made images of murder the centerpiece of its new message. Its production quality is so good that it has spawned the term “jihadi cool.” Whereas al-Qaeda produced rather flat websites that merely posted radical content (“cyber jihad 1.0”), the Islamic State produces videos and online magazines that are on par in quality, editing, and message delivery with current Western media. It practices “cyber jihad 2.0” at the least through its production quality and cutting-edge use of social media. It keeps pace with advances in Western media production, aided, no doubt, by the many Western supporters it has managed to attract. Its video production, in particular, is constantly uploaded, taken down but then uploaded again to numerous video sites so that it ultimately reaches its intended audience.²⁰ Islamic State videos proclaim righteous victory over the Shi'a and other so-called non-believers, about which there is nothing unusual or unexpected. But it showcases acts of brutality, a new phenomenon that Western analysts ignore at all our peril. ISIS professionals have managed to frame brutality in such a way that it engenders pride and a sense of inclusion, rather than revulsion.

It does not occur to most normal adults in Western countries how this can work. We do not readily understand why a first- or second-generation Muslim living in London, or Amsterdam, or Marseilles, or Toronto would want to leave a typical middle-class life to go wallow in blood in the middle of the Syrian desert. Until we do come to understand this, and understand why some such people are attracted by the opportunity to do unspeakably brutal things to total strangers, we will never defeat the Islamic State.

What to Do

To repeat, the strategic goal of the U.S. government is to defeat al-Qaeda and the Islamic State. To do so, the United States must shut down the insidious messages of its jihadi enemies and contest their presence on the internet. Counter-Islamist efforts, therefore, must make it a priority to shut down its militant websites and social media.

Well-meaning professionals argue that these websites and social media outlets serve as the means to identify, monitor, and assess jihadi groups and their sympathizers. But the argument that the intelligence loss would outweigh the gain of contesting these sites misunderstands the end goal: denying the enemy's ability to recruit, support operations, pass weapons information and formulae, and promote extremist ideology that encourages terrorism. The point is to end the threat, not write reports about it.

Internet key to ISIS

The internet is the most important venue for terrorist communication -

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” The American Interest, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

The Islamic State of Iraq and al-Sham (ISIS) would not exist today were it not for its prolific and shrewd use of the internet and social media. Al-Qaeda would have likely died years ago, too, had its appeal not been kept alive by the same means. Without contesting extremist use of the internet, the United States and its allies will fail to defeat the Islamic State and to eliminate al-Qaeda, both of which are, let us remember, the stated goals of U.S. policy. Certainly, bombing ISIS without a broad and complementary political strategy will not work, and may even prove counterproductive in the long run by strengthening evidence for the radical Salafi narrative that all means of defense are justifiable since the West started a war with Islam.

Lacking infrastructure and the resources of a state, Islamist extremists use the web to redress strategic disadvantages in planning attacks, maintaining and financing their organizations, and recruiting and inspiring new affiliates. ISIS leaders and workers will likely rely on the web to maintain a global presence and reach, but also use it in creatively offensive ways that al-Qaeda never did.

There are three types of Salafi websites: official Islamic State and al-Qaeda websites; “wanna-be sites” (by groups that want to be recognized as aligned); and mirror sites (groups or individuals who merely re-post extremist content). Through the internet, these groups also maintain a somewhat organized command-and-control structure.

Given the heavy physical stress the United States and its allies have placed on al-Qaeda in particular since 2001, some argue that al-Qaeda leadership has since devolved into “only” a media organization that now practices terrorism only when it can get its depleted ways and means together. It is a “terrorism studio” today and not much else; it no longer attempts much strategic planning and plotting, or deploys facilitators, logisticians, operators, and execution managers. Once al-Qaeda lost its physical safe havens where it hid from U.S. harassment, it established virtual safe havens.

The Islamic State’s internet presence, however, is not residual and defensive in nature; it is increasingly sophisticated and effective. The Islamic State has established an internet sanctuary, perhaps learning from al-Qaeda’s experience. But it has added much more savvy operational security (OPSEC) to its communications, especially through social media. It has rejected al-Qaeda’s squeamishness about the murder of Muslims (not that al-Qaeda has not murdered a great many Muslims anyway) and made such murder the centerpiece of its online message. It seems to work for recruitment purposes; murder has become a form of performance art by which the Islamic State advances its brand.

Given that al-Qaeda and the Islamic State use cyberspace to attack us in the real world, it follows that cyberspace should constitute no special sanctuary for them. Yet for all practical purposes it does. Their presence in cyberspace is more or less uncontested, enabling the internet to serve well

as a “drive-thru” radicalization asset. Anyone from anywhere can read the radical ideology of al-Qaeda and the Islamic State unmolested, getting their fill of pseudo-intellectual ideology and bomb-making instructions. The internet thus serves as a kind of on-ramp for those who then travel abroad for specific training or to make personal connections. Once in theater, the clever use of social media allows the Islamic State to use temporary email accounts, Twitter accounts, and hashtag re-postings to communicate crude operational commands.

The internet has become a key means for the Islamic State leadership to bring the ideological seeker and mentor together, and thus operationalize its forces via an infrastructure that the United States and its Western allies developed, financed, installed, and still maintain. It provides that sense of identity and belonging required for the disaffected and psychologically vulnerable to move to the stage of violence. In other words, the internet has become not just a jihadi mentor—a “virtual spiritual sanctioner” as it has been called—but also a virtual, globe-spanning minbar, the podium from which sermons in the mosque are delivered.¹ The internet provides jihadi support groups with a source of religious justification that characterizes and is required of all jihadi cells.² As a result, given that radicalization via online mentoring can move faster than mentoring in person, the use of the internet shortens the timeframe between the beginning of radicalization and the onset of terrorist activity.³

The internet gives ISIS a global recruiting presence and ability to keep communications secret

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” The American Interest, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

Online and OPSEC Savvy

The leadership of the Islamic State uses the internet, dedicated websites, and social media such as YouTube, Twitter, and Facebook to propagate its ideology, history, impressive recruitment record, and claims of battlefield success. It can do this because there is an audience. There are almost three million Facebook members in Iraq, more than one million in Syria; 10,000 Twitter users in Iraq, 8,000 in Syria. The Islamic State has more than 50,000 Twitter followers.⁴ Many of these consumers knew how to read al-Qaeda online, and now have transferred over to the “strong horse”, the radical organization that now leads the pack. Through social media the Islamic State leadership proclaims to the world explicitly that it is the successor to Osama bin Laden’s legacy and is fulfilling the original goal of establishing a caliphate.⁵

According to the cybersecurity company Zerofox, not only has the Islamic State built an online propaganda strategy using many social media networks; it also employs experts in marketing, public relations, and visual-content production with a sophistication far surpassing al-Qaeda.⁶ For example, ISIS activists will use a trending hashtag as a means of infiltrating conversations by adding that hashtag to one of their unrelated tweets. They also mass-tweet using their own designated hashtags, which gets them to trend. In addition, ISIS has created its own app, an Arabic-language Twitter app called “The Dawn of Glad Tidings” (or just “Dawn”). When users sign up, they give ISIS permission to send tweets through their own personal accounts. This allows ISIS tweets to reach hundreds or thousands more accounts, giving the perception that its

content is bigger and more popular than it is. The Dawn app is used as an education tool, distributing news and information about ISIS to its users.

ISIS also uses networks of computers it has infiltrated (“bots”) to carry out its campaigns via remote control, rendering the individuals behind the activities unidentifiable. Because these bot armies are so widespread and continually regenerate accounts, the group is always one step ahead of governments and social media networks attempting to thwart its maneuvers. ISIS also distributes propaganda specifically designed to target a Western audience, for instance by using hashtags they know the Western world is searching for—like #worldcup2014 #fifaworldcup—for the purposes of recruitment or inciting fear. In addition to promoting information about itself, ISIS also educates its social media followers on how to access information blocked by governments and social media sites through TOR/anonymizer tutorials.

Quite aside from their technical prowess, those who labor for the Islamic State also produce attractive and effective content. They produce high-quality video, which chronicles the group’s alleged historical success and records its violence, including executions, beheadings, and attacks, to intimidate opponents and the regimes it aspires to topple. It blends recent history, such as its supposed success against U.S. occupation forces in post-Ba’athi Iraq, with historical allusions to the great apocalyptic Sunni struggles against opponents of Islam, implying to would-be recruits that now is the time to join the great, successful Islamic State struggle. ISIS workers have also reportedly created recruitment propaganda using video game formats.

So much for the internet being an ineffective base of operations for offensive maneuvers. As for defense, the Islamic State leadership practices online operational security to stay anonymous and advises online readers on how to enhance their anonymity as well. It also uses temporary accounts, changes accounts periodically, and uses TOR to mask IPs, making the Islamic State’s communications largely dark, hard to track or target, and resilient.

The State’s self-proclaimed leader, Abu Bakr al-Baghdadi, and his followers have proven exceptionally difficult to track because they reportedly encrypt their communications and take steps to avoid being detected by enemy surveillance. Islamic State leaders also likely use FireChat, a commercially available service that permanently deletes messages sent via the internet, making them nearly impossible to intercept.⁷ Finally in this regard, Islamic State operators study Western media carefully, including the history of successful Western counterterrorism operations against al-Qaeda. They do this to learn how to protect their work and their masters from similar attacks in the future.

By maintaining multiple official and non-official accounts, Islamic State cyber-operators promote the ISIS brand and message, solicit funds, recruit followers, and maintain a crude organizational structure. Although such use is contrary to Twitter policy, the geometric propagation of messages via use of hashtags with links to advance perishable messages and images has allowed the Islamic State to maintain a resilient and disposable communications structure to connect with supporters even if accounts are subsequently shut down by Western or local internet service providers. Through decentralization, it has largely secured its communications from the traditional warfare techniques of jamming or interception. In a sense, it has crowd-sourced its communications.

The internet is vital to ISIS command and control

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” *The American Interest*, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

All Islamic State web media productions fall under the umbrella of Al-Furqan Media, while another media organization associated with ISIS, Fursan Al-Balagh Media, works on video transcriptions, giving viewers the chance to both read and watch all productions.⁸ And whether by accident or design, Islamic State operators have created a new form of operational command and control: C2 via app.

Thousands of Twitter followers have downloaded a Twitter app—the aforementioned Dawn of Glad Tidings—through which users give permission to receive Islamic State messages, images of military success, and video feeds, affording the Islamic State a Hollywood-quality feel.⁹ The application, flagged by Twitter as “potentially harmful”, requests user data and personal information.¹⁰ After downloading it, the app sends news and updates on ISIS operations in Syria and Iraq. Islamic State cadres include selected individuals who are expert at Adobe and video production. Each Islamic State region has its own dedicated social media accounts and supporters worldwide provide further channels through which to get its message to Western media.¹¹

In addition to official Islamic State social media accounts, hundreds of Islamic State sympathizers use private accounts to connect to thousands of internet followers. Islamic State media products are thus tweeted and then its hashtags re-tweeted by “private” supporters, enablers, and voyeurs, using the power of social media to project an image beyond its true capability, creating what is now-known as a “Twitter storm.”¹² Imagery, slogans, and would-be success stories are all crowd-sourced, allowing quality production to rise to the top through the power of social media. It is equivalent to allowing individual experts in Hollywood, Silicon Valley, and beyond to advance a positive image of America independently of any government oversight or direction.

Examples of these tactics illustrate the cleverness of ISIS media operations, which have propelled the Islamic State far beyond al-Qaeda-affiliated groups in the effectiveness of their information operations:

One Islamic State supporter tweeted during the 2014 World Cup, ‘This is our ball,’ along with a photo of a decapitated head and the #WorldCup hashtag, which ensured that it would pop up on news feeds on the World Cup.¹³

On July 4, 2014, Abu Bakr al-Baghdadi appeared unexpectedly on social media to give a sermon that was pre-posted via Twitter (before his video was uploaded onto YouTube) to guarantee its dissemination.¹⁴

A video series named ‘Mujatweets’ shows the life of Muslims in the Islamic State and testimonials from Western militants reporting their alleged commitment to the new Islamic State.¹⁵

The ISN (Islamic State News), a new, online Islamic State publication in English, provides news, information, and inspirational stories to readers worldwide (including, of course, the Western media).

Launched in May 2014, a new Islamic State media branch, Al-Hayat Media, distributes materials in several languages, including video with subtitles, as well as articles, news reports, and translated jihadi materials. Its main Twitter account is in German, but it also publishes in English and French, as well as Turkish, Dutch, Indonesian, and Russian. Al-Hayat Media's videos and materials are also distributed via Archive.org and other free web-hosting services; they are also regularly listed on justepaste.it, a web service for sharing free user-created contents, as well as on lesser-known social media such as Quitter and diaspora.¹⁶

On July 8, 2014, The ISR (Islamic State Report), also known as “An Insight Into the Islamic State”, which contains articles on Islamic State events, first began to release its showcase online magazine, Dabiq, consisting of detailed, well-written stories in fluent English. It resembles the well-known but cruder English-language magazine, Inspire, published by al-Qaeda in the Arabian Peninsula, famous for providing bombing-making instructions (in slightly broken English) to aspiring terrorists worldwide.¹⁷ Dabiq is named after the area Halab (Aleppo) in Sham (Syria), mentioned in the hadith as the place for Malahim (“Armageddon”)—an allusion to the site of a major 16th-century battle where the Ottomans defeated their enemies and established their first caliphate.¹⁸

In short, the Islamic State’s information operations are slick, de-centralized, and resilient, designed to withstand private-sector account cancellations for violations of terms of service. They have propelled the Islamic State to the forefront of terrorist information-operations success. Today, the Islamic State, al-Qaeda, and al-Qaeda affiliates use media services to upload pleas for readers to conduct local and worldwide terrorism, manuals on how to create improvised explosive devices, invitations to join the fight in the Middle East, and claims of success and ideological purity. Someday they may also disseminate cyber weapons via the web, should they acquire or devise them. The odds they will are high unless they are stopped beforehand.

OCOs solve

OCO's are key to stop ISIS

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” The American Interest, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

The Fifth Domain of Warfare, so called by the Department of Defense, is here, like it or not. Cyber attacks can amount in their significance to armed attacks, subject to international humanitarian law and the rules of war, according to the U.S. State Department’s Legal Advisor. What is unique about this domain is the fact that Islamist extremist activity on the web takes place every day. It is a war without timeouts or truces.

What is also unique about this domain is that the private sector more or less owns most of this infrastructure. The Islamic State exists in the cyber domain and specifically in social media. Unless we demand that social media companies cleanse themselves of violent extremist content, we will need to get used to the fact that our own counterterrorism cyber forces will be forced to fight in this media as well. Few of us want to go there, given the hornet’s nest of constitutional issues that will arise from it. But we may have no choice.

No counter-Islamic State strategy that ignores its use of the internet and social media will succeed. No military strategy or comprehensive whole-of-government approach can really be whole without addressing the Islamic State’s use of the internet. All warfare today includes the new Fifth Domain, and the sooner we recognize its importance to our adversaries, the sooner we will begin to address the threat seriously.

Interfering with the ISIS internet generates greater intelligence gathering and moderates extremism

Van de Velde, 15 - adjunct professor at the Johns Hopkins University, Georgetown University, and the National Intelligence University (James, “Crash Their Comms” The American Interest, <http://www.the-american-interest.com/2015/06/10/crash-their-comms/>

There are several other secondary, but important, aspects to contesting the extremist message on the internet. Interfering with extremist websites and social media stimulates communications and useful chatter (“hey, what’s going on?”) for intelligence collection. As suggested above, curtailing the aggregate number of extremist websites allows more moderate Muslim voices to be heard among the discussion groups and above the din of the militant ones. Contesting such websites forces extremist groups to expend valuable time, resources, infrastructure, and technical expertise to compete with these other sources. Challenging the al-Qaeda/Islamic State internet presence is not technically difficult for host nations, allies, and the United States. (We simply choose not to do so for political reasons or because of the myth that such actions would be futile.)

Intelligence Critical to National Security

Intelligence failure responsible for Pearl Harbor

Stuart **Taylor, April 29, 2014**, The Big Snoop: Life, Liberty, and the Pursuit of Terrorists, <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.)

Beginning in the second half of the 19th century, however, technological advances made it easier for the government to “search and seize” the contents of private communications without citizens’ knowledge, thus depriving them of the ability to object. **Wiretapping is almost as old as the telegraph, going back at least to the Civil War. Phone tapping has been an instrument of law enforcement and counterespionage since the beginning of the 20th century. An early instance of it was useful in probing the intentions of real and potential foreign enemies. In the first months of 1917, the British intercepted, decoded, and passed to Washington the “Zimmermann telegram”: a proposal from the Kaiser Wilhelm II’s foreign minister to the Mexican government promising that if Mexico allied itself with Germany in the event that the United States entered World War I on the side of the Allies, Germany would reward it with the return of formerly Mexican territory in Texas, New Mexico, and Arizona.** The revelation helped stoke support for Congress’s declaration of war that April.

However, once the war had ended, President Herbert Hoover’s secretary of state, Henry Stimson, famously shut down the “Black Chamber,” a precursor of the NSA, which had begun intercepting and decoding foreign diplomats’ cables in peacetime, too. “Gentlemen,” Stimson harrumphed, “don’t read each other’s mail.” Others in the U.S. government were not so naïve. **By the late thirties, Army and Navy intelligence officers, aided by civilian experts and technicians, were decoding diplomatic cables from Tokyo. By New Year’s Day 1941, they were picking up hints that Japan was preparing to attack the United States. But there was a failure of what today would be called “connecting the dots.” As a result, the nation’s leaders—including Stimson, who was then Franklin Roosevelt’s secretary of war—took no action to protect the Pacific Fleet.** Senator Feinstein, the daughter of an air raid warden in San Francisco, was 8 years old in December that year. Pearl Harbor, she feels, engendered her hawkish views on national security and intelligence. She remembers the blackout after the attack and a submarine net draped across the Golden Gate to prevent the Japanese from sneaking into San Francisco Bay.

Joel Brenner views that national trauma as a reminder that the nation’s most damaging intelligence scandals pertain not to over-zealousness, but to its opposite, “the failure to collect or understand critical information” in time to identify a threat and provide enough advance warning to prepare for it or, better yet, preempt it.

Intelligence necessary to protect against WMD proliferation and terrorism

Report and Recommendations of the President's Review Group on Intelligence, December 2013,
Liberty and Security in a Changing World, December 12,
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare. A robust foreign intelligence collection capability is essential if we are to protect ourselves against such threats. Because our adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

UNFETTERED INTELLIGENCE IS CRITICAL TO PREVENT TERRORISM

Ambassador L. Paul Bremer, National Commission on Terrorism Chair, 2000

["New Terrorist Threats and How to Counter Them," 7/31,
<http://www.heritage.org/Research/HomelandDefense/hl678.cfm>]

It is obvious that there is no substitute for good intelligence if you are going to have an effective counterterrorist policy. I have worked in and around government for 35 years now, and I have never seen a field in which intelligence is more central to good policy and intelligence is more difficult to get than in the field of terrorism. If you don't have good intelligence on terrorists, you simply don't have an effective counterterrorist policy and, most of all, you cannot prevent attacks. After all, the basic objective of counterterrorism is to stop the attacks before they happen.

INTELLIGENCE VITAL TO THWARTING TERRORISM

Fernando Reinares, Department of Politics and Sociology, Universidad Nacional de Education a Distancia, Madrid, War on Terrorism, ed. Alan O'Day, 2004, p. 226-7

Given the clandestine and unpredictable nature of terrorism, however, all these resources may not be effective unless they are accompanied by mechanisms for detecting and preventing future threats. Reliable intelligence is an essential tool. Experience shows that, as long as the other components function as they should, success in the state's counter-terrorism campaign is directly proportional to the emphasis placed on the gathering and analyzing of reliable information. On the contrary, when intelligence is insufficient or inadequate, the terrorist group may sense the window of opportunity they are being offered and will not hesitate to exploit this advantage by escalating its campaign of insurgent violence. In 1976, for reasons that have never been sufficiently clarified, the Italian Government decided to dismantle the special anti-terrorist

units it had created only a few years earlier and ordered far-reaching reorganization of its secret services. Terrorist attacks, which until then had been diminishing in frequency, immediately began to pick up and did not ease again until the early 1980s. Not coincidentally, by that time, revamped intelligence services put under greater supervisory control of the legislative and executive branches, had begun to produce results.

Intelligence Necessary to Prevent Genocide

Intelligence necessary to prevent human trafficking and mass atrocities

Report and Recommendations of the President's Review Group on Intelligence, December 2013,

Liberty and Security in a Changing World, December 12,

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Intelligence is designed not only to protect against threats but also to safeguard a wide range of national security and foreign policy interests, including counterintelligence, counteracting the international elements of organized crime, and preventing drug trafficking, human trafficking, and mass atrocities.

RFID Links

RFID technology defeats terrorism

Gene Kaprowski, August 13, 2014, UPI, "Wireless World: RFID to Thwart Terrorism,"

http://www.upi.com/Science_News/2004/08/13/Wireless-World-RFID-to-thwart-terrorism/88291092413872/ DOA: 5-1-15

An associate of Osama bin Laden crawls into a container -- along with some new luxury cars -- in a shipyard in Hamburg, Germany. **The goal -- shipping himself to the United States** and evading the Department of Homeland Security, with its high-tech officers on the ground at major airports, armed with databases of suspects' photos. **He is foiled**, however, **when a silent alarm is triggered, and an alert is sent to security over the airwaves, as he lifts the lid of the container in the warehouse. A wireless radio frequency identification or RFID security tag on the container sent the signal, silently, without alerting the intruder.** This scenario is one the government, major shippers and transportation companies are envisioning as possible for the near future. "The security of American ports continues to be a critical issue for homeland security," Robert Jackson, an attorney with Reed Smith LLP, located in the firm's Washington, D.C., office, told United Press International. **RFID technology**, long touted as in-store anti-theft devices for retailers, is evolving and now **is "the answer for homeland defense at our ports,"** Ben Quinones, a partner in the technology law practice of Pillsbury Winthrop in California's Silicon Valley, told UPI. The technology, developed by private sector research and development labs -- at companies like Avery Dennison, among others -- goes by several names, but one well-known product is called the "security strap," a spokesman for the company told UPI. Once goods are sealed inside a box, a longshoreman or another worker affixes the security strap. That enables shippers to track the cargo containers through their entire overseas trip. Tampering with the seal brings a security check. Companies like SAMSys are moving forward with second-generation RFID security technologies that may be even more effective. Sun Microsystems Inc. recently opened a test center in Dallas, giving customers a location to test an array of RFID scenarios, a spokesman told UPI. Even food and drug companies are eyeing the technology, fearful that rogues may tamper with or, worse yet, counterfeit the nation's pharmaceutical supplies. **The technology also is garnering funds at government research laboratories, as scientists are anxious to improve the state of the art for RFID.** Last month, the U.S. Department of Energy's Oak Ridge National Laboratory reached a development deal with Spectrum Signal Processing Inc. for a RFID platform, endorsed by the Pentagon, for an array of applications, a spokesman told UPI. RFID security technology currently comes in many forms, experts said. "Tags on containers, for rail cars, are fairly large and are active," John Parkinson, chief technologist, North American Region, with the consulting firm Capgemini in suburban Chicago, told UPI. "They contain a power source and can broadcast a signal that can be tracked by a satellite. Load the tag with a manifest of what's in the container, and you can track it as it moves along the global supply chain." Other kinds of tags operate passively but still are good for catching stowaways, Parkinson said. "Pass the tag through a broadcast RF (radio frequency) from a reader and the tag gets enough energy to squawk out a short code so it can be used to look up what's on the pallet or in the carton," he said. "If the passive tag IDs point to data that specifies size and weight, a quick calculation and weighbridge datum tells you if the container is full and over or under weight. Stowaways or added materials would show up." Some technology companies, like RAE Systems Inc. and a wireless semiconductor maker called Ember Corp., don't think RFID tags provide enough information or security. They believe wireless sensor technology will be more effective at monitoring shipping containers. Around Christmas last year, the companies demonstrated a prototype wireless security monitoring system, designed to help carriers of cargo comply with federal regulations seeking to prevent terrorists from smuggling nuclear weapons and other weapons of mass destruction into the United States. The Department of Homeland Security last Nov. 18 declared it wanted cargo companies that ship to American ports to equip their containers to prevent terrorist threats. The prototype technology developed by RAE Systems and Ember uses embedded RF chips and networking software to wrap cargo in a virtual Web network, which can detect weapons grade materials, as well as detail when containers have been opened. "It's easier to detect potential terrorists in American ports when we know what's happening inside the container at all times," RAE Systems Chief Executive Officer Robert Chen said in a statement. **More than 7 million**

shipping containers pass through U.S. ports each year, experts said. "The sheer volume of cargo entering our country every day makes it too easy for terrorists to smuggle dangerous cargo," Ember CEO Jeff Grammer said in a statement. The movement for wireless technology to track potential terrorist threats also is creating some consumer spin-offs, experts said. The Airport IT Trends Survey, sponsored by the airline information technology industry, reported **8 percent of responding airports already offer RFID tracking for passenger baggage. This is expected to increase to 25 percent of airports during the next two years. That could, one day, mean no more irretrievable luggage, lost forever in some cargo bin. Long-term, RFID also could speed up the process for importers to bring legitimate goods into the United States.** The Department of Homeland Security has started using RFID tags to identify freight-carrying trucks as they cross the border with Canada and, by the end of the year, the technology is expected to be deployed to other land entry points into the United States. Another use is RFID cards for those people who frequently cross the border into the U.S. Congress is eyeing these technology developments, especially now that the Pentagon and Homeland Security are pushing RFID projects, and views them as replacing less-effective video surveillance methods. "RFID chips are more powerful than today's video surveillance technology," said Sen. Patrick Leahy, D-Vt., during a conference this spring at the Georgetown University Law Center. "RFIDs are more reliable, they are 100 percent automatic, and they are likely to become pervasive, because they are significantly less expensive."

RFID technology provides security against terrorism

Laura Wiegler, 2014, June 20, RFID Insider, "Securing Entry: RFID is Making us Safer," DOA: 5-2-15

In 2001, the database the Department of Homeland Security (DHS) uses to check visa and passport applicants held about 7 million visa records and over 2 million passport records, according to the DHS. Further, they said that, "**If a visa applicant turned out to be a possible match for a terrorism-related CLASS record, the consular officer requested a Security Advisory Opinion (SAO) from the Visa Office in Washington. Such requests were sent via cables,** as were the Department's responses. This multi-step cable process to communicate with posts and to coordinate with other government agencies resulted in long wait times for both the consular officers and the applicants." A simpler, more efficient way **By 2005, though, those long wait times were going to change – at least in theory – as RFID was introduced to the average American passenger traveling internationally.** Today, the State Department issues both passport cards and passport books that are "smart" enough to read our information, the former at a distance and the latter at close range. The U.S. employs biometrics, which can be obtained through facial recognition, fingerprints, or the scanning of irises, but apparently requirements can vary. Michael Holly, Senior Advisor for International Affairs, Passport Services in the U.S. Department of State Bureau of Consular Affairs told **RFIDinsider** that "We use both fingerprints and facial recognition [for visas]. We've also studied the use of iris images." He did not elaborate further, but it's widely speculated that scanning iris images is not as reliable, and thus less popular, than scanning fingerprints and recognizing faces. **For passports, moreover, a digitized and readable photo is used, forgoing fingerprints on its contactless chip.** Insofar as the Government's rationale behind RFID's use, Holly claims the history far precedes 9-11, a common barometer for measuring the nation's security practices. Indeed, according to the U.S. Government, RFID has been used along the nation's land borders with Canada and Mexico since 1995. While Holly didn't spell this out, **the new passports have been designed to better protect the public from terrorism**, even though it's arguable whether or not they are also easing hassles at airports. Toward that end, there are bells and whistles attached to modern-day passports, and depending on whether one has the "card" or the "book", the technology differs. "What we provide to a U.S. traveling citizen bearing a passport card is a protective sleeve with that document," Holly says. "But with a passport we do a number of things – these are two different technologies: proximity and vicinity." He says with a passport card "vicinity technology" is employed; and a number of things are done to protect it "from the possibility of skimming data from the chip, and eavesdropping. We use anti-attenuation tape, a skimming sleeve that blocks the possibility of someone trying to skim data from the chip if the book is closed," he says. The borders agent can thus obtain information discreetly, and in real time, according to Holly. "They're [the passport issuers] using PKI (public key infrastructure) and in association with the RFID chip we can ...confirm data that appears on the passport's data page and [which one] can authenticate using the digital signatures," he says. Obviously, in

an era when a plane can go missing for weeks or months, and two passengers can board with stolen passports, security at least worldwide is hardly foolproof. Nevertheless, Holly believes that over about the past decade, the American traveler's experience is far more secure than it was in the halcyon days of early air travel. "We use a security protocol known as the "basic access control" that requires, in order for the chip to communicate with a reader, that [the passport owner's] book must be open, that the machine-readable zone be read." He says this "zone" is two lines of OCR code at bottom of the passport page, and from which "a number of pins are derived, and then once that happens, the chip will communicate with the reader, releasing the data on the chip." In the case of passport books, the readers are at the customs booths for use upon entry to the foreign country. But in the case of cards, which he explains are commonly used when U.S. citizens travel by car from the northernmost and southernmost parts of the country, the data is read from a greater distance. (See article on toll booth RFID use.) Both [the card type and book type] are passports but the book uses RFID proximity technology, he explains. "The chip in the passport book is a microprocessor. It stores data on it. ...The passport card does not store any data. It **simply points** [via a recognized serial number] to a record stored in a secure database." The Netherlands-based Gemalto, a global digital security firm, has been working with the U.S. Government for several years on rolling out RFID for use on or with passports. Gemalto says on its website that in August of 2012, the Government Printing Office (GPO) awarded the company with a second consecutive five-year contract. "Gemalto first partnered with [the] GPO in 2006 following stringent evaluations to meet agency requirements," the company says on its site

Borders Links

Border surveillance is k2 preventing terrorism

Smarick et al. 12 ,(Kathleen Smarick and Gary D. LaFree of the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland. 11/12 “Border Crossings and Terrorist Attacks in the United States: Lessons for Protecting against Dangerous Entrants” START,

http://www.start.umd.edu/sites/default/files/files/publications/START_BorderCrossingsTerroristAttacks.pdf CCC)

An essential step in this project was determining the frequency and dynamics of border crossings by individuals who conducted or who wanted to conduct terrorism-related activities in the United States. Towards that goal, the project built upon the existing holdings of the American Terrorism Study (ATS) in this effort. The ATS, housed at the University of Arkansas, catalogs and systematically codes information on more than 300 Federal court cases involving Federal terrorist charges since 1980 and, following a review of other possible resources, proved to be the most useful starting point for compiling open-source, quantitative data on terrorist border crossings. Since 1989, the American Terrorism Study (ATS) has received lists of court cases and associated indictees that resulted from an official FBI terrorism investigation spanning 1980 through 2004. Housed at the University of Arkansas' Terrorism Research Center in Fulbright College (TRC), the ATS now includes almost 400 cases from the FBI lists. Of these, approximately 75% of cases have complete court documentation, and almost all of those collected have been coded into the ATS database, while the ATS team continues to track new cases by collecting, reviewing, and coding new and additional court documentation. The ATS includes terrorism incidents and attacks, thwarted or planned terrorism incidents sometimes referred to as preventions, material support cases for terrorism, general terrorism conspiracies, and in some cases, immigration fraud; the common denominator among all ATS events is that the FBI investigated these events as terrorism-related incidents. During preliminary research for this project, court records from 378 terrorism cases found in the ATS dataset were reviewed for information on potential border crossing events related to terrorism cases. The documents for each court case were manually reviewed by researchers to determine whether the collected records reported that one of the defendants or accomplices in a case crossed a U.S. border at some point. Thirty-eight percent of the reviewed cases—145 cases—from 1980 through 2004 were found to either have: • direct mention of a border crossing in the court documents, or • a link to a terrorism incident that involved a known border crossing, either before or after an incident. After compiling this list of court cases for inclusion, each identified court case was then linked to a criminal incident involving terrorism charges. Initial reviews revealed a connection to a border-crossing event in a total of 58 successful terrorist attacks, 51 prevented or thwarted attacks, 26 material support cases, 33 immigration fraud incidents, and 4 general terrorism conspiracies. Additional reviews of relevant information on indictees and their activities resulted in a reduction

in the number of successful terrorist attacks associated with these individuals to a total of 43. Appendix 2 provides more details on the data collection process and how a reliable collection methodology was established to create the U.S. Terrorist Border Crossing Dataset (USTBC), using the ATS as a starting point. National Consortium for the Study of Terrorism and Responses to Terrorism A Department of Homeland Security Science and Technology Center of Excellence Border Crossings and Terrorist Attacks in the United States 12 Systematic evaluation by the research team revealed that the American Terrorism Study is a reliable and useful resource for identifying individuals associated with terrorist attacks or terrorist criminal cases (such as conspiracies) and for determining which of these individuals crossed U.S. borders in advance of or in the wake of their terrorism-related behavior. This is largely because the ATS is based on court documents, which among sources of data on terrorism are the most likely to reference relevant border crossing activity. The Global Terrorism Database, which is based primarily on media sources, can serve a supporting role in this research, but the ATS is the primary source allowing for construction of a new, relational database on U.S. Terrorist Border Crossings (USTBCs). That being said, it is important to recognize that the ATS is not a perfect data source. As noted above, its contents are limited to individuals and information related to court cases in which one or more defendant was charged with Federal terrorism charges. As such, the contents of ATS clearly represent a subset of all terrorists or attempted terrorists in the United States, as it systematically omits those who: • were never arrested or faced any charges, • were charged with offenses not directly related to terrorism, • were charged at the non-Federal level, or • were engaged in dangerous activity that does not meet the FBI's definition of a terrorism case. Throughout this project, the research team was careful to respect the limitations of this data collection and to draw conclusions that recognize that the border crossing events included in this project likely represent a non-representative subset of all border crossing attempts by terrorists or intended terrorists. Despite these limitations, though, the data that was built upon the baseline of ATS provides important insights into the nexus between border crossings and terrorism. The U.S. Terrorism Border Crossing Dataset The final versions of the codebooks used to develop the U.S. Terrorist Border Crossing (USTBC) data collection are presented in Appendix 3. Based upon knowledge gained from pilot efforts (as discussed above and in Appendix 2), the project resulted in two codebooks—one focused on dynamics of a bordercrossing event involving someone associated with a Federal terrorism court case, and another focused on the characteristics of the individuals associated with Federal charges who were involved in the bordercrossing event. Data collection for the USTBC lasted for approximately one year and was primarily conducted by research assistants at the Terrorism Research Center at the University of Arkansas.³ The resultant data that comprise the USTBC are available in Appendix 4. Table 4 provides a snapshot summary of these data, which include detailed information on the location of an attempted crossing, the timing of a crossing relative to attempted or actual terrorist activity, the origin or destination of an attempted crossing, and more. The data also include specific information on border crossers, including their citizenship status, their criminal history, and key demographics (including level of education, marital status, etc.) Appendix 5 provides descriptive statistics from the border-crossing and border-crosser data. 3 Special thanks to Kim Murray and Summer Jackson of the Terrorism Research Center for their efforts in combing through the courtcase material and assembling these data for the USTBC. National Consortium for the Study of Terrorism and Responses to Terrorism A Department of Homeland Security Science and Technology Center of Excellence Border Crossings and Terrorist Attacks in the United States 13 Border Crossings Identified in USTBC Attempts to Enter the United States Of the 221 border crossings identified in this project as involving individuals who were indicted by the U.S. government in terrorism-related cases, the

majority (129 crossings) involved an individual attempting to enter the United States, while the remainder (92 crossings) involved an individual attempting to exit the United States. Eighty-seven percent of the attempted border crossings were successful, rather than being thwarted by law enforcement or foiled by some other events or developments. Additional discussion on the nature of successful crossings versus those who were apprehended at the border is presented below.

Among those attempts to enter the United States, the most frequent origin for these crossing efforts was Canada.⁴ But, as Figure 2 illustrates, such attempted entries originated from all corners of the world.

US Border Patrol proves that surveillance is key to anti-terror efforts

Stamey 14 (Barcley; DOMESTIC AERIAL SURVEILLANCE AND HOMELAND SECURITY: SHOULD AMERICANS FEAR THE EYE IN THE SKY; March 2014)

The leading national agency currently using drones to combat a wide range of domestic threats is U.S. Customs and Border Protection. With its fleet of seven MQ-1 Predators and three MQ-1 Guardians—Predators modified for marine surveillance—CBP 26 is at the forefront of large-scale drone operations. With an annual budget exceeding \$11 billion, CBP is well equipped for protecting our national security while combating potential terrorist threats.⁵⁵ But how efficiently are those funds being used, and what is meant by effectiveness? According to Merriam-Webster, effectiveness is “producing a decided, decisive, or desired effect or result.”⁵⁶ Ultimately, that desired result is safe international borders. Accomplishing this result involves the apprehension of illegal immigrants, interdiction of illicit drugs, and prevention of terrorist infiltration, which CBP does quite well, but with respect to UAS, effectiveness must be viewed on a much broader scale. This section takes into account the size of CBP, its operational budget, and couples it with published results. According to CBP, the primary mission of drone use is “anti-terrorism by helping to identify and intercept potential terrorists and illegal cross-border activity.”⁵⁷ CBP uses its Predators and Reapers to accomplish this goal through human detection and tracking, surface asset coordination, and threat detection through IR sensors in multiple scenarios. Previously mentioned sensor suites allow the Predator to detect movement along the border, identify actual personnel numbers, and track the location of threats all while being unobserved to the individuals on the ground. With their long loiter times, Predators allow officials to monitor gaps along the border while maximizing the efforts of ground personnel in actual interdiction missions. After witnessing the functionality of actual Predator operations in Afghanistan, this author realizes the value in having high definition video sensors overhead during dangerous operations. This type of technology certainly has a place in homeland security missions, and future capabilities will provide a clear advantage to U.S. personnel in combating border security. This force multiplier mindset is one CBP has adopted and publicizes regularly to justify the success of its drone program. Long loiter times, remote area access, and flexibility during National Special Security Events are common claims.

Unmanned Ariel Vehicles fill current surveillance gap on the border

Haddal 10 (CC; Homeland Security: Unmanned Arial Vehicles and Border Surveillance CRS Report RS21698. Washington, DC: Library of Congress, Congressional Research Service, July 8, 2010.)

One potential benefit of UAVs is that they could fill a gap in current border surveillance by improving coverage along remote sections of the U.S. borders. Electro-Optical (EO) sensors (cameras) can identify an object the size of a milk carton from an altitude of 60,000 feet.14 UAVs also can provide precise and real-time imagery to a ground control operator, who would then disseminate that information so that informed decisions regarding the deployment of border patrol agents can be made quickly. Additionally, the Predator B used along the southern border can fly for more than 30 hours without having to refuel, compared with a helicopter's average flight time of just over 2 hours. The ability of UAVs to loiter for prolonged periods of time has important operational advantages over manned aircraft. The longer flight times of UAVs means that sustained coverage over a previously exposed area may improve border security. The range of UAVs is a significant asset when compared to border agents on patrol or stationary surveillance equipment. If an illegal border entrant attempts to transit through dense woods or mountainous terrain, UAVs would have a greater chance of tracking the violator with thermal detection sensors than the stationary video equipment which is often used on the borders. It is important to note, however, that rough terrain and dense foliage can degrade the images produced by a UAV's sensory equipment and thus limit their effectiveness at the borders. Nevertheless, the extended range and endurance of UAVs may lessen the burdens on human resources at the Homeland Security: Unmanned Aerial Vehicles and Border Surveillance Congressional Research Service 4 borders. Also, UAV accidents do not risk the lives of pilots, as do the helicopters that currently patrol U.S. borders

Border security stops terrorism

Zuckerman, Bucci, Carafano, no date

(Jessica Zuckerman, Steven P. Bucci, Ph.D. Director, Douglas and Sarah Allison Center for Foreign and National Security Policyj and James Jay Carafano, Ph.D. Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and the E. W. Richardson Fellow, 13, 7-22-2013, "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," Heritage Foundation,

<http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism> CCC)

Chiheb Esseghaier and Raed Jaser—April 2013. **Chiheb Esseghaier and Raed Jaser were arrested in April 2013 for attempting to carry out an attack on a Via Railway train travelling from Canada to the U.S.** The attack, authorities claimed, was supported by an al-Qaeda element in Iran, although there is currently no evidence that it was state-sponsored.[205] The exact route of the targeted train has not been identified, and Iranian authorities vehemently deny that al-Qaeda is operating within Iranian borders.

Esseghaier and Jaser have been charged in Canada with conspiracy to commit murder for the benefit of a terrorist group, participating in a terrorist group, and conspiring to interfere with transportation facilities for the benefit of a terrorist group. Esseghaier has also been charged with

participating in a terrorist group, and both men face up to life in prison.[206] The two men are awaiting trial. Chiheb Esseghaier wants to represent himself, basing his defense on the Quran instead of on the Canadian criminal code, which has caused delays in the proceedings.[207]

Continued use of border surveillance technology is crucial to the detection of and response to threats on the border

Haddal, Specialist in Immigration Policy, 8/11/10 (Chad C. Haddal, Congressional Research Service report, August 11, 2010, “Border Security: The Role of the U.S. Border Patrol” <https://www.fas.org/sgp/crs/homesec/RL32562.pdf>, accessed 7/15/15 JH @ DDI)

Perhaps the most important technology used by the Border Patrol are the surveillance assets currently in place at the border. The program has gone through several iterations and name changes. Originally known as the Integrated Surveillance Information System (ISIS), the program’s name was changed to the America’s Shield Initiative (ASI) in FY2005. DHS subsequently folded ASI into the Secure Border Initiative (SBI) and renamed the program SBInet Technology (SBInet). Once it is beyond the pilot phase, SBInet will, according to DHS, develop and install “new integrated technology solutions to provide enhanced detection, tracking, response, and situational awareness capabilities.”¹⁹ The other program under SBI is the SBI Tactical Infrastructure program, which, according to DHS, “develops and installs physical components designed to consistently slow, delay, and be an obstacle to illegal cross-border activity.”²⁰ In the late 1990s, the Border Patrol began deploying a network of Remote Video Surveillance (RVS) systems (i.e., camera systems), underground sensors, and the Integrated Computer Assisted Detection (ICAD) database into a multi-faceted network designed to detect illegal entries in a wide range of climate conditions. This Integrated Surveillance Intelligence System (ISIS) attempted to ensure seamless coverage of the border by combining the feeds from multiple color, thermal, and infrared cameras mounted on different structures into one remote-controlled system with information generated by sensors (including seismic, magnetic, and thermal detectors). When a sensor is tripped, an alarm is sent to a central communications control room at a USBP station or sector headquarters. USBP personnel monitoring the control room screens use the ICAD system to re-position RVS cameras towards the location where the sensor alarm was tripped (although some camera positions are fixed and cannot be panned). Control room personnel then alert field agents to the intrusion and coordinate the response.

Information gathered from surveillance activities is key to any effective response to terrorist threats along the border

Fisher, U.S. Customs and Border Protection Office of Border Patrol Chief, 5/8/12 (Michael, Department of Homeland Security, “Written testimony of U.S. Customs and Border Protection Office of Border Patrol Chief Michael Fisher for a House Committee on Homeland Security, Subcommittee on Border and Maritime Security hearing titled “Measuring Border Security: U.S. Border Patrol’s New Strategic Plan and the Path Forward.””)

<http://www.dhs.gov/news/2012/05/08/written-testimony-us-customs-and-border-protection-house-homeland-security>; accessed 7/15/15 JH@ DDI)

Information gathered from reconnaissance, community engagement, sign-cutting and technology together provide situational awareness and intelligence and helps us to best understand and assess the threats we face along our borders. Information and intelligence will empower Border Patrol leadership and front line agents to get ahead of the threat, be predictive and proactive. Integration denotes CBP corporate planning and execution of border security operations, while leveraging partnerships with other federal, state, local, tribal, and international organizations. Integration of effort with these organizations will ensure we bring all available capabilities and tools to bear in addressing threats. Lastly, through rapid response, we will deploy capabilities efficiently and effectively to meet and mitigate the risks we confront. Put simply, rapid response means the Border Patrol and its partners can quickly and appropriately respond to changing threats. Goal 1: Secure America’s Borders The 2012 Strategic Plan has two interrelated and interdependent goals. In the first goal, the Border Patrol will work with its federal, state, local, tribal, and international partners to secure America’s borders using information, integration and rapid response in a risk-based manner. There are five objectives within this goal: Prevent Terrorists and

Terrorist Weapons from Entering the United States Manage Risk Disrupt and Degrade Transnational Criminal Organizations (TCOs) Whole-of-Government Approach Increase Community Engagement I. Prevent Terrorists and Terrorist Weapons from Entering the United States The current risk environment is characterized by constantly evolving threats that are both complex and varying, and the Border Patrol must strategically apply intelligence to ensure that operations are focused and targeted against the greatest threats. The Border Patrol's ability to prevent and disrupt such threats is enhanced through increased information sharing and operational integration, planning, and execution with our domestic and foreign law enforcement partners. Integration with our federal, state, local, tribal, and international partners' intelligence and enforcement capabilities into the planning and execution of CBP operations is critical to our ability to secure our nation's borders.

The use of necessary surveillance technology is key to the identification and prevention of terrorist threats on the border

Office of Border Patrol, September 2004 (THE OFFICE OF BORDER PATROL AND THE OFFICE OF POLICY AND PLANNING, US CUSTOMS & BORDER PROTECTION, "National Border Patrol Strategy"

http://www.au.af.mil/au/awc/awcgate/dhs/national_bp_strategy.pdf, accessed 7/15/15 JH @ DDI)

The Border Patrol currently uses a mix of agents, information, and technology to control the border. The Border Patrol's ability to establish situational awareness, monitor, detect, respond to, and identify potential terrorists, instruments of terrorism, and criminals relies heavily on interdiction and deterrence-based technology. Having the necessary technology to support the Border Patrol priority and traditional missions cannot be overstated. In the future, there must be continued assessment, development, and deployment of the appropriate mix of personnel, technology, and information to gain, maintain, and expand coverage of the border and ensure that resources are deployed in a cost-effective, efficient fashion. Technology which enhances operational awareness and effectiveness includes camera systems for day/ night/infrared work, biometric systems such as IDENT/IAFIS, processing systems like ENFORCE, sensoring platforms, large-scale gamma X-rays, and aerial platforms, and other systems. Technologies requiring modernization include wireless and tactical communications and computer processing capabilities. Coordination between Border Patrol and inspectional personnel at the ports of entry ensures the most efficient use of trained personnel and technology. In the future, the Border Patrol will take advantage of the targeting and selectivity tools made available in the Automated Commercial Environment (ACE) and the National Targeting Center. The continued testing, evaluation, acquisition, and deployment of appropriate border enforcement technologies will be pursued vigorously so that the maximum force-multiplier effect is achieved in support of both the priority and traditional missions.

Any gap in security on the border allows international terror groups to come into the United States

Wilson 15 [Reid Wilson, 2/26/15, covers national politics for the Washington Post, "Texas officials warn of immigrants with terrorist ties crossing southern border," Washington Post, <http://www.washingtonpost.com/blogs/govbeat/wp/2015/02/26/texas-officials-warn-of-immigrants-with-terrorist-ties-crossing-southern-border/jf>]

A top Texas law enforcement agency says border security organizations have apprehended several members of known Islamist terrorist organizations crossing the southern border in recent years, and while a surge of officers to the border has slowed the flow of drugs and undocumented immigrants, it's costing the state tens of millions of dollars. In a report to Texas elected officials, the state Department of Public Safety says border security agencies

have arrested several Somali immigrants crossing the southern border who are known members of al-Shabab, the terrorist group that launched a deadly attack on the Westgate shopping mall in Nairobi, Kenya, and Al-Itihad al-Islamiya, another Somalia-based group once funded by Osama bin Laden. **Another undocumented immigrant arrested crossing the border was on multiple U.S. terrorism watch lists**, the report says. According to the report, **one member of al-Shabab, apprehended in June 2014**, told authorities he **had been trained for an April 2014 suicide attack in Mogadishu**. He said he escaped and reported the planned attack to African Union troops, who were able to stop the attack. The FBI believed another undocumented immigrant was an al-Shabab member who helped smuggle several potentially dangerous terrorists into the U.S. Authorities also apprehended immigrants who said they were members of terrorist organizations in Sri Lanka and Bangladesh. The Department of Public Safety said the report, first published by the Houston Chronicle, was not meant for public distribution. “[T]hat report was inappropriately obtained and [the Chronicle was] not authorized to possess or post the law enforcement sensitive document,” department press secretary Tom Vinger said in an e-mail. U.S. Customs and Border Protection did not respond to requests for comment. **The department said it had come into contact in recent years with “special interest aliens,” who come from countries with known ties to terrorists or where terrorist groups thrive.** Those arrested include Afghans, Iranians, Iraqis, Syrians, Libyans and Pakistanis. In all, immigrants from 35 countries in Asia and the Middle East have been arrested over the past few years in the Rio Grande Valley. The department says there is no known intelligence that specifically links undocumented immigrants to terrorism plots, but the authors warn it’s almost certain that foreign terrorist organizations know of the porous border between the U.S. and Mexico. **“It is important to note that an unsecure border is a vulnerability that can be exploited by criminals of all kinds,”** Vinger said. **“And it would be naive to rule out the possibility that any criminal organizations around the world, including terrorists, would not look for opportunities to take advantage of security gaps along our country’s international border.”**

Maximized surveillance on the border is key to stopping terrorism

Willis et al 10 [Henry H. Willis, 2010, director of the RAND Homeland Security and Defense Center, with Joel B. Predd, Paul K. Davis and Wayne P. Brown, RAND.org,

“Measuring the Effectiveness of Border Security Between Ports-of-Entry”,
http://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR837.pdf, jf]

One of the unexpected results of our study was recognition of the importance of networked intelligence in elaborating objectives for and measuring effectiveness of border security.¹¹ This came about for many reasons. First, all of the focus missions are best understood in national terms: **Border security contributes significantly to several high-level national objectives**, but results depend sensitively on interactions with and the performance of other federal and local agencies, as well as economic and demographic conditions outside of DHS’s control. Second, **national-level effectiveness depends not just on individual component or agency effectiveness but also on components’ ability to share information** and work collaboratively, i.e., to network. **This is perhaps most obvious with respect to preventing terrorism, in that individuals might enter the country who are vaguely suspicious but who cannot reasonably be arrested at the border.** Responsibility for follow-up then transfers to, e.g., the Federal Bureau of Investigation (FBI). However, **the FBI’s ability to follow up**—either immediately or when further information emerges—**might depend critically on information collected** and effectively transferred **by border agencies** to the FBI. The word “effectively” is key because all agencies are deluged with data. The 9/11 Commission’s report dramatized the consequences of ineffectiveness: It is not that information for apprehending the perpetrators did not exist, but rather that the dots were not connected and the relevant agencies did not cooperate well (National Commission on Terrorist Attacks upon the United States, 2004). Third, national-level law enforcement also depends on the effectiveness of the justice

system, including the ability to convict and punish. That, in turn, often depends on authorities being able to construct an extensive, fact-based story of criminal behavior from which, cumulatively, guilt can reasonably be inferred by a jury. Fourth, the **nature and quality of information collected by border-security components, the consistency with which it is collected**, and the effectiveness with which the data are both transferred to national databases and—where appropriate—highlighted in cross-agency actions, are leverage points for improved national-level effectiveness, especially in relation to terrorism- or drug-related functions. Border-security efforts sometimes will query detected travelers against data sets of known or suspected terrorists or criminals. This is especially relevant at ports of entry, ports of egress in some modes, and in cases in which border enforcement detains an illegal crosser. In other settings, **border-enforcement agencies collect as much information as possible on individuals, their conveyances, license plates, accounts, and other records of persons detained for crossing illegally but for whom no prior records exist**. The same is true in the maritime regions when individuals are arrested for illegal drug smuggling or illegal migrant smuggling. **The collected information can become future tactical intelligence** (and used in prosecutions) **if the detained person becomes involved in criminal or terrorist functions at a later date**. Discussions with component agencies indicate that this is an important capability to measure. Technologically, **it is even possible to tag individuals so that subsequent surveillance within the United States** (or another country) is possible.¹²

Border surveillance prevents terrorist groups from attempting attacks

Willis et al 10 [Henry H. Willis, 2010, director of the RAND Homeland Security and Defense Center, with Joel B. Predd, Paul K. Davis and Wayne P. Brown, RAND.org,
“Measuring the Effectiveness of Border Security Between Ports-of-Entry”,
http://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR837.pdf, pg 19, jf]

The principal contributions that **border security** makes to counterterrorism relate to **preventing** certain kinds of **terrorist attacks dependent on flows into the country** of people or materials. These contributions can be illustrated by considering what opportunities exist to disrupt terrorist attacks while they are being planned and orchestrated. Through a number of planning efforts, **DHS and its components have developed detailed planning scenarios of terrorist events** (DHS, 2006). **Each of these scenarios has been deconstructed into attack trees that are useful for considering how DHS border-security programs contribute to terrorism security efforts**. In their most generic form, these attack trees specify dimensions of attack scenarios with respect to building the terrorist team, identifying a target, and acquiring a weapon (see Figure 4.1). This decomposition of attack planning provides a structure around which to consider how interdiction, deterrence, and networked intelligence contribute to preventing terrorist attacks and, thus, why it is relevant to measure these functions. **DHS border-security efforts focus on interdiction of terrorist team members and weapons or weapon components when they cross U.S. borders**. Examples of initiatives that are intended to enhance these capabilities include the Secure Border Initiative, the acquisition of Advanced Spectroscopic Portals for nuclear detection, the Secure Communities Initiative, and US-VISIT. In addition, it is often pointed out that, **when border-security measures are perceived to be effective, terrorist groups may be deterred from attacking in particular ways, or possibly from attacking at all**. This could

result from awareness of what type of surveillance is occurring or the capability of interdiction systems. In either case, **deterrence refers to the judgment of terrorists that they will not be successful**, leading them to choose another course of action. Finally, many **border-security initiatives also contribute information to the national networked-intelligence picture**. For example, the Secure Communities Initiative has implemented new capabilities to allow a single submission of fingerprints as part of the normal criminal arrest and booking process to be queried against both the FBI and DHS immigration and terrorism databases. This effort makes it easier for federal and local law enforcement to share actionable intelligence and makes it more difficult for terrorists to evade border-security efforts.

Prisons

Current prisons k2 stopping terrorism

Kaplan 09 (Fred Kaplan 9, 5-29-2009, "There are already 355 terrorists in American prisons," Slate Magazine, http://www.slate.com/articles/news_and_politics/war_stories/2009/05/there_are_already_355_terrorists_in_amERICAN_prisons.html CCC)

President Obama's remark that some Guantanamo detainees might be transferred to American prisons has prompted an extraordinary, and intellectually feeble, storm of protest. Former Vice President Dick Cheney kicked off the campaign when he said, during his May 21 speech at the American Enterprise Institute, that "to bring the worst terrorists inside the United States would be a cause for great danger and regret in the years to come." Sitting lawmakers—especially those from states such as Kansas and Colorado where federal prisons are based—raised the same specter and shouted the ancient cry of principled rebellion: "Not In My Back Yard!" It makes one wonder: Do any of these legislators know who's in their backyards already, with no apparent detriment to their constituents' daily lives, much less the nation's security? According to data

provided by Traci L. Billingsley, spokeswoman for the U.S. Bureau of Prisons, federal facilities on American soil currently house 216 international terrorists and 139 domestic terrorists. Some of these miscreants have been locked up here since the early 1990s. None of them has escaped. At the most secure prisons, nobody has ever escaped, period.

As recited in Congress and on cable-news talk shows, the fears of moving Gitmo prisoners here seem to be these: that the terrorist prisoners might escape (statistics to the contrary be damned), that they might convert their fellow inmates with jihadist propaganda, that other members of al-Qaida might infiltrate the surrounding communities (to do what—spring them?), or that their presence might sow panic in those communities. Maybe these people don't understand what life is like in these "supermax" prisons. Take ADX Florence, the supermax in Colorado—"the Alcatraz of the Rockies"—that serves as the home to Omar Abdel-Rahman, the "blind sheikh" who organized the 1993 World Trade Center bombing; Zacarias Moussaoui, one of the Sept. 11 plotters; Richard Reid, the shoe-bomber; Theodore Kaczynski, the "Unabomber"; and Terry Nichols, who helped plan the Oklahoma City bombing, to name a few. These are all truly dangerous people, but it's not as if they run into one another in the lunch line or the yard. There is no lunch line; there is no yard. Most of the prisoners are kept in solitary confinement for 23 hours a day. For one hour, they're taken to another concrete room, indoors, to exercise, by themselves. Their only windows face the sky, so they have no way of knowing even where they are within the prison. Phone calls to the outside world are banned. Finally, the prison is crammed with cameras and motion detectors. Compartments are separated by 1,400 remote-controlled steel doors; the place is surrounded by 12-foot-high razor-wire fences; the area between the wire and the walls is further secured by laser beams and attack dogs. The Bureau of Prisons operates similar facilities—also full of terrorists and murderers—in Terre Haute, Ind.; Marion, Ill.; and elsewhere. And the Defense Department operates a few dozen military prisons scattered around the country, some of which would be suitable for housing the exiles from Guantanamo.

FISA links

Prohibiting NSA data collection under FISA prevents extensive analysis if data, k2 prevent terrorism

Bradbury 15 (Steven. G, "BALANCING PRIVACY AND SECURITY", HARVARD JOURNAL OF LAW AND PUBLIC POLICY, https://scholar.google.com/scholar?as_ylo=2011&q=FISA+approvals&hl=en&as_sdt=0,5)

Responding to public opposition to the NSA's telephone metadata program, Congress is currently considering legislation[¶] that would prohibit the collection of bulk metadata under[¶] FISA. In my view, such a restriction is a bad idea. Under this[¶] legislation, the NSA would be unable to collect data from multiple[¶] companies where necessary to assemble a single, efficiently[¶] searchable database.³¹ This restriction would also mean that[¶] the NSA would be prevented from collecting and storing data[¶] in bulk where doing so is the only way to preserve important[¶] business records that may be useful for a counterterrorism investigation.³² Without the ability for U.S. intelligence agencies[¶] to acquire the data in bulk under FISA, these important business[¶] records would only exist for as long as the private companies[¶] happen to retain the data for their own business purposes[¶] or as required by regulatory agencies for reasons unrelated to national security.³³ For example, telephone companies typically[¶] retain their metadata calling records for only 18 months, as specified by the Federal Communications Commission for purposes of resolving customer billing disputes.³⁴ Under its[¶] metadata program, on the other hand, the NSA was storing the[¶] data for five years, so that it could conduct more extensive historical[¶] analyses of calling connections involving suspected terrorist[¶] numbers—historical analyses that can often provide very[¶] important new leads for FBI investigations.

FISA is an archaic mechanism that doesn't allow law enforcement to respond to modern threats, Status quo allows for sufficient NSA capabilities

CFR 13 (Council on Foreign Relations, "U.S. Domestic Surveillance" CFR, <http://www.cfr.org/intelligence/us-domestic-surveillance/p9763>)

After 9/11, the Bush administration opted not to seek approval from the FISC before intercepting "international communications into and out of the United States of persons linked to al-Qaeda (PDF) or related terrorist organizations." The special secret court, set up in 1978 following previous administrations' domestic spying abuses, was designed to act as a neutral overseer in granting government agencies surveillance authorization.[¶] After the NSA program was revealed by the New York Times in late 2005, former attorney general Alberto R. Gonzales argued (PDF) that President Bush had the legal authority under the constitution and congressional statute to conduct warrantless surveillance on U.S. persons "reasonably believed to be linked to al-Qaeda." The 2001 Authorization for Use of Military Force (AUMF), without specifically mentioning wiretapping, grants the president broad authority to use all necessary force "against those nations, organizations, or persons he determines planned, authorized, committed, or aided the [9/11] terrorist attacks." This includes, administration officials say, the powers to secretly gather domestic intelligence on al-Qaeda and associated groups.[¶] The Bush administration maintained that the Foreign Intelligence Surveillance Act (FISA) was an outdated law-enforcement mechanism that was too time-consuming given the highly fluid, modern threat environment.

Administration officials portrayed the NSA program as an "early warning system" (PDF) with "a military nature that requires speed and agility." Moreover, the White House stressed that the program was one not of domestic surveillance but of monitoring terrorists abroad, and publicly referred to the operation as the "Terrorist Surveillance Program." Opponents of the program referred to it as "domestic spying."¹ Under congressional pressure, Gonzales announced in January 2007 plans to disband the warrantless surveillance program and cede oversight to FISC, but questions about the legality of the program lingered in Congress and Gonzales resigned months later.¹ But Washington's vow to seek FISA approval for domestic surveillance was short-lived. In July 2007--weeks before Gonzales stepped down--intelligence officials pressed lawmakers for emergency legislation to broaden their wiretapping authority following a ruling by the court overseeing FISA that impacted the government's ability to intercept foreign communications passing through telecommunications "switches" on U.S. soil.

Financial Surveillance Links

Financial surveillance is key to stopping terrorist organizations

Atlas 15 [Terry Atlas, 2-6-2015, Senior Writer in Foreign Policy/National Security Team for Bloomberg News, "Follow the money new game plan in thwarting terrorism," Seattle Times, <http://www.seattletimes.com/news/follow-the-money-new-game-plan-in-thwarting-terrorism/>]

Economic and financial intelligence is critical to targeting and enforcing sanctions against Iran, North Korea and Russia; **strangling the flow of money to terrorist organizations**, drug cartels and weapons traffickers; **tracking nuclear proliferation**; and assessing the strength of nations such as Russia and China that are now part of the global economy. Treasury personnel in Washington, D.C. — and in Afghanistan, Pakistan and the Persian Gulf — have worked with **intelligence** and military colleagues to **attack the finances of the Taliban, al-Qaida and other terrorist groups**. The department has provided expertise and actionable intelligence to civilian and military leaders through “threat finance cells” for Afghanistan and Iraq, and worked elsewhere with the U.S. Special Operations Command. How much the intelligence mission has changed is highlighted by the move this month by David Cohen, the Treasury undersecretary for terrorism and financial intelligence to become deputy director of the Central Intelligence Agency. Cohen, 51, whose Treasury responsibilities included sanctions policy, replaces Avril Haines, a lawyer who’s now President Obama’s deputy national security adviser. It’s the first time a Treasury official has moved into such a senior CIA post. That has been noticed in the intelligence community, where the Treasury has become a recognized power, and among the specialized legal and financial community affected by the nation’s increasing use of economic coercion against adversaries. **“Financial intelligence is incredibly important, and it’s much more important than it used to be,”** said attorney Christopher Swift, a former Treasury official who investigated financing of terrorist groups and weapons proliferators. “Cohen’s move to CIA underscores that.” **Financial intelligence has come into its own as the U.S. increasingly turns to sanctions, asset freezes and other financial actions to thwart adversaries from al-Qaida** operatives to Russian President Vladimir Putin. It’s a tactic that Ian Bremmer, the president of New York-based Eurasia Group, recently called the “weaponization of finance.” The U.S. strategy is “premised on the simple reality that all of our adversaries, to one degree or another, need money to operate, and that by cutting off their financial lifelines, we can significantly impair their ability to function,” Cohen said at a conference in London in June. **Financial intelligence exposes vulnerabilities of adversaries** — whether nations or individuals — who need access to the global financial system. **Concealing financial flows can be harder than avoiding surveillance of emails and phone calls, which terrorists have tried to do in the aftermath of Edward Snowden’s disclosures about U.S. communications**

intercepts. “When people think about intelligence, they think about James Bond and running operations against the Russians or the Chinese, and that still goes on and we shouldn’t diminish the importance of it,” said Swift, an adjunct professor of national security studies at Georgetown University in Washington, D.C. “But if you’re looking at the other types of organizations in the global community that are causing problems for the United States and its allies, a lot of them are non-state actors, they’re criminal syndicates, they’re narcotics syndicates, they’re transnational terrorist syndicates, and **the best way to figure out how those organizations work, who’s part of those organizations, and the best way to degrade those organizations is follow the money,**” he said. The U.S. government has vastly expanded its collection and use of financial intelligence, bolstered by a series of post-9/11 laws and executive orders that have given the Treasury Department a leading role in financial intelligence and sanctions. The Treasury Department has more than 700 personnel dealing with terrorist and financial intelligence. The Treasury’s **Terrorist Finance Tracking Program**, which has access to the Swift international banking transaction network, **participated in investigations into the 2013 Boston Marathon bombing, threats to the 2012 London Summer Olympic Games and the 2011 plot to assassinate the Saudi Arabian ambassador in D.C.**, which U.S. officials said originated with senior members of the Quds force of Iran’s Islamic Revolutionary Guards Corps. The Financial Crimes Enforcement Network, a part of the Treasury’s intelligence operation that regulates the financial industry to prevent money laundering and terrorist financing, receives **more than a million reports a year on potentially suspect cash movements from financial institutions**, Cohen said in a speech in January. FinCen’s information, combined with data from other sources, **assists investigators in “connecting the dots” involving sometimes previously unknown individuals and businesses**, according to the Treasury.

Links specific to Phone Meta-Data

Phone Meta-Data key to check attacks on the homeland.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

6. One of the greatest challenges the U.S. faces in combating international terrorism and preventing potentially catastrophic terroristic attacks on our country is identifying terrorist operatives and networks, particularly those operating within the U.S. Detecting and preventing threats by exploiting terrorist communications has been, and continues to be, one of the tools in this effort. It is imperative that we have the capability to rapidly detect any terrorist threat inside the U.S. 7. One method that the NSA has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the U.S. The term "telephony metadata" or "metadata" as used here refers to data collected under the program that are about telephone calls—such as the initiating and receiving telephone numbers, and the time and duration of the calls—but does not include the substantive content of those calls or any subscriber identifying information. 8. By analyzing telephony metadata based on telephone numbers associated with terrorist activity, trained expert intelligence analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the U.S. 9. Foreign terrorist organizations use the international telephone system to communicate with one another between numerous countries all over the world, including calls to and from the U.S. When they are located inside the U.S., terrorist operatives also make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the U.S., or those that are purely domestic, because those communications are particularly likely to identify suspects in the U.S. whose activities may include planning attacks against the homeland.

Meta-data vital to check terror attacks - 9-11 proves.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984

as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

10. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting such communications between known or suspected terrorists who are operating outside of the U.S. and who are communicating with others inside the U.S., as well as communications between operatives who are located within the U.S. 11. Detecting and linking these types of communications was identified as a critical intelligence gap in the aftermath of the September 11, 2001 attacks. One striking example of this gap is that, prior to those attacks, the NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using overseas signals intelligence capabilities, but those capabilities did not capture the calling party's telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysis mistakenly concluded that al-Mihdhar was overseas and not in California. Telephony metadata of the type acquired under this program, however, would have included the missing information and might have permitted NSA intelligence analysts to tip FBI to the fact that al-Mihdhar was calling the Yemeni safe house from a U.S. telephone identifier. 12. The utility of analyzing telephony metadata as an intelligence tool has long been recognized. As discussed below, experience also shows that telephony metadata analysis in fact produces information pertinent to FBI counterterrorism investigations, and can contribute to the prevention of terrorist attacks.

() Yes, Meta-data has checked specific terror attacks. It also exposes broader terror cells.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

55. **The value of telephony metadata** collected under Section 215 **is not hypothetical**. While many specific instances of the Government's use of telephony metadata under Section 215 remain classified, a number of instances have been disclosed in declassified materials. 56. **An illustration** of the particular value of the bulk metadata program under Section 215—and a tragic example of what can occur in its absence—is the case of 9/11 hijacker Khalid al-Mihdhar, which I have described above. The Section 215 telephony **metadata** collection program **addresses the information gap that existed at the time of the al-Mihdhar case**. It allows the NSA to rapidly and effectively note these types of suspicious contacts and, when appropriate, to tip them to the FBI for follow-on analysis or action. 57. Furthermore, once an identifier has been detected, **the NSA can use** bulk telephony **metadata along with other data** sources **to quickly identify the larger network** and possible coconspirators both inside and outside the U.S. for further investigation by the FBI with the goal of preventing future terrorist attacks.

Meta-data key – their “alternatives” would hamper the counter-terror ops of several agencies, not just NSA.

Shea ‘14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director’s Fellow. Since her tour as a Director’s Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda’s Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with “I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge”. Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

58. As the case examples in the FBI declaration accompanying this declaration demonstrate, Section 215 bulk telephony metadata is a resource not only in isolation, but also for investigating threat leads obtained from other SIGINT collection or partner agencies. This is especially true for the NSA-FBI partnership. The Section 215 telephony **metadata** program **enables** NSA intelligence **analysts to evaluate** potential **threats that it receives** from or reports to the FBI **in a more complete manner than if this data source were unavailable**. 59. Section 215 bulk telephony **metadata complements** other counterterrorism-related collection **sources by serving as a significant enabler for** NSA intelligence **analysis**. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 **metadata can help** the NSA **prioritize** for content **analysis** communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis **so that the U.S. Government gains the best possible understanding of** terrorist target **actions and intentions**. 60. **Reliance solely on traditional case-by-case intelligence gathering methods, restricted to known terrorist identifiers, would significantly impair** the NSA's ability to accomplish many of the aforementioned **objectives**. 61. **Without the ability to obtain** and analyze bulk **metadata**, the NSA **would lose a tool for detecting communication chains** that link to identifiers associated with known and suspected terrorist operatives, **which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts** both within the U.S. and abroad. Having the bulk telephony metadata available to query is part of this effort, as there is no way to know in advance which numbers will be responsive to the authorized queries. 62. The bulk metadata allows retrospective analyses of prior communications of

newly discovered terrorists in an efficacious manner. Any other means that might be used to attempt to conduct similar analyses would require multiple, time-consuming steps that would frustrate needed rapid analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis. 63. If the telephony metadata are not aggregated and retained for a sufficient period of time, it will not be possible for the NSA to detect chains of communications that cross different providers and telecommunications networks. But for the NSA's metadata collection, the NSA would need to seek telephonic records from multiple providers whenever a need to inquire arose, and each such provider may not maintain records in a format that is subject to a standardized query. 64. Thus, the Government could not achieve the aforementioned benefits of Section 215 metadata collection through alternative means. 65. The use of more targeted means of collection—whether through subpoenas, national security letters ("NSLs"), or pen-register and trap-and-trace ("PR/TT") devices authorized under the FISA—solely of records directly pertaining to a terrorism subject would fail to permit the comprehensive and retrospective analyses detailed above of communication chains that might, and sometimes do, reveal previously unknown persons of interest in terrorism investigations. Targeted inquiries also would fail to capture communications chains and overlaps that can be of investigatory significance, because targeted inquiries would eliminate the NSA's ability to collect and analyze metadata of communications occurring at the second "hop" from a terrorist suspect's initial "seed"; rather, they would only reveal communications directly involving the specific targets in question. In other words, targeted inquiries would capture only one "hop." As a result, the Government's ability to discover and analyze communications metadata revealing the fact that as-yet unknown identifiers are linked in a chain of communications with identified terrorist networks would be impaired. 66. In sum, any order immediately barring the Government from employing the Section 215 metadata collection program would deprive the Government of unique capabilities that could not be completely replicated by other means, and as a result would cause an increased risk to national security and the safety of the American public.

Phone Meta-data key to boost terror detection.

Shea '14

At the time of this testimony, Teresa Shea was the director of signals intelligence, or SIGINT, which involves intercepting and decoding electronic communications via phones, email, chat, Skype, and radio. Ms. Shea graduated from the Georgia Institute of Technology with a Bachelor of Science degree in Electrical Engineering. She earned her Master of Science Degree in Electrical Engineering from Johns Hopkins University. Ms. Shea is a graduate of the National Security Studies Leadership Program at the Maxwell School, Syracuse University. She also attended the Intelligence Community Program at the Kellogg School of Management. Ms. Shea joined the NSA workforce in 1984 as an Electrical Engineer where she developed technical solutions to SIGINT requirements. Since then she has served as project engineer, program manager, technical director, and line manager in the Signals Intelligence Directorate and its predecessor organizations. Ms. Shea participated in the NSA Graduate Fellowship Program and was selected to be a Director's Fellow. Since her tour as a Director's Fellow, Ms. Shea has served in multiple management positions. Ms. Shea was the Chief of Tailored Access Operations group within the Data Acquisition organization in the Signals Intelligence Directorate. Amicus Brief for Smith v. Obama – before The US District Court for THE DISTRICT OF IDAHO – December 20th – This cite is a bit tricky to find – it was submitted within the addendum section of Acting Assistant Attorney General Branda's Amicus Brief in the matter of Smith v. Obama – *before the United States Ninth Circuit Court of Appeals*. Her testimony concludes with "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge". Jan 23rd - It is towards the bottom of a lengthy addendum section – <https://www.eff.org/document/governments-smith-answering-brief>

47. Among other benefits, the bulk collection of telephony metadata under Section 215 has an important value to NSA intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland, in support of FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks both in the U.S. and abroad. By applying the FISC-ordered RAS standard to telephone identifiers used to query the metadata, NSA intelligence analysts are able to: (i) detect domestic identifiers calling foreign identifiers associated with one of the foreign terrorist organizations and discover identifiers that the foreign identifiers are in contact with; (ii) detect foreign identifiers associated with a foreign terrorist organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers; and (iii) detect possible terrorist-related communications occurring between communicants located inside the U.S. 48. Although the NSA possesses a number of sources of information that can each be used to provide separate and independent indications of potential terrorist activity against the U.S. and its interests abroad, the best analysis occurs when NSA intelligence analysts can consider the information obtained from each of those sources

together to compile and disseminate to the FBI **as complete a picture as possible** of a potential terrorist **threat**. While telephony **metadata** is not the sole source of information available to NSA counterterrorism personnel, it **provides a component of the information** NSA intelligence **analysts rely upon to execute** this **threat identification** and characterization role.

Restrictions on FBI/CIA Cooperation

FBI/CIA cooperation is critical to continued CT

Dinshaw 6-13-15, Reporter

Fram, “Animosity between CIA and FBI before 9/11 debilitated spies: newly declassified documents”, <http://www.nationalobserver.com/2015/06/13/news/animosity-between-cia-and-fbi-911-debilitated-spies-newly-declassified-documents>

According to a trove of documents declassified by the CIA on June 12, al-Qa’ida’s operational activity in the United States and Canada was greater than previously thought leading up to the 9/11 attacks on the World Trade Center and the Pentagon, with Tenet’s leadership blamed for much bad judgement. The CIA report details how tension between the CIA and FBI hindered counter-terrorism investigations, and how intelligence agencies repeatedly failed to put future 9/11 hijackers on a watch list. It describes an often-vicious conflict between George Tenet’s CIA and the FBI before 9/11, as well as the spy agency’s difficulties in gathering Human Intelligence (HUMINT) and mounting a covert strike to capture or kill bin Laden, after his organization bombed US embassies in East Africa and attacked the USS Cole in 2000. “The key pre-9/11 CIA-FBI relationship with respect to al-Qa’ida, that between UBL (Usama Bin Laden) station and the FBI’s New York Field Office (the Bureau’s office of origin or office with responsibility for al-Qa’ida), was troubled at best and dysfunctional at worst,” states the documents. One CIA member told the investigating team that an FBI representative from the Bureau’s New York Field Office was there to spy on behalf of his chief, who did not trust the UBL station. The FBI representative, in turn, told investigators that he was mistrusted as New York’s ‘spy’ and felt like an outcast, saying: “...many of his supervisors and peers did, in fact, characterize him that way.” Many of those interviewed said that the worst animosity occurred in a crucial period between 1997 and 1999, after which attempts were made to mend fences, with little success. The report notes that the CIA’s UBL station had a smoother relationship with FBI Headquarters’ counter-terrorism office, but those interviewed said that supposedly monthly meetings were erratic at best. Nonetheless, the UBL station and FBI counter-terrorism heads established a good working relationship. Lack of cooperation despite stepping up effort to investigate bin Laden. But on Dec. 24 1998, then-CIA chief George Tenet called in a memo for “a new phase in our effort against bin Ladin,” urging that efforts against al-Qa’ida’s chief be stepped up dramatically. “We need an integrated plan which captures these elements and others which may be appropriate. This plan must be fully co-ordinated with the FBI,” said Tenet in his memo. But co-operation between the CIA and other agencies remained inadequate. On at least three occasions from January 2000 – August 2001, agencies “failed to recommend future 9/11 hijackers Nawaf al-Hazmi and Khalid al-Mihdhar for watchlisting.” “...the Director of Central Intelligence (DCI) acknowledged in his testimony that [the] CIA was not sufficiently focused on advising the State Department to watchlist all terrorist operatives, attributing this to uneven practices, bad training, and a lack of redundancy,” the report states.

FBI and CIA cross-agency cooperation is essential

Jackson et al ’9, American lawyer and the Chief United States district judge on the United States District Court for the Middle District of Louisiana

Brian Anthony, "The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency",
https://books.google.com/books?id=1MYQCCfuv4QC&dq=%22domestic+surveillance%22+%22interagency+cooperation%22&source=gbs_navlinks_s

As time has passed, the cast of agencies involved in domestic intelligence activities has grown, and therefore, coordination among these agencies has grown increasingly complicated. The events of 9/11 highlighted interagency-coordination problems, and once again, calls for reorganization arose. "The establishment of the Department of Homeland Security promises to further complicate both the delineation of responsibilities and coordination across agencies. The coordination of domestic intelligence activities is particularly complex because such activities overlap with the responsibilities of so many agencies. The military and CIA have gradually been restricted to foreign intelligence activities, while the FBI has taken on the primary role in domestic intelligence activities. However, there must be coordination and information exchange among these agencies because threats have become increasingly transnational in nature. In addition to these historical interagency-coordination problems, the events of 9/11 also led to increasing calls to separate law enforcement and intelligence activities. Since the late 1950s, the FBI increasingly took on surveillance activities until the Church Committee reforms in the 1970s put additional oversight and accountability mechanisms in place. With the events of 9/11, the FBI has once again been asked to take on increased surveillance responsibilities, and some have questioned whether law enforcement and intelligence activities can be conflated in a single organization because of the risk that such activities will come into conflict with one another. Thus, domestic surveillance efforts in the United States have historically been extremely complex because they require coordination across various government agencies, coordination across international and domestic activities, and melding of various organizational cultures. The nation has always struggled with the delineation of responsibilities across agencies and how to streamline the domestic intelligence enterprise. "The calls for reorganization since the 9/11 attacks are merely the latest episode in a cyclical reevaluation of the organizational structure of the country's domestic surveillance activities.

Interagency cooperation is crucial to domestic intelligence

Rosenbach and Peritz '9, Executive Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School and Associate at the Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government

Eric and Aki, "Confrontation or Collaboration? Congress and the Intelligence Community",
<http://belfercenter.ksg.harvard.edu/files/IC-book-finalasof12JUNE.pdf>

Domestic Intelligence. Unlike many nations, the United States does not have a dedicated organization focused on domestic intelligence collection. Although the Federal Bureau of Investigation (FBI) is the principal domestic intelligence agency, the Central Intelligence Agency (CIA) and Department of Defense (DoD) also play limited domestic intelligence roles. In response to criticism following the attacks of 9/11, the FBI began reforms to increase their collection and analysis of domestic intelligence, especially in regards to terrorism. Nonetheless, critics contend that FBI intelligence collection continues to play a secondary role to the FBI's primary mission, federal law enforcement. This memo provides new members of Congress with an overview of U.S. domestic intelligence and the issues most relevant to the 111th Congress. Domestic Intelligence before September 11, 2001. Since its creation in 1908, the FBI has been

responsible for both domestic intelligence and law enforcement. From the 1930s through 1960s, the FBI focused on cases of espionage and foreign subversion. The Church Committee investigation of intelligence abuses in the 1970s disclosed a series of FBI—along with CIA and NSA—violations of Americans' civil liberties. Congress passed a series of reform laws in the late 1970s, including the Foreign Intelligence Surveillance Act (FISA), to prevent future abuses. In the wake of the intelligence scandals of the 1970s, concern about the potential for intelligence agencies to inappropriately collect information that could be used to prosecute citizens prevailed. This concern eventually morphed into a mistaken belief that intelligence officials could not legally share information with FBI criminal investigators. The resulting “wall” of bureaucratic obstacles virtually halted the flow of intelligence information provided to domestic law enforcement agencies. The 9/11 Commission highlighted this shortcoming as a major impediment to national security. Post-9/11 Domestic Intelligence Paradigm: The attacks of 9/11 resulted in major organizational and functional changes within the Intelligence Community and dramatically shifted FBI priorities from traditional criminal matters to international counterterrorism threats and intelligence gathering. After much debate, the 9/11 Commission recommended against creating a dedicated domestic intelligence agency, and instead recommended that the FBI expand and improve its intelligence. The Belfer Center for Science and International Affairs | The Harvard Kennedy School 45 capabilities. In order to improve its domestic intelligence capacity, the FBI pursued the following initiatives: Joint Terrorism Task Forces (JTTFs): The JTTFs are multi-agency task forces located in more than 100 locations nationwide. JTTFs bring local, state, and federal law enforcement and intelligence agencies together to share information and conduct operations to prevent terrorist operations. Prior to September 11, 2001, the United States had 35 JTTFs. Shortly after the attacks, the FBI Director instructed all FBI field offices to establish formal terrorism task forces. Personnel: The FBI hired hundreds of counterterrorism analysts and linguists, and re-tasked more than 700 personnel from criminal investigations to counterterrorism and counterintelligence duties. National Security Branch: The Bureau merged its intelligence, counterintelligence, and counterterrorism divisions into a unified “National Security Service” in 2005. Field Intelligence Groups (FIGs): FIGs are composed of Special Agents, Intelligence Analysts, and other FBI specialists in each of the FBI's 56 field offices. They are designed to integrate the “intelligence cycle” into FBI field operations and manage the Field Office Intelligence Program in coordination with the Directorate of Intelligence at FBI Headquarters. Domain Management Initiative: In November 2005, the FBI launched the Domain Management Initiative to focus attention on national security threats within each field office's “geographic domain.” The goal of program is to develop a comprehensive understanding of the threats relevant to each field office's region.

Link Boosters: vs Critical Terrorism Affs

Their critique of islamophobia undercuts the effectiveness and resolve of the fight against terrorism – this risks large-scale violence

Hanson '4

(Victor Davis, Professor of Classical Studies at CSU Fresno, City Journal, Spring, http://www.city-journal.org/html/14_2_the_fruits.html)

Rather than springing from realpolitik, sloth, or fear of oil cutoffs, much of our appeasement of Middle Eastern terrorists derived from a new sort of anti-Americanism that thrived in the growing therapeutic society of the 1980s and 1990s. Though the abrupt collapse of communism was a dilemma for the Left, it opened as many doors as it shut. To be sure, after the fall of the Berlin Wall, few Marxists could argue for a state-controlled economy or mouth the old romance about a workers' paradise—not with scenes of East German families crammed into smoking clunkers lumbering over potholed roads, like American pioneers of old on their way west. But if the creed of the socialist republics was impossible to take seriously in either economic or political terms, such a collapse of doctrinaire statism did not discredit the gospel of forced egalitarianism and resentment against prosperous capitalists. Far from it. If Marx receded from economics departments, his spirit reemerged among our intelligentsia in the novel guises of post-structuralism, new historicism, multiculturalism, and all the other dogmas whose fundamental tenet was that white male capitalists had systematically oppressed women, minorities, and Third World people in countless insidious ways. The font of that collective oppression, both at home and abroad, was the rich, corporate, Republican, and white United States. The fall of the Soviet Union enhanced these newer post-colonial and liberation fields of study by immunizing their promulgators from charges of fellow-traveling or being dupes of Russian expansionism. Communism's demise likewise freed these trendy ideologies from having to offer some wooden, unworkable Marxist alternative to the West; thus they could happily remain entirely critical, sarcastic, and cynical without any obligation to suggest something better, as witness the nihilist signs at recent protest marches proclaiming: "I Love Iraq, Bomb Texas." From writers like Arundhati Roy and Michel Foucault (who anointed Khomeini "a kind of mystic saint" who would usher in a new "political spirituality" that would "transfigure" the world) and from old standbys like Frantz Fanon and Jean-Paul Sartre ("to shoot down a European is to kill two birds with one stone, to destroy an oppressor and the man he oppresses at the same time"), there filtered down a vague notion that the United States and the West in general were responsible for Third World misery in ways that transcended the dull old class struggle. Endemic racism and the legacy of colonialism, the oppressive multinational corporation and the humiliation and erosion of indigenous culture brought on by globalization and a smug, self-important cultural condescension—all this and more explained poverty and despair, whether in Damascus, Teheran, or Beirut. There was victim status for everybody, from gender, race, and class at home to colonialism, imperialism, and hegemony abroad. Anyone could play in these "area studies" that cobbled together the barrio, the West Bank, and the "freedom fighter" into some sloppy global union of the oppressed—a far hipper enterprise than rehashing Das Kapital or listening to a six-hour harangue from Fidel. Of course, pampered Western intellectuals since Diderot have always dreamed up a "noble savage" who lived in harmony with nature precisely because of his distance from the corruption of Western civilization. But now this fuzzy romanticism had an updated, political edge: the bearded killer and wild-eyed savage were not merely better than we because they lived apart in a pre-modern landscape. No: they had a right to strike back and kill modernizing Westerners who had intruded into and disrupted their better world—whether Jews on Temple Mount, women in Westernized dress in Teheran, Christian missionaries in Kabul, capitalist profiteers in Islamabad, whiskey-drinking oilmen in Riyadh, or miniskirted tourists in Cairo. An Ayatollah Khomeini who turned back the clock on female emancipation in Iran, who murdered non-Muslims, and who refashioned Iranian state policy to hunt down, torture, and kill liberals nevertheless seemed to liberal Western eyes as preferable to the Shah—a Western-supported anti-communist, after all, who was engaged in the messy, often corrupt task of bringing Iran from the tenth to the twentieth century, down the arduous, dangerous path that, as in Taiwan or South Korea, might eventually lead to a consensual, capitalist society like our own. Yet in the new world of utopian multiculturalism and knee-jerk anti-Americanism, in which a Noam Chomsky could proclaim Khomeini's gulag to be "independent nationalism," reasoned argument was futile. Indeed, how could critical debate arise for those "committed to social change," when no universal standards were to be applied to those outside the West? Thanks to the doctrine of cultural relativism, "oppressed" peoples either could not be judged by our biased and "constructed" values ("false universals," in Edward Said's infamous term) or were seen as more pristine than ourselves, uncorrupted by the evils of Western capitalism. Who were we to gainsay Khomeini's butchery and oppression? We had no way of understanding the nuances of his new liberationist and "nationalist" Islam. Now back in the hands of

indigenous peoples, Iran might offer the world an alternate path, a different “discourse” about how to organize a society that emphasized native values (of some sort) over mere profit. So at precisely the time of these increasingly frequent terrorist attacks, the silly gospel of multiculturalism insisted that Westerners have neither earned the right to censure others, nor do they possess the intellectual tools to make judgments about the relative value of different cultures. And if the initial wave of multiculturalist relativism among the elites—coupled with the age-old romantic forbearance for Third World rogues—explained tolerance for early unpunished attacks on Americans, its spread to our popular culture only encouraged more. This nonjudgmentalism—essentially a form of nihilism—deemed everything from Sudanese female circumcision to honor killings on the West Bank merely “different” rather than odious. Anyone who has taught freshmen at a state university can sense the fuzzy thinking of our undergraduates: most come to us prepped in high schools not to make “value judgments” about “other” peoples who are often “victims” of American “oppression.” Thus, before female-hating psychopath Mohamed Atta piloted a jet into the World Trade Center, neither Western intellectuals nor their students would have taken him to task for what he said or condemned him as hypocritical for his parasitical existence on Western society. Instead, without logic but with plenty of romance, they would more likely have excused him as a victim of globalization or of the biases of American foreign policy. They would have deconstructed Atta’s promotion of anti-Semitic, misogynist, Western-hating thought, as well as his conspiracies with Third World criminals, as anything but a danger and a pathology to be remedied by deportation or incarceration.

There isn’t a root cause of terrorism – and if there is, trying to find it just allows violence to flourish. We must win the fight first and figure out what caused it later

ElShtain ‘7

(Jean Bethke Elshtain is the Laura Spelman Rockefeller Professor of Social and Political Ethics at the University of Chicago, The Price Of Peace: Just War in the Twenty-First Century, Edited by Charles Reed and David Ryall)

Of course it is sometimes the case that elements of movements that resort to terrorism – say, the Irish Republican Army – also develop a political arm and begin negotiating a political settlement. No political solution is possible, however, when the destruction of innocent civilians and some fantastic notion, say, of restoration of the classical caliphate, as in bin Ladenism, is the alleged aim. Thus, bin Laden, in fatwa after fatwa, calls upon the faithful to kill ‘crusaders, Jews and infidels’ wherever and whenever they are found. He disdains any distinction between Americans in uniform and those going about daily civilian life. His claim is that to kill all Americans anywhere is a ‘duty for every Muslim’ . . . God willing, America’s end is near.’6 Terrorism is terrorism Before turning to the context of ethical evaluation and restraint within which just war thinkers insist terrorism and measures used to combat it should be located, it is important to examine some apologies for terrorism, that remove the onus of moral criticism and condemnation from those committed to terrorist deeds. For there are some who insist now, as they have in the past, that the victims of terror somehow ‘had it coming’. Others claim that those who resort to terror have no other option as they are in a state of ‘rage’ as well as helplessness so they must use whatever weapons they can. Then, too, there is the ‘everybody does it’ claim. These lines of thought strip away a moral vocabulary of the sort required to make crucial distinctions between rule-governed war making and terrorism. One often finds rationales for terrorist acts that, in the rush to exculpate, wind up patronising those who resort to terrorism. As theologian David Yeago writes: To suppose that the Islamic faith, or Arab culture, or poverty and the experience of oppression somehow lead young men directly, of themselves, to be capable of flying an airliner full of passengers into a building crowded with unsuspecting civilians is deeply denigrating to Muslims, to Arabs, and to the poor and oppressed. It requires us to suppose that Muslims, or Arabs, or the poor lie almost beyond the borders of a shared humanity, that however much we pity and excuse them, we cannot rely on them simply because they are Muslims, Arabs, or oppressed to behave in humanly and morally intelligible ways. I would suggest that

this is a dangerous line of thought, however humanely motivated it may initially be.⁷ This is a powerful – and controversial – argument and it warrants some unpacking. Often arguments that take the form of ‘they have no other option’ are working with crude binary models of victim/victimiser or oppressor/ oppressed. If the victimising is absolute on one side of the pair, it follows that victimisation is absolute. If this is so, then victims will and must resort to anything they can to undo their ‘oppression’. The origins of such an approach conceptually most likely lie with Hegel’s famous (or infamous) master/slave dialogue. More recently, this argument is associating with a text that was a staple in third worldist ideological circles, namely, Franz Fanon’s *The Wretched of the Earth*.⁸ Unsurprisingly, these sorts of arguments have resurfaced with Islamist fanaticism and terrorism. But no one has thus far made a convincing case that ‘structural’ causes lie behind a resort to terrorism – like poverty and desperation. It is, therefore, clear that we must look at terrorism not as epiphenomenal to some underlying problem but as itself the problem. Poverty does not breed terrorism. The vast majority of the poor never resort to terrorism. The attackers of 9/11 were middle class and reasonably well educated. Alan Krueger and Jitka Maleckova have explored in depth the relationship, if any, between economic deprivation and terrorism. They conclude that a ‘careful review of the evidence provides little reason for optimism that a reduction in poverty or an increase in educational attainment would, by themselves, meaningfully reduce international terrorism’. The issue is important, they aver, because drawing a false causal connection between poverty and terrorism is potentially quite dangerous. We may be led to do nothing about terrorism, and we may also lose interest in providing support for developing nations should the terrorism threat wane. By ‘falsely connecting terrorism to poverty’, policy-makers, analysts and commentators only ‘deflect attention from the real roots of terrorism’, which are political, ideological and religious.⁹ There is a huge gap between claiming that poverty ‘causes’ terrorism and acknowledging the ways in which terrorist entities exploit various conditions, including desperation of all sorts. The key lies in the word ‘exploit’. Terrorists exploit certain conditions. These conditions are part of the matrix out of which terrorism grows. It does not follow that terrorism is caused by these conditions. Because terrorists exploit certain conditions, it makes good sense for those who are victimised by terrorism to seek to ameliorate the conditions out of which terrorism may flow. But this gets very tricky very fast, not only for the reasons noted above, but because a good bit of al-Qaeda terrorism of the sort that stunned the United States and Great Britain is the act of those who became ideologically inflamed actors within the very bosom of the society they seek to destroy. In light of the enormous varieties of circumstances that may yield up terrorists, those combating terrorism must in their response, first and foremost, concentrate on terrorism itself. Confronted with a serial killer, the first thing police seek to do is to stop the violence. Attempting to discern what particular concatenation of circumstances led to this particular person taking up serial killing comes later. Urgency is added to this effort if one recognises that there are always unscrupulous political leaders who are only too happy to exploit the very conditions that make terrorist recruitment easier. To alter the circumstances is to alter their own fortunes, to the extent that they have profited from the misery of their own people. Acknowledging this in no way removes responsibility from the shoulders of others, but what it does do is to alert us to a kind of sacralisation of victimhood that invites exculpation when the ‘victim’ commits abhorrent acts. This is itself a patronising gesture that traffics in the most demeaning sorts of cultural stereotypes.

Their lack of resolve is defeatism: causes the US to use nuclear force against terrorists – which is obviously worse than the quo

Peters ‘5

(Ralph, fmr US Army intel officer, prizewinning writer and strategist, *New Glory*, 72-75)

We all hope that we shall never have to use a nuclear weapon. But faced with implacable enemies determined to destroy us, inadequate conventional measures increase the likelihood that we will eventually need to resort to weapons of mass destruction ourselves. The use of such weapons seems unthinkable today, but sufficient destruction wreaked against our homeland could bring about a rapid change of heart. We value our sense of humanity, but we, too, will do whatever it takes to survive. In world of nuclear proliferation—which neither of our political parties, nor our closest allies, have demonstrated the strength of will to stop—the chance that we will live out our lives without witnessing at least a regional nuclear exchange is far lower than any one of us might like. Weapons of mass destruction are ideal for enemies intent upon mass destruction. At least some of our current and future enemies—Islamist fanatics—seek nothing less than the elimination of our country and the destruction of civilization. They do not, and will not, have the strength to achieve their goal, but they are likely to gain the capability

to inflict losses on our society and economy far more painful than those of 9/11. If we lack the fortitude to do whatever it takes to win we may be certain that our enemies do not share our reticence. Despite the terrible dangers of the Cold War, the truth is that American and its allies have lived through a golden age of safety. That age is now at an end. Despite our best efforts to secure our homeland, we live in an age of vulnerability unprecedented since our frontier days. And the only enduring means to reduce that vulnerability isn't frisking Grandma at the airport. We must carry the struggle relentlessly to our enemies, as we have done with broad success since 9/11. We can win the War on Terror. Or any other war. But only if we are willing to fight for a long time to come. The losers in the War on Terror will be those who first despair. Our fanatical enemies cannot defeat us. But we can defeat ourselves through a failure of will. The nonsense that "victory isn't possible today" is an absurdity foisted upon us by academics and pundits. Victory is always possible. If we're willing to pay the price. And if we are not we should not engage in military adventures that only worsen the plight of a broken world. To do great good with the military you often must begin by doing great harm to the enemies of the good. Sparing our enemies is not an act of virtue. Nor does it mean that they will choose to spare us. It is essential that our military help civilian decision makers escape the cancerous lies concocted by think tanks and university faculties about war. The military's first domestic mission is education: to help civilian decision makers unlearn the nonsense they have been taught throughout their careers. If our uniformed leaders neglect this educational mission they will have no right to complain when their advice is ignored in a crisis, when our troops are misused, and when the nation's leaders leave our military holding the (body) bag after things go wrong. Warfare is a bath of blood in a pool of horror. Any imagined alternative is not war. The observations offered above sound cruel. But warfare is not kind. If we are unwilling to accept that it is not enough to defeat an enemy technically, but that [they] he must be convinced of [their] his defeat, we will continue to falter. The shock of an attack by our military in a general war should be so overwhelming—so deadly, graphically destructive, and uncompromising—that the enemy, faced with unbearable losses, loses his will to fight. When we face particularly tenacious enemies whose resolve to resist does not waver we must be willing to destroy them. If we shrink from the acts of destruction necessary to defeat an enemy thoroughly we will find ourselves suffering unnecessary casualties in a needlessly protracted struggle. Even in comparatively benign peacekeeping operations we always should display overwhelming force. No potential enemy should be allowed to calculate a chance of success for himself. In operations short of war the appearance of irresistible strength can sometimes obviate the need to use that strength. But when we allow ourselves to appear diffident we only compound our problems. Many strategic lessons come from the schoolyard—no bully respects weakness, for example. Our ambition to do everything military cleanly, quickly, and cheaply in political terms has brought us to the point where we are often better at encouraging our enemies than we are at defeating them. Only strength is respected in the world beyond our shores. Not kindness, not wisdom, not the philosophical constructs so impressive to graduate students, but strength. A strong state that allows itself to appear weak will be challenged by weak states hoping to appear strong. There is no substitute for being feared. Paradoxically, we are undermined by our own capabilities. As we saw in Iraq, even when stripped to a bare minimum of forces our military is so skilled that it can wage campaigns and win conventional wars with breathtaking speed. But a swift war without attendant devastation inflicts no pain on the enemy population—and often too little on the enemy's combatants. It is not enough to win fast, although speed is increasingly essential. The victory must be devastating. Under different circumstances and against different opponents the amount of physical destruction required will vary widely. But while we may wish to minimize friendly casualties, it's a counterproductive absurdity to go to outlandish lengths to spare our enemies. We must get rid of the notion that we can make our enemies love us. This sounds harsh to American ears. But many of us will live to see our enemies commit such horrendous acts of brutality that the fiercest observations offered here will become second nature to us. Once enough of our fellow citizens have been slaughtered because of our fecklessness we will learn to kill with relish once again.

Critiquing the underpinnings of existing strategy is a link Peters '6

(Ralph, fmr US intelligence officer and best-selling author, Never Quit the Fight, 220-221)

The difference is that the extremists in Iraq don't expect a battlefield victory. They're fighting for time. They hope to wear us down, to maintain a level of photogenic chaos in just enough of Iraq to keep the media hot. They'll keep chipping away at our forces, praying that our will will prove far weaker than our weapons. They don't expect to force out our military through violence. They hope our political leaders will withdraw our troops. The terrorists have done their homework. They know that a disheartening number of our politicians share one of their beliefs: a low opinion of the American people, a notion that we're weak, that we're quitters. The terrorists know that our Marines aren't afraid of them. But they believe that our politicians are terrified. Of you. So you're the target of every bomb, bullet, and blade our enemies wield. Those Marines were killed to discourage you. They were targeted to ignite political discord in the United States. They died to give ammunition to those in Washington who view our dead only as political liabilities. There are practical military issues the administration hasn't addressed. Our forces in Iraq always have been too few. Much of the equipment with which our Marines and soldiers are equipped is old, inappropriate, and inadequate. We went to war with a military designed by defense contractors, not by warriors. But while those issues are real, we can't afford to play politics with the vital global struggle of our times, the battle with the psychotic strain of Islam that generates terror. Ultimately, the fate of Iraq won't be decided by our enemies. And it won't be decided by our troops. It's going to be decided by you. By your voice and your vote. The terrorists mean to help you make your decision.

Digital Surveillance

Digital surveillance is key – obstructs terrorist organization and execution

Sergei Boeke 15, research fellow at the International Center for Counter-Terrorism, LLM from Vrije Universiteit Amsterdam, Quirine Eijkman, "State surveillance in cyberspace," from Terrorism Online: Politics, Law and Technology ed. Jarvis, MacDonald, Chen, 3/24/15, pp. 133

**modified for gendered language; original text retained

Digital surveillance or eavesdropping does, however, have a severe disruptive effect on the workings of terrorist groups and their operations. Despite the shroud of secrecy that intelligence services would like to maintain over SIGINT collection, **terrorists are well aware of the risks of using the telephone and the Internet. One reason that the search for bin Laden took ten years was his systematic avoidance of all phones and the Internet.** It would be his courier, Al Kuwaiti, who would lead the CIA to bin Laden's hideout in Abbottabad, Pakistan. SIGINT, nonetheless, played a vital role. **In the summer of 2010, for the first time in almost a year, Al Kuwaiti, a known acquaintance of bin Laden, used the cellphone sim card that US intelligence had linked to him,** and he accepted a call with that sim card close to bin Laden's compound (ABC News 2011). **He had previously always followed fastidious operational security,** driving more than an hour-and-a-half from the compound before inserting the battery in his cell phone, thereby **preventing the NSA from pinpointing his starting point. The call he accepted in 2010 was from an old friend** who asked what he was up to. Al Kuwaiti replied that he was back with the people he was with before, eliciting the response "may God facilitate" (Woodward 2011). This set analysts on the trail, mobilising further human sources and satellite imagery to finally identify the compound where bin Laden was hiding. **This example of targeted surveillance illustrates three important points.** First, it makes clear that **top terrorist operators follow strict operational security procedures, whereby some avoid telephones completely and** others can have many different ones, switching their use and taking the batteries out when they can. The terrorist leaders who avoid phones altogether **are forced to communicate through other means, often reverting to the old fashioned letter. This places serious impediments on the organisation and its ability to execute of complex attacks.**" Second, there are indications that **whereas terrorist leaders are often exceptionally careful with their telephone or Internet communications** when it concerns their "professional" activities, **they can be more careless with their social contacts.** Unless a terrorist is acting **completely alone** and has perfect online and telephone discipline **there is a good chance that somewhere in the chain of events [they] he cannot resist** an old friends call or place a digital misstep during which **[they compromise themselves] he compromises himself** (Schmidt and Cohen 2013). Third, content and context remain essential. Without a good translation (preferably by native speakers) and knowledge of the context, Al Kuwaiti's words would have remained meaningless and the value of his call misunderstood.

Internet Surveillance

Internet surveillance is key to counter homegrown terrorism – threats are underestimated

Victor Beattie 5/11, Editor of Voice of America, official external broadcast institution of the United States federal government, "Homeland Security Chief: Global Terror Threat Has Entered 'New Phase,'" 5/11/15, www.voanews.com/content/us-security-chief-warns-of-new-phase-in-terrorist-threat/2762237.html

U.S. Homeland Security Secretary Jeh Johnson says the fight against global terrorism has entered a new phase with groups like the Islamic State (IS) successfully using social media to inspire others to join them or to launch domestic attacks. Johnson's comments Sunday on the ABC program This Week followed the revelation that federal law enforcement has hundreds of investigations underway to determine who might pose a threat of homegrown terrorism. Secretary Johnson noted the Islamic State group's ability to reach into the homeland to recruit homegrown jihadists.¶ Because of the use of the Internet, we could have little, or no, notice in advance of an independent attacker attempting to strike. And so, that's why law enforcement at the local level needs to be ever more vigilant, and we're constantly reminding them to do that," said Johnson.¶ Johnson says every attack or attempted attack represents a lesson learned and, as the threat evolves since the September 11, 2001 attacks, there has been closer cooperation among federal, state and local law enforcement officials.¶ Last week, the director of the Federal Bureau of Investigation (FBI), James Comey, warned there might be thousands of Islamic State followers online in the United States and the challenge is to determine who among them poses a real threat. Earlier this month, two gunmen attacked an event near Dallas, Texas, where cartoons of Islam's Prophet Muhammad were being judged in a contest. The gunmen were killed in an exchange of gunfire with police, in which a security guard was also wounded. Comey said his agency had warned the Garland, Texas police to be on the lookout for Elton Simpson and accomplice Nadir Soofi hours before the attack.¶ Johnson said he and other federal officials are trying to counter social media recruitment efforts by reaching out to the Muslim community in the United States.¶ "Since I have been secretary, I have personally participated in engagements with community leaders in the Islamic community and elsewhere. I've been to New York, Boston, Minneapolis, Chicago, Los Angeles and other places where I personally meet with community leaders about countering violent extremism in their communities. That has to be part of our efforts in this new phase," said Johnson.¶ Johnson said a lot of the counter-narrative to what he acknowledges to be a "slick and effective" message by the IS group to would-be terrorists on social media must come from those communities.¶ "It has to come from Islamic leaders who, frankly, can talk the language better than the federal government can and so, when I meet with community leaders, Islamic leaders, it's one of the things we urge them to do. Some have begun it. We've seen some good progress, but there's a lot more than can be done," he said.¶ Johnson described as prudent and cautious steps taken by the U.S. military to increase security at bases across the country, after the FBI warned that Islamist militants could target troops or local police.¶ Appearing on the Fox News Sunday broadcast from Paris, Congressman Michael McCaul, chairman of the House Homeland Security Committee, said there has been an uptick in threat streams against local police and military bases.¶ "We're seeing these on an almost daily basis. It's very concerning. I'm over here with the French counter-terrorism experts on the Charlie Hebdo case, how we can stop foreign fighters coming out of Iraq and Syria to Europe. But then, we have this phenomenon in the United States where they (terrorists) can be activated by the Internet. And, really, terrorism has gone viral." said McCaul.¶ McCaul said the potential terror threat may even be greater than the FBI has outlined. He said the United States faces two threats: one from fighters coming out of the Middle East and the other from thousands at home who will take up the call to arms when the IS group sends out an Internet message. He warned the threat will only get worse, largely because of the existence of so many failed states in the Middle East and North Africa.

Surveillance-Proof Channels

Any surveillance-proof channels will be used by terrorists

Rahul Sagar 15, Associate Professor of Political Science at Yale-NUS College, “Against Moral Absolutism: Surveillance and Disclosure After Snowden,” Ethics & International Affairs 29(2),, pp. 145-159

A second deficiency relates to the disproportionality of the disclosures. Even though the NSA's domestic surveillance program was deemed lawful by the FISC, we could take the view that the lack of public debate about the capture of domestic metadata justified Snowden and Greenwald's disclosure of this particular program. But even so, it is hard to see how we could justify their disclosure of domestic surveillance methods, bearing in mind that these methods could help gather intelligence on what even Snowden and Greenwald might consider legitimate targets, namely, domestic terror plots.[¶] It is harder still to understand what purpose was served by disclosing NSA foreign surveillance methods such as the deployment of “backdoors” in commonly used hardware and software. Apparently the purpose was to alert countries and individuals around the world to the threat that the NSA poses to their privacy. Snowden and Greenwald have since encouraged countries to develop new infrastructure so that their communications do not have to transit through the United States, and have urged individuals to employ encryption and to cease using the services of companies that collaborate with the NSA. But this approach misses the point: if channels of communication that are immune to surveillance exist, these would be used not only by dissidents but also by terrorists. This is why the NSA is obliged to use all available means to crack new channels of communications (or else they could rightly be accused of negligence in the wake of a terrorist attack that relies on such channels). The approach taken by the President's Review Group is more balanced. Troubled by the prospect that aggressive surveillance methods could lead to a loss of trust in Internet-based services, they recommend that the United States should typically disclose known vulnerabilities in widely used software and hardware, but allow nonetheless that “in rare instances” the government may “briefly authorize” using such a vulnerability for “priority intelligence collection.”²⁷

Frontlines for Terror DA

FT Cyber Link Turn

The link outweighs the turn – they can't solve cyberterror because the database still exists, BUT any period without data collection increases the risk of an attack

Christi Parsons 5/28, Brian Bennett, "If NSA surveillance program ends, phone record trove will endure," 5/28/15, www.latimes.com/nation/la-na-nsa-phones-20150529-story.html?page=1

The National Security Agency will mothball its archive of Americans' telephone records, isolating the computer servers where they are stored and blocking investigators' access. **but will not destroy the database if its legal authority expires** on schedule this Sunday, officials said Thursday. **The NSA's determination to keep billions of domestic toll records for counter-terrorism and espionage investigations adds another note of uncertainty**, to a debate that pits the Obama administration's national security team against opponents who argue the government data trove violates Americans' privacy and civil liberties. The political and legal dispute will come to a head Sunday when the Republican-led Senate returns to work a day early to seek a resolution — hours before the law used to authorize the controversial NSA program, and several other key counter-terrorism provisions, expires at 11:59 p.m. The final eight hours — starting at 3:59 p.m. Sunday — will see a flurry of activity at U.S. phone companies and at the NSA as engineers take down servers, reconfigure monitoring software and unplug hardware from the main pipeline of telephone data traffic, according to several senior administration officials. If the Senate stalemate pushes past 7:59 p.m., holes in the incoming data will begin to appear — and will grow — until nothing is collected after midnight, the officials said, speaking on condition of anonymity to discuss internal planning. **We're in uncharted waters," one official said.** **"We have not had to confront the terrorist threat without these authorities. And it's going to be fraught with unnecessary risk.** At that point, even if the Senate acts, the officials said it could take three or four days to go back to the Foreign Intelligence Surveillance Court, also known as the FISA court, for a legal order to restart the system and to reboot the complex data transfer networks at the telephone companies and at the NSA headquarters at Ft. Meade, Md. Any Senate action short of approving legislation that already has passed the House will result in a gap in the NSA archive of so-called metadata — records that show the time, date and numbers called, but not the contents — of virtually every domestic phone call. **Letting the bulk collection program go dark even for a few days is "playing national security Russian roulette,"** said another official **and "hoping that we don't** have an instance where the FBI **need [the data] to do a national security investigation.** If lawmakers vote before 8 p.m. Sunday, the NSA could reverse the shutdown and prevent a gap, the officials said. But that last-hour possibility appears unlikely. Sen. Rand Paul (R-Ky.), who is running for the GOP presidential nomination and who has fought the NSA domestic program and filibustered to stop it, told supporters in a fundraising letter Thursday that he was determined to "relegate the NSA's illegal spy program to the trash bin of history, where it belongs." Administration officials have stepped up their own alarms. On Wednesday, **Atty. Gen.**

Loretta Lynch said a failure to act would cause "a serious lapse in our ability to protect the American people." The provision in the law used to authorize the NSA's bulk collection program is one of three legal authorities set to expire. **U.S. intelligence and law enforcement officials say all three are vital to tracking potential terrorists in the United States.**

The bulk collection of U.S. phone records was started in secret after the Sept. 11, 2001, terrorist attacks. It was specifically authorized by the FISA court starting in 2006, and was revealed to the public in 2013 in documents leaked by renegade former NSA contractor Edward Snowden. President Obama vowed to change the NSA program after Snowden's disclosures sparked an uproar, and the White House has embraced the so-called USA Freedom Act, which passed the House on May 13 by a bipartisan vote of 338 to 88. The measure would shift the burden of holding the data back to the telephone companies, and require them to configure their systems so the NSA could access the data. It also would require the government to get a court order to search the records for phone numbers linked to suspected terrorists at home and abroad. It sets a six-month transition period for the changes to take effect. Lynch and James R. Clapper, the director of national intelligence, assured House leaders in a letter this month that the bill "preserves the essential operational capabilities of the telephone metadata program and enhances other intelligence capabilities needed to protect our nation and its partners." But the Senate debate hit a roadblock when Paul and others, including Democratic Sen. Ron Wyden of Oregon, argued that the NSA program should simply expire, and efforts to pass the House bill founders in disarray Saturday before the lawmakers decamped for a weeklong holiday recess. At that point, the NSA put planning teams on "hot standby" and started working through telecommunications engineering to prepare for shutting down the networks that now connect investigators to the phone records, according to one senior official involved in the planning. The NSA contacted telephone companies to explain their plans and discuss how to help the private companies stop the automatic provision of calling records. They also have sought to configure monitoring software so officials can't access the archive. If they do, alerts will trigger and features will block the delivery of off-limits information. "You can't make a mistake on this," said one of the officials. "This is the most regulated thing that we do at NSA." If the authority lapses, he added, the agency would "lock it down with the same certainty with which we operate." The NSA won't wipe the collected data off its servers, officials said, but will lock all doors into the system. Investigators could use the trove only if Congress acts and the FISA court approves new searches. In addition to cutting off the phone searches, the expiration of the law would end the "roving wiretap" authority that lets FBI agents keep up with suspected terrorists or spies who switch "burner" phones to evade surveillance. Another authority set to expire is the "lone wolf" provision that lets the FBI apply to the court for permission to conduct wiretaps on a target they think is engaged in a terrorist activity but who isn't linked to a specific terrorist group. That authority hasn't been used, but it becomes more valuable every time Islamic State militants use the Internet to urge supporters to launch independent attacks, said one senior domestic security official. **As we face a decentralized and increasingly dispersed terrorism threat** and one where [Islamic State] is extolling actors to conduct opportunistic attacks, this is not a tool that we want to see go away.

official said. **Counter-terrorism officials would be facing "a big roll of the dice"** if the authorities are allowed to expire. Rep. Adam B. Schiff (D-Burbank), ranking member of the House Intelligence Committee, said in a telephone interview from Los Angeles.

FT Doesn't Solve

It's try-or-die for counter-terrorism – empirics are meaningless in the context of prevention

Rachel Brand 14, Senior Advisor to the U.S. Chamber Litigation Center and member of the Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," 1/23/14, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

There is no easy way to calculate the value of this program. But the test for whether the program's potential benefits justify its continuation cannot be simply whether it has already been the key factor in thwarting a previously unknown terrorist attack. Assessing the benefit of a preventive program such as this one requires a longer-term view. The overwhelming majority of the data collected under this program remains untouched, unviewed, and unanalyzed until its destruction. But its immediate availability if it is needed is the program's primary benefit. Its usefulness may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad. But if that happens, analysts' ability to very quickly scan historical records from multiple service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot. Evidence suggests that if the data from the Section 215 program had been available prior to the attacks of September 11, 2001, it could have been instrumental in preventing those attacks.⁶⁹³ The clear implication is that this data could help the government thwart a future attack. Considering this, I cannot recommend shutting down the program without an adequate alternative in place, especially in light of what I view to be the relatively small actual intrusion on privacy interests.

Death counts don't quantify efficacy – domestic surveillance confers numerous strategic benefits

Elizabeth Cook 14, member of the Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," 1/23/14, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

Finally, I have a different view from the Board as to the efficacy and utility of the Section 215 program. Although the Report purports to consider whether the program might be valuable for reasons other than preventing a specific terrorist attack, the tone and focus of the Report make clear that the Board does believe that to be the most important (and possibly the only) metric. I consider this conclusion to be unduly narrow. Among other things, in today's world of multiple threats, a tool that allows investigators to triage and focus on those who are more likely to be doing harm to or in the United States is both good policy and potentially privacy-protective. Similarly, a tool that allows investigators to more fully understand our adversaries in a relatively nimble way, allows investigators to verify and reinforce intelligence gathered from other programs or tools, and provides "peace of mind," has value. I would, however, recommend that the NSA and other members of the Intelligence Community develop metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs. The natural tendency is to focus on the operation of a given program, without periodic reevaluations of its value or whether it could be implemented in more privacy-protective ways. Moreover, the natural tendency of the government, the media, and the public is to ask whether a particular program has allowed officials to thwart terrorist attacks or save identifiable lives. Periodic assessments would not only encourage the Intelligence Community to continue to explore more privacy protective alternatives, but also allow the government to explain the relative value of programs in more comprehensive terms. I hope that our Board will have the opportunity to work with the Intelligence Community on such an effort.

Statistics are irrelevant – effective counter-terrorism is a question of political clout

Beatrice **de Graaf** 10, Bob de Graaff, “Bringing politics back in: the introduction of the ‘performative power’ of counterterrorism,” Critical Studies on Terrorism 3(2), 2010

In sum, it is almost impossible to measure arithmetically the outcome of counterterrorism efforts. However, this does not mean that we cannot and should not try to assess the effect of governmental policies. The issues outlined above suggest that it is not necessarily the policy measures and their intended results as such, but much more the way in which they are presented and perceived that determine the overall effect of the policy in question. The key question is therefore really: What do counterterrorism policy-makers want? They set the agenda with respect to the phenomenon of terrorism, define it in a certain way and link it to corresponding measures. Subsequently, they execute these measures, behind closed doors, and with the tacit permission of the public – or, conversely, they feel forced to ‘market’ their measures first, in order to generate a substantial level of public and political support. The way in which they perform, or in other words carry out the process of countering terrorism, can have more impact than the actual arrests being made (or not being made). This is what we call the performativity of counterterrorism, or its ‘performative power’. The authors would like to introduce the concept ‘performativity’ 1 in this discussion, expressing the extent to which a national government, by means of its official counterterrorism policy and corresponding discourse (in statements, enactments, measures and ministerial remarks), is successful in ‘selling’ its representation of events, its set of solutions to the terrorist problem, as well as being able to set the tone for the overall discourse regarding terrorism and counterterrorism – thereby mobilising (different) audiences for its purposes. 2

FT metadata solves

Encryption prevents access to key communication data

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))^{*Edited for easier flow}

Law enforcement and national security investigators need to be able to access communications and information to obtain the evidence necessary to prevent crime and bring criminals to justice in a court of law. We do so pursuant to the rule of law, with clear guidance and strict judicial oversight. But increasingly, even armed with a court order based on probable cause, we are* [the FBI is] too often unable to access potential evidence. The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers to be able to implement court orders for the purpose of intercepting communications. But that law wasn't designed to cover many of the new means of communication that exist today. Currently, thousands of companies provide some form of communication service, but most do not have the ability to isolate and deliver particular information when ordered to do so by a court. Some have argued that access to metadata about these communications - which is not encrypted - should be sufficient for law enforcement. But metadata is incomplete information, and can be difficult to analyze when time is of the essence. It can take days to parse metadata into readable form, and additional time to correlate and analyze the data to obtain meaningful and actionable information.

FT cloud solves

Cloud storage fails – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

Additional Considerations Some assert that although more and more devices are encrypted, users back-up and store much of their data in ‘the cloud,’ and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many companies impose fees to store information there - fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal’s or terrorist’s phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves devices which are increasingly encrypted.

FT hacking solves

Brute force attacks fail – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets. A common misperception is that we can simply break into a device using a ``brute force`` attack - the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today's highlevel encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data. Finally, a reasonable person might also ask, ``Can't you just compel the owner of the device to produce the information in a readable form?'' Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court's order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography. Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can't provide us with the password, especially when time is of the essence.

NSA can't crack encryption—Need encryption keys to access

The Nation '15 (The Nation is America's oldest continuously published weekly magazine, devoted to reporting on politics and culture. The Nation has bureaus in Washington, D.C., London, and South Africa, with departments covering architecture, art, corporations, defense, environment, films, legal affairs, music, peace and disarmament, poetry, and the United Nations, <http://www.nationmultimedia.com/breakingnews/NSA-can't-crack-common-encryption-software-top-hack-30251390.html>)CK

Publicly available encryption programmes are so tough that they can't be cracked by the experts at the US National Security Agency (NSA), an authoritative expert has told one of the world's top hacker jamborees. The assurance, delivered by Jacob Applebaum during this month's Chaos Communication Congress (CCC) in Hamburg, Germany, ends months of speculation that the NSA may have found a backdoor into such privacysoftware. Services like PGP for protecting emails and OTR (off the record) for protecting messaging are pretty safe, agreed experts at CCC, which attracts some of the globe's top hacking experts every January. "PGP and OTR are two ways to keep spies from looking through your stuff," says US activist Applebaum. He said communications protected end to end with these services cannot be read by the NSA. Period. Options like the SSL encryption protocol can be surmounted though, he said. SSL is used - often by banks and internet retail - to keep prying eyes from seeing which websites are being accessed and what's sent to them. SSH, used by system administrators to get into other computers and run them, can also be cracked. It's not clear, though, if the NSA has actually cracked their protocols. Instead, it seems the US electronic intelligence agency is trying to collect keys so it can crack encrypted communication by other methods. That's according to documents released by

whistleblower Edward Snowden, a former NSA contractor, which have been published by German news magazine Der Spiegel.

FT court order solves

Court orders can't compel decryption – backdoors are key

Crocker, attorney at the Electronic Frontier Foundation, 14 (Andrew Crocker, Graduate of Harvard Law and attorney at the Electronic Frontier Foundation in civil liberties, “Sifting Fact from Fiction with All Writs and Encryption: No Backdoors”, 12/3/14, [//EM*Edited for easier flow](https://www.eff.org/deeplinks/2014/12/sifting-fact-fiction-all-writs-and-encryption-no-backdoors)

Following recent reports in the Wall Street Journal and Ars Technica, there's been new interest in the government's use of a relatively obscure law, the All Writs Act. According to these reports, the government has invoked the All Writs Act in order to compel the assistance of smartphone manufacturers in unlocking devices pursuant to a search warrant. The reports are based on orders from federal magistrate judges in Oakland and New York City issued to Apple and another unnamed manufacturer (possibly also Apple) respectively, requiring them to bypass the lock screen on seized phones and enable law enforcement access. These reports come at an interesting time. Both Apple and Google have announced expanded encryption in their mobile operating systems. If a device is running the latest version of iOS or Android, neither company will be able to bypass a user's PIN or password and unlock a phone, even if the government gets a court order asking it to do so.

The announcements by Apple and Google have in turn led to calls for “golden keys”—hypothetical backdoors in devices intended to allow only law enforcement to access them. As we've explained, we think these proposals to create backdoors totally misunderstand the technology and make for terrible policy. Amid this prospect of a second “Cryptowar” is the lurking fear that the government might force unwilling companies to include backdoors in their products, even if they're not required by Congress to do so. We sometimes hear from jaded developers and others who think that all it would take to force a backdoor is one National Security Letter. While NSLs are unconstitutional, even the government admits that they* [NSLs] can only be used to obtain limited information, which does not include forcing anyone to backdoor a product. Nevertheless, this fear is feeding some of the interest generated by the press reports about the government's invocation of All Writs Act in the unlocking cases.

Court orders fail – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 (Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM)

Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks. In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default - without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice. Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search

warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection.

Data encryption eviscerates the third party doctrine – Lack of encryption permits government access

Christopher Soghoian Ph.D 06 (Principal Technologist with the Speech, Privacy, and Technology Project at the American Civil Liberties Union. He is also a Visiting Fellow at Yale Law School's Information Society Project. Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era Privacy and Law Enforcement pg. 391
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553)CK

“The third party doctrine is the Fourth Amendment rule that scholars love to hate. It is . . . widely criticized as profoundly misguided. Decisions applying the doctrine *top[] the chart of [the] most-criticized Fourth Amendment cases.”⁹⁵ However, for the purposes of this article, it can be summarized by stating that online service providers can be compelled to reveal their customers’ private documents with a mere subpoena.⁹⁶ As such, the government is not required to obtain a search warrant,⁹⁷ demonstrate probable cause⁹⁸ or go before a judge. While the third party doctrine is certainly the current tool of choice for the government’s evisceration of the Fourth Amendment, is not completely to blame for the lack of privacy online. The real and often overlooked threat to end-user privacy is not this legal rule, but the industry-wide practice of storing customers’ data in plain text, forgoing any form of encryption. Simply put, if encryption were used to protect users’ stored data, the third party doctrine would for the most part be moot.

FT voluntary solves

Compelling fails – backdoors are key

Hess, Executive Assistant Director of the FBI, 15 ([Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667//EM](#))

But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets. A common misperception is that we can simply break into a device using a “brute force” attack - the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today’s highlevel encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data. Finally, a reasonable person might also ask, “Can’t you just compel the owner of the device to produce the information in a readable form?” Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court’s order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography. Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can’t provide us with the password, especially when time is of the essence.

FT Sunset Thumper

Sunset provisions allowed for continuing investigations

Benjamin Wittenberg, Senior Fellow in Governance Studies at the Brookings Institution, “On the oddity of the Patriot Act sunset provisions,” Nov 2014, <http://www.lawfareblog.com/2014/11/on-the-oddity-of-the-patriot-act-sunset-provisions/>

Last week, the New York Times’s Charlie Savage had what seems to me a pretty big, if under-discussed, scoop—or perhaps we should say that he channelled to the public a pretty big scoop by former Senate Intelligence Committee chief counsel Michael Davidson. The news, which certainly caught me unawares, is that the Patriot Act sunset provision—stated in Section 105 of this law and extended until June 1, 2015 in this one—doesn’t quite say what everyone—from advocates to members of Congress to the administration itself—seems to think it says. Writes Savage: The law says that Section 215, along with another section of the Patriot Act, expires on “June 1, 2015, except that former provisions continue in effect with respect to any particular foreign intelligence investigation that began before June 1, 2015, or with respect to any particular offense or potential offense that began or occurred before June 1, 2015.”

Michael Davidson, who until his retirement in 2011 was the Senate Intelligence Committee’s top staff lawyer, said this meant that as long as there was an older counterterrorism investigation still open, the court could keep issuing Section 215 orders to phone companies indefinitely for that investigation. “It was always understood that no investigation should be different the day after the sunset than it was the day before.” Mr. Davidson said, adding: “There are important reasons for Congress to legislate on what, if any, program is now warranted. But considering the actual language of the sunset provision, no one should believe the present program will disappear solely because of the sunset.” Mr. Davidson said the widespread assumption by lawmakers and executive branch officials, as well as in news articles in The New York Times and elsewhere, that the program must lapse next summer without new legislation was incorrect.

FT “Name an attack that the program stopped”

Our 1NC Boot ev says 50 terror attacks have been stopped. Our Lewis ev proves others have been discouraged.

Meta-data does not need to *directly* stop attacks – it’s *indirectly* allowed for prioritization.

Lewis ‘14

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy. Before joining CSIS, he worked at the US Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His diplomatic experience included negotiations on military basing in Asia, the Cambodia peace process, and the five-power talks on arms transfer restraint. Lewis received his Ph.D. from the University of Chicago. *“Underestimating Risk in the Surveillance Debate”* - CENTER FOR STRATEGIC & INTERNATIONAL STUDIES - STRATEGIC TECHNOLOGIES PROGRAM – December - <http://csis.org/publication/underestimating-risk-surveillance-debate>

Assertions that a collection program contributes nothing because it has not singlehandedly prevented an attack reflect an ill-informed understanding of how the United States conducts collection and analysis to prevent harmful acts against itself and its allies. Intelligence does not work as it is portrayed in films: solitary agents do not make startling discoveries that lead to dramatic, last-minute success (nor is technology consistently infallible). Intelligence is a team sport. Perfect knowledge does not exist and success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture. Analysts assemble this mosaic from many different sources and based on experience and intuition. Luck is still more important than anyone would like and the alternative to luck is acquiring more information. This ability to blend different sources of intelligence has improved U.S. intelligence capabilities and gives us an advantage over some opponents.

Aff demand to “name one attack the program stopped” is *wrong* and a poor standard.

Branda ‘14

(et al; JOYCE R. BRANDA, Acting Assistant Attorney General, BRIEF FOR THE APPELLEES - Amicus Brief for Smith v. Obama – before the United States Ninth Circuit Court of Appeals. “Amici” means “friend of the court” and – in this context – is legal reference to the Reporters Committee – October 2nd - <https://www.eff.org/document/governments-smith-answering-brief>)

Plaintiff asks the government to show more, claiming that the program is an unconstitutional means of serving the paramount need of preventing terrorist attacks because the government has not “describe[d] a single instance” in which the program has “actually stopped an imminent attack” or “aided . . . in achieving any objective that was time-sensitive in nature.” Pl. Br. 33 (quoting Klayman, 957 F. Supp. 2d. at 40). The Constitution does not require an anti-terrorism program to have demonstrably prevented a specific terrorist attack to be reasonable. See Von Raab, 489 U.S. at 676 n.3 (“a demonstration of danger as to any particular airport or airline” is not required since “[i]t is sufficient that the Government

have a compelling interest in preventing a n otherwise pervasive societal problem from spreading"); Cassidy, 471 F.3d at 84-85; MacWade, 460 F.3d at 272. Nor is it problematic that the Section 215 program is only “one means” among many government programs that work together to accomplish the paramount goal of counterterrorism. Pl. Br. 35. To protect the Nation, the government employs a range of counter-terrorism tools and investigative methods in concert, which often serve different functions in order to complement one another in the service of achieving the overarching goal of preventing attacks. Those tools rarely, however, operate in isolation, and nothing in the Fourth Amendment's special needs jurisprudence requires a showing that any single program is essential or itself prevented a particular attack. The government has provided examples in which the Section 215 program provided timely and valuable assistance to ongoing counter-terrorism investigations. See ER 74-75.

FT Arab-American Relations, Intel Coop turn

() Even if Arab-American communities are frustrated with Fed policy, it doesn't mean they don't cooperate with Federal investigations.

Miller '6

Joel – holds a Ph.D. Sociology from Surrey University; and M.Sc. Social Research Methods (Awarded Distinction) from Surrey University; and a B.A. (Hons) Human Sciences, Oxford University, UK. Visiting Professor at The Institute of Criminology, University of Malaga, Spain; and Senior Research Associate, Vera Institute of Justice - "LAW ENFORCEMENT & ARAB AMERICAN COMMUNITY RELATIONS AFTER SEPTEMBER 11, 2001 Technical Report" - June 2006 -
http://www.vera.org/sites/default/files/resources/downloads/Arab_American_technical_report.pdf

Relations between Arab American communities and law enforcement agencies overall fell into two qualitative categories. Toward local police agencies, **Arab American** reported a fair amount of good will, even in jurisdictions where the two have little interaction. Where departments acted on this good will, evidence indicates that their efforts have already paid dividends in the form of reduced tension and improved rates of reporting. Community **perceptions of federal law enforcement**, on the other hand, **were less positive**. Even **though** most of the **FBI field offices in the study had reached out to Arab American communities, many Arab Americans remained fearful and suspicious of federal efforts**. **Despite the challenges enumerated above, our research also found that both community members and law enforcement respondents want to improve relations**. In fact, a select number of police **departments have already implemented promising practices to do so**, such as providing police officers with cultural sensitivity training relevant to their work, recruiting Arab American officers, and establishing police-community liaisons. However, more jurisdictions could benefit from these and similar undertakings, including, for example, creating clearly defined policies for dealing with issues relevant to immigrant communities, conducting consistent outreach to Arab communities, and demonstrating cultural awareness during community interactions. Where adopted, **Such efforts can lead not only to increased dialogue but also to meaningful partnerships that**, consistent with community policing philosophy, **better address** concerns about local and **national security**.

() Their turn is a myth – it's complete hype to suggest that Muslim Americans aren't already cooperating with law enforcement.

M.P.A.C. '11

The Muslim Public Affairs Council is a public service agency working for the civil rights of American Muslims, for the integration of Islam into American pluralism, and for a positive, constructive relationship between American Muslims and their representatives. Since 1988, MPAC has worked diligently to promote a vibrant American Muslim community and enrich American society through exemplifying the Islamic values of Mercy, Justice, Peace, Human Dignity, Freedom, and Equality for all. Over the years, MPAC has built a reputation as a consistent and reliable resource for government and media, and is trusted by American Muslims as an authentic, experienced voice. "Muslim Americans and Law Enforcement Partnerships" - Muslim Public Affairs Council website – Feb 11th -
<http://www.mpac.org/programs/government-relations/dc-news-and-views/muslim-americans-and-law-enforcement-partnerships.php>

Despite the enormous effort to separate mainstream Islam and Muslims from bin Laden's extremism and violence, **a dangerous myth of "Muslim silence" on terrorism persists**. Anti-Muslim pundits have gone as far as to accuse Muslim Americans of being a "fifth

column" or enemy within our nation, and even claim the community sympathizes and harbors violent extremists. This myth-laden discourse has reached such a fever pitch that officials such as Rep. Peter King (R-NY) are now planning Congressional hearings examining the "non-cooperation" of Muslim Americans with law enforcement, and their supposed failure to tackle extremists' ideology. The fact is that law enforcement officials and security experts have been tackling this issue head-on alongside the Muslim American community. Earlier this week, MPAC hosted a briefing on Capitol Hill to discuss law enforcement engagement with Muslim American communities. The forum's featured experts were CNN National Security Analyst Peter Bergen, former National Security Council Director Roger Cressey, Los Angeles County Sheriff Lee Baca and MPAC Government and Policy Analyst Alejandro Beutel.

FT Only Suspected Terrorists

“Suspected terror monitoring” is ineffective because it doesn’t stop the unknown terrorist

James Andrew Lewis 14, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies, December 2014, “Underestimating Risk in the Surveillance Debate,”

http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf

The echoes of September 11 have faded and the fear of attack has diminished. We are reluctant to accept terrorism as a facet of our daily lives, but major attacks—roughly one a year in the last five years—are regularly planned against U.S. targets, particularly passenger aircraft and cities. America’s failures in the Middle East have spawned new, aggressive terrorist groups. These groups include radicalized recruits from the West—one estimate puts the number at over 3,000—who will return home embittered and hardened by combat. Particularly in Europe, the next few years will see an influx of jihadis joining the existing population of homegrown radicals, but the United States itself remains a target.

America’s size and population make it is easy to disappear into the seams of this sprawling society. Government surveillance is, with one exception and contrary to cinematic fantasy, limited and disconnected. That exception is communications surveillance, which provides the best and perhaps the only national-level solution to find and prevent attacks against Americans and their allies. Some of the suggestions for alternative approaches to surveillance, such as the recommendation that NSA only track “known or suspected terrorists,” reflect both deep ignorance and wishful thinking. It is the unknown terrorist who will inflict the greatest harm.

FT Useless Data

No such thing as useless data – it stops us from going after false leads

James Andrew **Lewis** 14, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies, December 2014, “Underestimating Risk in the Surveillance Debate,”

http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf

What is left out of this picture (and from most fictional portrayals of intelligence analysis) is the number of false leads the analysts must pursue, the number of dead ends they must walk down, and the tools they use to decide that something is a false lead or dead end. Police officers are familiar with how many leads in an investigation must be eliminated through legwork and query before an accurate picture emerges. Most leads are wrong, and much of the work is a process of elimination that eventually focuses in on the most probable threat. If real intelligence work were a film, it would be mostly boring. Where the metadata program contributes is in eliminating possible leads and suspects.

This makes the critique of the 215 program like a critique of airbags in a car – you own a car for years, the airbags never deploy, so therefore they are useless and can be removed The weakness in this argument is that discarding airbags would increase risk. How much risk would increase and whether other considerations outweigh this increased risk are fundamental problems for assessing surveillance programs. With the Section 215 program, Americans gave up a portion of their privacy in exchange for decreased risk. Eliminating 215 collection is like subtracting a few of the random pieces of the jigsaw puzzle. It decreases the chances that the analysts will be able to deduce what is actually going on and may increase the time it takes to do this. That means there is an increase in the risk of a successful attack. How much of an increase in risk is difficult to determine, but this is crucial for assessing the value of domestic surveillance programs.

If the risk of attack is increasing, it is not the right time to change the measures the United States has put in place to deter another 9/11. If risk is decreasing, surveillance programs can be safely reduced or eliminated. A more complicated analysis would ask if the United States went too far after 9/11 and the measures it put in place can be reduced to a reasonable level without increasing risk. Unfortunately, precise metrics on risk and effectiveness do not exist,¹² and we are left with the conflicting opinions of intelligence officials and civil libertarians as to what makes effective intelligence or counterterrorism programs. There are biases on both sides, with intelligence officials usually preferring more information to less and civil libertarians can be prone to wishful thinking about terrorism and opponent intentions.¹³

Interviews with current and former intelligence officials give us some guidance in deciding this. The consensus among these individuals is that 215 is useful in preventing attacks, but the least useful of the programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215 before any others, but ending 215 would not come without some increase in risk.

FT Link Turn- Data Overload

New data programs solve info overload

Lavenda 3-21-15, Technology strategist

David, "How Smartphone Metadata Can Help Prevent Information Overload",
<http://www.cmswire.com/cms/mobile-enterprise/how-smartphone-metadata-can-help-prevent-information-overload-024591.php?pageNum=2>

Where to Next? Where No Man Has Gone Before: The rapid deployment of sensor-rich smart mobile devices, coupled with the proliferation of distributed, heterogeneous cloud services provides a fertile ground for almost limitless opportunities to define contexts that could pinpoint and surface the information you need "right here, right now." Validation of this trend was provided by Microsoft's recent announcement of the Office Graph. Microsoft's Office Graph uses "signals from email, social conversations, documents, sites, instant messages, meetings and more to map the relationships between the people and things that make your business go." Apps that can tap into the intelligence of Office Graph and related sources, might finally be able to crack the information overload problem. The Internet of Things is ultimately the top level of sophistication available for context-aware situations. Specifically, when devices will be able to communicate amongst themselves, the sky is literally the limit about what is possible. The opportunities to reduce information overload afforded by the coupling of sensors, context and machine-machine interactions will be covered in a future article.

Data tagging and organization do too

Harari 6-23-15, Thompson Reuters

Ofer, "Big Data Intelligent Tagging: Bringing Order to Information Overload",
<http://tabbforum.com/opinions/big-data-intelligent-tagging-bringing-order-to-information-overload>

Data has long been the driving force in financial services, and it continues to play an important role powering everything from governments to healthcare. In this era of Big Data, the ongoing flow of information can be overwhelming or distracting. But when used intelligently, today's open data economy can drive informed, strategic decisions and give a financial service firm an edge in the marketplace. Structured, machine-readable and intelligent information is essential in an evolving landscape in which there are more than three billion online users globally, generating millions of text documents daily. For example, satellite images now offer incredible detail about the state of crops in various parts of the world. Machines can sort through corporate SEC filings faster than any human. Bricks-and-mortar retailers can track the number of people going into stores, how long they spent there and what they walked out with – while online rivals such as Amazon know what people searched for and can make a good guess about what they might order and when. News is now disseminated on social sites such as Twitter faster than through traditional news agencies – and it comes in greater quantity than ever before. [Related: "In-House Alpha: Mining the Unstructured Data Within"] But the abundance of data is only the beginning – firms still face the crucial task of making sense of it all and deriving tangible benefits from it. In a vast digital world, how can a company get to the heart of what is needed and make valuable connections between people, subjects, places and more? For Big Data to be useful, our clients must connect the dots, find what is relevant and leave the rest behind – in other words, separate the wheat from the chaff. Thomson Reuters Intelligent Tagging, powered by Calais, has been

used for the past six years inside Thomson Reuters to effectively mine content, help analysts collect and curate information, and make content searchable in our flagship products such as Eikon, WestlawNext and more. We are now making this exact same service available to our clients as well, providing technology and business professionals access to the automatic generation of rich, semantic metadata and providing a way to link, tag and find relationships within content to increase its value and gain competitive advantage. But Intelligent Tagging also goes far beyond classic entity identification. It uses Natural Language Processing (NLP), text analytics and data mining technologies to derive meaning from all that unstructured information – including research reports, news articles and blog posts. It then connects extracted entities to Thomson Reuters “core entity masters,” which provide even more information and connections to leverage for search and analytics. Thomson Reuters internal Content Marketplace defines a global information model across the organization where each content set is managed centrally with keeping “one version of the truth” and with ontology and linkages to other content sets (like Organization Authority, People Authority, Industries, Deals and more). Thomson Reuters Intelligent Tagging is the glue that links any unstructured content, using metadata, to the relevant authorities (e.g., a News story that mentions a merger deal will be linked to the latest Deals tear sheet and the data on those companies in the Organization Authority). Our unified approach provides a comprehensive and unique perspective that cuts through the clutter and makes relevant connections. It helps clients standardize data definitions, share information across the enterprise and leverage knowledge hidden in the daily deluge of information as well as in data stores. This allows end users, such as analysts, managers, advisors or anyone seeking information, to move from long, challenging data searches, to gaining the insight and advantage that provide a competitive edge. Intelligent Tagging: As Simple as Child’s Play With this service available now to our clients, data can be easily searched for meaningful, usable information that can help the business be more competitive. 1. Tagging Using NLP, machine learning and other methods, Thomson Reuters Intelligent Tagging analyzes any kind of documents and finds the entities and events within it. This automatically adds rich, semantic, machine-readable metadata to the client’s content that is connected to the highly curated data of Thomson Reuters. 2. Intelligence The tags are delivered to the client’s platforms and incorporated into applications for search, analytics, alerts, news aggregation and other use cases. 3. Linkages Linkages to Thomson Reuters authorities with up-to-date metadata are available at any point in time. As a news and information company, Thomson Reuters has been amassing a host of data for years, giving us unparalleled ability to make the connections we’re now sharing through Intelligent Tagging. Our own teams rely on this proprietary service as an essential building block for developing new products and services. As the marketplace moves faster and grows more competitive, the relevance of intelligent information is becoming increasingly clear. With Intelligent Tagging, the ability to sort through the universe of information to find the news item, document or dataset that could put you ahead of the competition has become “child’s play.” Data About Data Metadata is “data about data.” For example, a book’s title and author is metadata. In information systems, a tag is a non-hierarchical keyword or term assigned to a piece of information (such as an Internet bookmark, digital image, or computer file). This kind of metadata helps describe an item and allows it to be found again by browsing or searching. By tagging, clients can start to create an organized, linked metadata store that can be constantly updated and searched for intelligent insight. For example, by tagging entities in a given article and then connecting those entities to Thomson Reuters’ rich metadata, a user would have access to a wealth of information, such as: Entities: Examples are companies, people, places and products. Relationships: John Doe works for Acme Corp., which is a pharma company in Dallas. Facts: John Doe is a 42-year-old, male

CFO, Events: Jane Doe was appointed a board member of Acme Corp., Topics: Story is about M&As in the pharma industry.

No risk of info overload – NSA is using graph analysis and has a massive storage center. Large data records are key to investigations.

Harris 13 (Derrick Harris, Senior writer about technology at Gigaom and Senior Research Analyst at Mesosphere, with a J.D. from the University of Nevada-Las Vegas School of Law, “Here’s how the NSA analyzes all that call data,” Gigaom, 6 June 2013, <https://gigaom.com/2013/06/06/heres-how-the-nsa-analyzes-all-that-call-data/>, *fc)

There are numerous methods the NSA could use to extract some insights from what must be a mind-blowing number of phone calls and text messages, but graph analysis is likely the king. As we’ve explained numerous times over the past few months, graph analysis is ideal for identifying connections among pieces of data. It’s what powers social graphs, product recommendations and even some fairly complex medical research.

But now it has really come to the fore as a tool for fighting crime (or intruding on civil liberties, however you want to look at it). The NSA is storing all those Verizon (and, presumably, other carrier records) in a massive database system called Accumulo, which it built itself (on top of Hadoop) a few years ago because there weren’t any other options suitable for its scale and requirements around stability or security. The NSA is currently storing tens of petabytes of data in Accumulo.

In graph parlance, vertices are the individual data points (e.g., phone numbers or social network users) and edges are the connections among them. In late May, the NSA released a slide presentation detailing how fast fast Accumulo is able to process a 4.4-trillion-node, 70-trillion-edge graph. By way of comparison, the graph behind Facebook’s Graph Search feature contains billions of nodes and trillions of edges. (In the low trillions, from what I understand.)

So, yes, the NSA is able to easily analyze the call and text-message records of hundreds of million of mobile subscribers. It’s also building out some massive data center real estate to support all the data it’s collecting.

How might a graph analysis work within the NSA? The easy answer, which the government has acknowledged, is to figure out who else is in contact with suspected terrorists. If there’s a strong connection between you and Public Enemy No. 1, the NSA will find out and get to work figuring out who you are. That could be via a search warrant or wiretap authorization, or it could conceivably figure out who someone likely is by using location data.

Having such a big database of call records also provides the NSA with an easy way to go back and find out information about someone should their number pop up in a future investigation. Assuming the number is somewhere in their index, agents can track it down and get to work figuring out who it’s related to and from where it has been making calls.

NSA can deal with big data – databases and partnerships with private companies allow for effective analysis

Gallagher, '13 (Sean [intelligence reporter and former Navy officer]; "What the NSA can do with "big data", Ars Technica, <http://arstechnica.com/information-technology/2013/06/what-the-nsa-can-do-with-big-data/2/>, page 2)

Ironically, about the same time these two programs were being exposed, Internet companies such as Google and Yahoo were solving the big data storage and analysis problem. In November of 2006, Google published a paper on BigTable, a database with petabytes of capacity capable of indexing the Web and supporting Google Earth and other applications. And the work at Yahoo to catch up with Google's GFS file system—the basis for BigTable—resulted in the Hadoop. BigTable and Hadoop-based databases offered a way to handle huge amounts of data being captured by the NSA's operations, but they lacked something critical to intelligence operations: compartmentalized security (or any security at all, for that matter). So in 2008, NSA set out to create a better version of BigTable, called Accumulo—now an Apache Foundation project. Accumulo is a "NoSQL" database, based on key-value pairs. It's a design similar to Google's BigTable or Amazon's DynamoDB, but Accumulo has special security features designed for the NSA, like multiple levels of security access. The program is built on the open-source Hadoop platform and other Apache products. One of those is called Column Visibility—a capability that allows individual items within a row of data to have different classifications. That allows users and applications with different levels of authorization to access data but see more or less information based on what each column's "visibility" is. Users with lower levels of clearance wouldn't be aware that the column of data they're prohibited from viewing existed. Accumulo also can generate near real-time reports from specific patterns in data. So, for instance, the system could look for specific words or addressees in e-mail messages that come from a range of IP addresses; or, it could look for phone numbers that are two degrees of separation from a target's phone number. Then it can spit those chosen e-mails or phone numbers into another database, where NSA workers could peruse it at their leisure. In other words, Accumulo allows the NSA to do what Google does with your e-mails and Web searches—only with everything that flows across the Internet, or with every phone call you make. It works because of a type of server process called "iterators." These pieces of code constantly process the information sent to them and send back reports on emerging patterns in the data. Querying a multi-petabyte database and waiting for a response would be deadly slow, especially because there is always new data being added. The iterators are like NSA's tireless data elves. Accumulo is just one weapon in the NSA's armory. The aggregated data pumped out of Accumulo can be pulled into other tools for analysis, such as Palantir's analytic databases and its Graph application. Graph builds a visualization of the links between "entities" based on attributes and relationships and searches based on those relationships—conceptually similar to Facebook's Unicorn search and social graph, Google's Knowledge Graph, and Microsoft Research's Satori.

Empirical examples have proven that “big data” is actually more effective in detecting terrorists.

Press, 13 (Gil Press, a marketing, publishing, research and education consultant, "The Effectiveness Of Small Vs. Big Data Is Where The NSA Debate Should Start", 6-12-2013, Forbes, <http://www.forbes.com/sites/gilpress/2013/06/12/the-effectiveness-of-small-vs-big-data-is-where-the-nsa-debate-should-start/>)

In his Wired story, Bamford pointed to a breakthrough in code-breaking and the building of a more powerful supercomputer as the prime motivations behind the sweeping of more and more data. And more to come—the reason for storing all the data is “What can’t be broken [as in code-breaking] today may be broken tomorrow.” But Bamford may have missed the rise of the big data and machine learning experts at the NSA and the replacement of supercomputers with “commodity” servers and storage devices for the cost-efficient processing of very large sets of data, using software that was first developed by Google, then enhanced and open-sourced by other Web-native companies (and that the NSA further developed and even gave back as the open-source Accumulo; see GigaOm and Wired). The availability of new hardware, software, and people well versed in the new ways of big data answered the new post-9/11 needs and probably drove a shift in focus from deciphering encrypted data to finding non-

encrypted “digital crumbs” left by and pointing to potential terrorists. If you’re looking for a needle in the haystack, you need a haystack.” Jeremy Bash, chief of staff to Leon E. Panetta, the former C.I.A. director and defense secretary, told MSNBC. That building a giant haystack is the way to go, and that you don’t need even to know what needle you are looking for, it will simply “emerge” from the data, is certainly what the NSA learned from big data advocates. “Now go out and gather some data, and see what it can do,” three Google researchers recommended in their influential 2009 paper, “The Unreasonable Effectiveness of Data” (PDF). That the paper dealt with a very specific domain—language processing—and argued only for the superiority of Google’s trillion-word corpus over pre-conceived ontologies, did not deter big data advocates from claiming the superiority of “data-as-a-model” (i.e., don’t use models, let the data speak) in all other domains, even claiming it is transforming science (forget about making hypotheses). The broad impact of these claims was evident last week when a Wall Street Journal editorial defending the NSA declared “The effectiveness of data-mining is proportional to the size of the sample, so the NSA must sweep broadly to learn what is normal and refine the deviations.” Size matters, end of story. The Wall Street Journal also reported that the NSA has tried, failed, and tried again to follow this “more data is better” philosophy until it saw success in 2010 with a program for the detection of the location of IEDs in Afghanistan. Analysts discovered that the system’s analysis improved when more information was added,” we are told. Whatever the magnitude of the improvement was, it could not have justified in my opinion this reaction from a former U.S. counterterrorism official, as reported by the Journal: “It’s the ultimate correlation tool... It is literally being able to predict the future.” But if you want to believe that some success in a specific, narrow task indicates you can predict the future everywhere else, you proceed to collect all the data you can collect because you assume eventually it will tell you whatever you want to know and even what you don’t know that you don’t know. The New York Times mentioned another strand of influence on the NSA in the early 2000s: “When American analysts hunting terrorists sought new ways to comb through the troves of [data]... they turned to Silicon Valley computer experts who had developed complex equations to thwart Russian mobsters intent on credit card fraud.” Rachel Schutt, Senior Research Scientist at Johnson Research Labs, brought up this venerable and fairly successful example of data mining when I asked her (via email) about the NSA: “If they are building something like the equivalent of a fraud detection system for a credit card company, or some sort of suspicious activity detection system, then that needs to be running on all data streaming into the system. If they didn’t let all calls go through the fraud detection system, then they’ll miss fraud. This would be like a credit card company not saving all transactions or observing all transactions.” Schutt also explained why the NSA task of identifying specific individuals is different from the population-level work of traditional statistics: “Our understanding of statistical modeling is different when it comes to user-level data. It used to be we thought in terms of sampling in order to make inferences about the entire population. But with user-level data, we want to know about every individual. For a specific individual, we might want to sample from their phone calls if we discover we don’t need to keep it all (though how can you be sure?). It could be we only take snapshots or aggregates for that individual over time and that is sufficient to know they are not a terror threat with some level of confidence.”

The NSA is using technological advancements, such as innovative algorithms and approaches, to successfully sort through big data—data overload is no longer a problem.

Ouellette, 13 (Jennifer Ouellette, writer for the Quanta Magazine, "Scientific Data Has Become So Complex, We Have to Invent New Math to Deal With It", 10-9-2013, WIRED, <http://www.wired.com/2013/10/topology-data-sets/>)

“How the hell do you analyze that data?” DeDeo wondered. It wasn’t the size of the data set that was daunting; by big data standards, the size was quite manageable. It was the sheer complexity and lack of formal structure that posed a problem. This “big data” looked nothing like the kinds of traditional data sets the former physicist would have encountered earlier in his career, when the research paradigm involved forming a hypothesis, deciding precisely what one wished to measure, then building an apparatus to make that measurement as accurately as possible. “In physics, you typically have one kind of data and you know the system really well,” said DeDeo. “Now we have this new multimodal data [gleaned] from biological systems and human social systems, and the data is gathered before we even have a hypothesis.” The data is there in all its messy, multi-dimensional glory, waiting to be queried, but how does one know which questions to ask when the scientific method has been turned on its head? DeDeo is not the only researcher grappling with these challenges. Across every discipline, data sets are getting bigger and more complex, whether one is dealing with medical records, genomic sequencing, neural networks in the brain, astrophysics, historical archives,

or social networks. Alessandro Vespignani, a physicist at Northeastern University who specializes in harnessing the power of social networking to model disease outbreaks, stock market behavior, collective social dynamics, and election outcomes, has collected many terabytes of data from social networks such as Twitter, nearly all of it raw and unstructured. “We didn’t define the conditions of the experiments, so we don’t know what we are capturing,” he said. Today’s big data is noisy, unstructured, and dynamic rather than static. It may also be corrupted or incomplete. “We think of data as being comprised of vectors – a string of numbers and coordinates,” said Jesse Johnson, a mathematician at Oklahoma State University. But data from Twitter or Facebook, or the trial archives of the Old Bailey, look nothing like that, which means researchers need new mathematical tools in order to glean useful information from the data sets. “Either you need a more sophisticated way to translate it into vectors, or you need to come up with a more generalized way of analyzing it,” Johnson said. Vespignani uses a wide range of mathematical tools and techniques to make sense of his data, including text recognition. He sifts through millions of tweets looking for the most relevant words to whatever system he is trying to model. DeDeo adopted a similar approach for the Old Bailey archives project. His solution was to reduce his initial dataset of 100,000 words by grouping them into 1,000 categories, using key words and their synonyms. “Now you’ve turned the trial into a point in a 1,000-dimensional space that tells you how much the trial is about friendship, or trust, or clothing,” he explained. Scientists like DeDeo and Vespignani make good use of this piecemeal approach to big data analysis, but Yale University mathematician Ronald Coifman says that what is really needed is the big data equivalent of a Newtonian revolution, on par with the 17th century invention of calculus, which he believes is already underway. It is not sufficient, he argues, to simply collect and store massive amounts of data; they must be intelligently curated, and that requires a global framework. “We have all the pieces of the puzzle — now how do we actually assemble them so we can see the big picture?” he said. “You may have a very simplistic model at the tiny local scale, but calculus lets you take a lot of simple models and integrate them into one big picture.” Similarly, Coifman believes that modern mathematics — notably geometry — can help identify the underlying global structure of big datasets. A data set might be organized by geography or climate, for example, each of which will produce a very differently shaped map.

FT HUMINT turn

HUMINT can't fill in – it's slow, limited to small-ball intelligence and terrorists will adapt. Big data is vital to mapping the entire network with enough warning to prevent attacks

Mudd, 13 - Mr. Mudd was deputy director of the CIA Counterterrorist Center, 2003-05, and senior intelligence adviser at the FBI, 2009-10. He is now director of Global Risk at SouthernSun Asset Management (Philip, “Mapping Terror Networks: Why Metadata Matters” Wall Street Journal, 12/29,

<http://www.wsj.com/articles/SB10001424052702304367204579270472690053740>

We met every afternoon in the CIA director's conference room at 5. At the FBI director's conference room, we met every morning shortly after 7.

At both agencies, the questions were similar: How best can we clarify the blurry picture of an emerging terror conspiracy overseas or in the United States? How can we identify the key players and the broader network of fundraisers, radicalizers, travel facilitators and others quickly enough so they can't succeed? And how do we ensure that we've mapped the network enough to dismantle—and not merely disrupt—it?

The only way to understand why the NSA collects and needs access to vast amounts of telephone metadata is to keep these questions in mind, especially the last. In ruling on Friday that the data collection is lawful, U.S. District Court Judge William H. Pauley III expressed it well: "The government needs a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data."

Mapping a network of people is simple in concept but complex in practice: find the key operators, and then find the support group. The challenge isn't limited to counterterrorism. Any group—from organized-crime enterprises to gangs, drug cartels, or human traffickers—consists of a team of people who interact and are organized for a particular purpose. If an analyst maps that network well enough, then a series of arrests or lethal operations can destroy it.

Map a network poorly, however, and you may miss peripheral players who will recreate a conspiracy after the core conspirators are arrested. The goal is to eliminate the entire spiderweb of a conspiracy; cutting off a piece, like the arm of a starfish, is a poor second choice. The starfish's arm regenerates.

Think of the range of linkages you might find among individuals in these networks. Money, phone calls, email exchanges, travel, social media, chat rooms—the modes constantly expand. How many linkages could a security service monitor electronically even two decades ago? Very few: Many of today's means of communication and interaction didn't exist.

A security service can also use human surveillance teams on the ground to map a network. This is more familiar and comforting, and it might sound less intrusive than the digital mapping programs run by NSA computers. But human surveillance operations are slow, inefficient and costly. And they have a higher risk of missing members of the network. The fastest, most

efficient solution to mapping a network of conspirators lies in following digital connections among people. And as digital trails expand, digital network mapping will increase in value.

There is a healthy debate about how far U.S. security services should delve into our digital trails, but emotions too often overcome common sense. Every week I hear someone comment on whether the government is listening to their conversations—as if there's some huge complex of government employees in a mythical Area 51, listening to other Americans. The debates about government intelligence collection should be clearer about distinguishing between what the government collects and what it does with it. They may be collecting my phone number; what I'd worry more about is what they do with what they collect.

For an ongoing investigation, the data might seem relatively straightforward: link cellphones, email contacts, financial transactions, travel and visa information, add in whatever else you can find, and sort through the data using modern network analysis tools. Bingo! Within a day, you can have the beginnings of an understanding of a complex network that might take old-school investigators weeks or more to piece together.

Even so, an analyst has to ask other questions. Where did the conspirators travel a year ago? Five years ago? Who did they live with? Who did they sit next to on an airplane? Who gave them money? And a thousand other questions.

Investigators need an historical pool of data, in other words, that they can access only when they have information that starts with a known or suspected conspirator in the middle of a spiderweb they don't fully understand. Meanwhile, time pressures lurk: If you're late by a day, you lose.

In the post-9/11 world, the harder debate and more difficult questions center on pre-emptive intelligence—potentially lethal unknowns. Consider Minnesota, with its significant Somali expatriate population. Should analysts look for youths who buy one-way cash tickets to a country neighboring Somalia? What if they've accessed extremist websites? Would that combination of digital signals—none of which is an illegal act—be sufficient to initiate an investigation? And if there are circumstances that would result in preventive investigations, how can we conduct them if we don't have access to historical data in real time?

There are few certainties in this debate. But we do know that our digital trails will grow as more of our lives appear in bits and bytes, in records held by tomorrow's Amazons and Facebooks. And we know that to piece together networks, law enforcement and intelligence will use these data streams and need historical data to do so.

Intelligence analysts will look for more clarity on how policy makers and the public want to balance the ability to discern troubling patterns in private citizens' data and the national interest in ensuring that America remains a land of personal freedom where privacy is respected. But given the threats the country faces, mapping digital interactions among people will become ever more critical to understanding terrorists, criminals and foreign spies.

These tools and access to historical data are essential to mapping how bad guys operate. The trick won't be choosing privacy over security but in balancing the two.

Risk-averse politics mean a HUMINT shift won't solve

Harman, 15 - Director, President and CEO, Wilson Center, member of the Defense Policy Board, the State Department Foreign Policy Board, and the Homeland Security Advisory Committee. (Jane, "Disrupting the Intelligence Community" Foreign Affairs, March/April, <https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community>

Another factor making human intelligence gathering a harder game to play is the broader American political culture. Developing informants (let alone embedding assets) within terrorist groups is a dicey proposition. And regardless of their personal courage or willingness to serve, intelligence officers must now operate in a political climate that discourages risk taking, because the American public reacts so strongly to U.S. casualties—something the fallout from the 2012 attack on the U.S. compound in Benghazi, Libya, which killed two Foreign Service officers and two security personnel, made clear. Of course, such political constraints and risk aversion affect the U.S. military, too. This is partly why many U.S. policymakers are cool to the idea of putting boots on the ground in the fight against ISIS. The irony is that an effective air war relies on precise targeting, which requires good intelligence collected on the ground, which itself exposes U.S. personnel to the sorts of risks an air war is supposed to avoid.

A combined approach to intelligence is best – neglecting any one component increases the risk of systemwide failure

Sims, 7 - Professorial Lecturer at Johns Hopkins University School of Advanced International Studies; former intelligence analyst for the State Department and the Defense Intelligence Agency (Jennifer Sims (2007) Intelligence to counter terror: The importance of all-source fusion, *Intelligence and National Security*, 22:1, 38-56, DOI: 10.1080/02684520701200772

Traditionally, US intelligence has used three types of collection to target opponents: technical intelligence (TECHINT), human intelligence (HUMINT) and open source or unclassified intelligence (OSINT). Technical intelligence includes the collection of imagery, intercepted communications, electronic signals emitted by equipment, engineering data from captured electronics or weapons systems, and data from equipment or materials in the environment that leave signatures of their presence, such as radiation, effluent plumes and noise, that trained analysts can discern using existing data as reference.⁸ The productivity of any of these collectors against a particular target will depend on that collector's access to the target's most vulnerable point. For example, if a network of spies uses wireless radios, picking up their electronic emissions (TECHINT) will be an effective way to find them; if they use couriers, human agents secretly opening the letters and packages (HUMINT) is likely to work best; if the adversary believes he is unobserved, collecting the names of those he visits from a phone book or the sites he visits while traveling as an ostensible tourist (OSINT) would be useful.

In any case, the best intelligence is obtained when the capabilities of all these collectors are quickly combined. Just as newspaper editors like to see multiple sources corroborating articles even from their best reporters, directors of national intelligence have greater confidence in

intelligence that comes from multiple collectors. Better than simply hearing that Osama Bin Laden has been sighted on a road in Pakistan would be seeing imagery of his convoy and receiving intercepts from his communications that each independently confirm the initial report.⁹ As long as an opponent runs reasonably complex operations, some collectors will work best against certain aspects of those operations, while others will work best against the rest. Thus ‘all source’ collection can yield many pieces of a puzzle that analysts can then assemble, jumble up, and reassemble as the adversary moves, reacts to countermoves, and moves again.

Beyond corroboration, however, is the concept of collection ‘boosting’ in which the productivity of one collector depends on input from others.¹⁰ The most obvious example of boosting within a single discipline is ‘direction finding’ (DFing), which may involve the use of multiple antennae to triangulate on a signal so that it can not only be identified, but also geo-located with some degree of precision.¹¹ During World War II, the SS paired up with the Gestapo and used direction-finding to locate the wireless radios used by a network of Stalin’s spies in Europe. To their great chagrin, these radios were found in Berlin – some next to the most sensitive government ministries.¹² Of course, boosting also works among collection disciplines, such as the use of spies (HUMINT) to steal the codes of adversaries so that analysts working on intercepted communications (TECHINT) can overcome the encryption methods and read the content of the messages.¹³ In fact, the more tightly integrated collectors are into the decision-making process the more likely an adversary’s spoofing of a collector will work to deflect or deceive one’s own decision-makers. Since securing collectors can be a costly and seemingly never-ending endeavor, one good way to compensate for inevitable vulnerabilities is to ensure collection is ‘constructively redundant’ – that is, sufficiently all-source that one collector’s vulnerability to spoofing will not lead to misperception or miscalculation.

This kind of constructively redundant all-source collection was a lynchpin of the allied strategy to defeat Hitler during World War II; it was employed, for example, to determine whether covert and clandestine collection operations had been compromised and, specifically, in the running of the famous British counterintelligence operation known as Double Cross.¹⁴ But the history of Double Cross also alerts us to the inherent dangers of redundant collection systems: since collectors improve the reliability of each other’s products by offering independent corroboration, they depend on good systemwide counterintelligence so an adversary cannot defeat or spoof one of them and thus sow ambiguity, uncertainty and confusion throughout an interlaced collection system. If systemic counterintelligence is weak, collectors have good reason not to share their ‘take’ lest it become tainted. Poor counterintelligence can lead to system-wide failure even when the majority of collection endeavors are robust and productive.¹⁵

In some respects, then, the business of all-source data fusion for countering terrorism follows what has been done in a traditional sense against other intelligence targets. What makes the counterterrorism a particularly challenging endeavor is the terrorists’ objective of committing stealthy crime – often on the victim’s home soil. This means that law enforcement information, including information on US residents or citizens living in close proximity to the terrorists, may be important intelligence information that needs to be shared with decision-makers at the federal level working to thwart terrorist activities on a nationwide scale. Law enforcement agents, dedicated to preserving the information for the purposes of arrest and prosecution, realize the need to pass the information over to these officials but do not always know the best and most secure ways to do so. At times, in fact, the most important decisions must be made very quickly by state and local officials if they are to prevent an impending attack. In these cases, circulating

information to Washington for recycling into intelligence products could delay action rather than assist it. The problem thus becomes the very nontraditional one of fusing all-source intelligence for a cop on the beat.

FT Allied cooperation turn

Intelligence cooperation remains high regardless of relations

Butler, 14 - Vice President of Government Strategies, IO, a privately-held data center, builder and provider. And he's also an Adjunct Fellow at the Center for New America Security, previously the First Deputy Assistant Secretary of Defense for Cyber Policy at the Pentagon (Bob, "THE INTERNATIONAL IMPLICATIONS OF THE NATIONAL SECURITY AGENCY LEAKS" 6/4)

MR. BUTLER: Sure. I'm going to talk briefly about defense and then I'm going to spend most of my time, based on where I sit today, talking about tech; an industry from a global datacenter perspective. Within defense, though, I think in light of the Snowden revelations I think Cam's explanation of a kind of a aircraft accident or a car accident, kind of, proceeding slowly, holds true. There is a sense -- there was a sense of awkwardness, and a lot -- I think a lot of folks just watching to see how the United States was going to deal with it.

At the same time, in these -- when these unfortunate situations happen, National Security and Defense dialogue trumps, so with coalition partners close allies, the conversation continues and it continues to grow. I think the other dimension is, you have two sides of a discussion, is above-the-table political discussion that's going on, and then there's a discussion within the defense and intelligence community. And again, from the substance of national interest, not only U.S. national interest, but foreign national interest, there is -- you know, we built alliances, coalitions and relationships based on dialogue.

Mutual self interest means those relationships are resilient

Jones, 14 - Senior Fellow and Director, Project on International Strategy and Order

The Brookings Institution (Bruce, "THE INTERNATIONAL IMPLICATIONS OF THE NATIONAL SECURITY AGENCY LEAKS" 6/4)

MR. JONES: Well, having been fairly response, let me be slightly more upbeat in this, because if I look out over several years, I'm -- and even a shorter term that I'm more inclined to -- your last point about, there's an old news phenomenal now, or at least there can be. It's well-timed, there's about to be Brazilian elections, and there just been Indian elections, when you look at the swing states and some of the other actors who are in this, they are not U.S. allies, but they are not adversaries so kind of friend -- neither friend nor foe country.

I think you've seen relatively quickly now, a sense of, look, it's just too costly to sustain tension with the United States, so let's find ways to move past this. And elections are helpful, either bringing in new actors or by sort of demarcating we can say, well that was that phase, and now we'll move on. Harold talked about that in the Brazilian context, I think we'll see that in the Indian context, a sense of, okay, that was that, let's move, let's move onwards.

And I think the kind of, used phrase, mutual self-interests, but when you look at these actors and what they are looking at in big-picture terms with China, with Russia, with the frame of different regimes, and they look at the United States, the mutual self-interest is pretty rapidly putting this one back in a box at a very strategic level at least.

Overall US-EU cooperation is high

Archick, 14 - Specialist in European Affairs at the Congressional Research Service (Kristin, “U.S.-EU Cooperation Against Terrorism” 12/1, <https://www.fas.org/sgp/crs/row/RS22030.pdf>

U.S.-EU cooperation against terrorism has led to a new dynamic in U.S.-EU relations by fostering dialogue on law enforcement and homeland security issues previously reserved for bilateral discussions with individual EU member states. **Despite some frictions, most U.S. policy makers and analysts view the developing partnership with the EU in these areas as positive.** Like its predecessor, the Obama Administration has supported U.S. cooperation with the EU in the fields of counterterrorism, border controls, and transport security.

At the November 2009 U.S.-EU Summit in Washington, DC, the two sides reaffirmed their commitment to work together to combat terrorism and enhance cooperation in the broader JHA field. In June 2010, the United States and the EU adopted a “Declaration on Counterterrorism” aimed at deepening the already close U.S.-EU relationship and highlighting the commitment of both sides to combat terrorism within the rule of law. In June 2011, President Obama’s National Strategy for Counterterrorism asserted that in addition to working with European allies bilaterally, “the United States will continue to partner with the European Parliament and European Union to maintain and advance CT efforts that provide mutual security and protection to citizens of all nations while also upholding individual rights.” The EU has also been a key U.S. partner in the 30-member Global Counterterrorism Forum, founded in September 2011 as a multilateral body aimed at mobilizing resources and expertise to counter violent extremism, strengthen criminal justice and rule of law capacities, and enhance international counterterrorism cooperation.¹²

Recently, U.S. and EU officials have been discussing ways to combat the foreign fighter phenomenon given increasing concerns that both European and American Muslims are being recruited to fight with Islamist groups in Syria and Iraq. U.S. policy makers, including some Members of Congress, have expressed worries in particular about such foreign fighters in light of short-term visa-free travel arrangements between the United States and most EU countries. In early July 2014, U.S. Attorney General Eric Holder asserted, “We have a mutual and compelling interest in developing shared strategies for confronting the influx of U.S. and European-born violent extremists in Syria. And because our citizens can freely travel, visa-free ... the problem of fighters in Syria returning to any of our countries is a problem for all of our countries.”¹³ In September 2014, the White House noted that U.S. officials from the Department of Justice and the Department of Homeland Security are “working closely” with EU counterparts to “address a wide range of measures focused on enhancing counter-radicalization, border security, aviation security, and information sharing” to address potential threats posed by foreign fighters.¹⁴

Allied cooperation is inevitable – US surveillance diplomacy

Keiber 15 (Jason, PhD in Political Science, subfield of International Relations from Ohio State University, “Surveillance Hegemony,” http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/snowden_hegemony/snowden_hege, Surveillance and Society, Volume 13, Number 2, 2015, silbs)

<< Surveillance Hegemony: Power, Norms and Institutions

The extraordinary material surveillance capabilities of the US is perhaps most easily “measured” by its exorbitant funding. Nearly a third of the US’s \$52.6 billion intelligence budget is dedicated to fighting terrorism (Gellman and Miller 2013). 4 The NSA in particular gets one fifth of the overall budget. This money sustains a talented workforce and produces cutting edge surveillance techniques. These capabilities are often put to use covertly and unilaterally. The US, however, can also influence others to participate in its broader, strategic surveillance efforts. One of the more striking examples of secret cooperation is the recently disclosed RAMPART-A program in which over a dozen countries allow the US to install equipment to “congested” cables so that the US can intercept phone and internet traffic (Gallagher 2014).

With some caveats, both the US and the host country reportedly get access to the fruits of that surveillance. In general there are 37 states that are “approved SIGINT partners” (Greenwald 2014). This highlights the fact that other states accept (to varying degrees) core premises of how surveillance should work on an international scale. This acceptance, in turn, rests on a broader set of norms that emphasize the threat of terrorism and the necessity of counterterrorism measures. On the normative side of the ledger, a modicum of international surveillance in the form of information sharing has become not just tolerated, but held up as a responsibility states owe each other. Finally there is an array of international institutions that support surveillance activities. The US has been able to use its influential position within these institutions—the UN in particular—to establish an array of information sharing practices, all of which benefit US surveillance goals.

Anti-terrorism norms existed prior to 9/11, but the attacks on that day in 2001 vaulted anti-terrorism business to the top of the agenda. Terrorism moved from a threat to the predominant threat. Pre-9/11 norms began emerging as early as the end of the 19th century as a response to anarchism (Jensen 2013), but developed more thoroughly in the 1970s (see Rapoport 2002 for more on the international dimensions of terrorism over time). The general emphasis was that states should refrain from supporting international terrorism. After 9/11 this changed into a norm urging states to actively intervene to stop international terrorism. This requires shoring up their own surveillance capacity at home and sharing information with others abroad. >>

Surveillance diplomacy and assistance to other states proves it’s inevitable

Keiber 15 (Jason, PhD in Political Science, subfield of International Relations from Ohio State University, “Surveillance Hegemony,” http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/snowden_hegemony/snowden_hege, Surveillance and Society, Volume 13, Number 2, 2015, silbs)

The hegemonic position of the US is evident in its CT strategies. First, the US offers carrots to “weak” states, promising to “strengthen the capacity of such War on Terror partners to reclaim

full control of their territory through effective police, border, and other security forces as well as functioning systems of justice” (The White House 2006: 16). Only a powerful state could offer (and sometimes foist upon other states) such assistance.

Second, over time the US shifts from unilateral bluster (which is implicitly backed by direct coercion) to a more international approach (which relies on US diplomatic strengths and advantages in international fora). In the 2006 CT strategy, the language of “willing and able” states persists, but the stark language from 2003 is absent. Instead, for those states “reluctant to fulfill their sovereign responsibilities to combat terrorist-related activities within their borders” the US would lean on diplomacy and the rest of “the international community to persuade [these] states to meet their obligations to combat terrorism and deny safe haven under U.N. Security Council Resolution 1373” (The White House 2006: 16). This is the approach of a hegemon relying on less coercive modes of influence.

There are two watchwords throughout these documents—capacity and partnership. Both reflect US hegemony, and both find increasing use in the subsequent CT national strategies. State “capacity” is used twice in 2003, nine times in 2006, and 17 times in 2011 (The White House 2011). References to “partnerships” occurred 25, 41, and 59 times in the respective years. The US sees its CT relationship with other “willing” states as that of a partnership. Partnerships with “able” states are exercised through more joint efforts. In its partnerships with weaker states the US would help build their capacity to fight terrorism—a capacity that includes surveillance. The expectation is that the US approach to surveillance would be dominated by cooperative efforts with more capable states and assistance for weaker states to shore up their domestic surveillance capability.

FT Going dark / encryption

NSA will circumvent encryption – they'll use Network Exploitation
Corera July 15th

(Gordon Corera is Security Correspondent for BBC News, major documentaries for the BBC on the NSA, He is the author of the THE ART OF BETRAYAL: LIFE AND DEATH IN THE BRITISH SECRET SERVICE and SHOPPING FOR BOMBS: THE RISE AND FALL OF THE AQ KHAN NETWORK. In 2014 he was named Information Security Journalist of the Year at the BT INFORMATION SECURITY AND JOURNALISM AWARDS, "GCHQ WILL CIRCUMVENT ENCRYPTION NO MATTER WHAT. HERE'S HOW", Wired, <http://www.wired.co.uk/news/archive/2015-07/15/how-spies-will-circumvent-encryption-anyway>, TMP)

On both sides of the Atlantic the battle over encryption is hotting up, with the FBI continuing to press its case for access and the British government making noises about its fears of what an encrypted future might mean. The talk is of how ubiquitous encryption will lead to spies and law enforcement "going dark". ¶ In recent years, the state could compel national telecoms providers to give them access to data traffic, which the spies could then read. But those companies are seeing more and more of what passes through their pipes encrypted by service providers. And since Edward Snowden revealed the extent of government surveillance, those providers and other tech companies have come to see offering privacy as a selling point to their customers. But if end-to-end encryption becomes increasingly ubiquitous, is it the end of the line for the spies? History suggests not. ¶ When encryption first became available to the public in the 70s, thanks to the development of public key cryptography, one of its inventors Whit Diffie had a conversation with Arthur Levenson, a senior figure at US spy agency, the NSA. Diffie told Levenson he thought signals intelligence was finished. Levenson was less sure. "Whit, we've heard these arguments before," Levenson (whose experience stretched back to Bletchley Park) replied. Forty years on, as Diffie recalled the conversation with me, he shook his head with a rueful smile. "I was clearly mistaken," he says. When it comes to signals intelligence, "the sources are fragile, but the phenomenon is robust" as Diffie remembers one official telling him.¶ One of the things that became clear to me while writing a book on the history of computers and spies, is that the talk of going dark is not new and the smartest spies know they can adapt. Signals intelligence is an inherently insecure business in which the tiniest change can instantly dry up a valuable stream of intelligence.¶ When Nazi Germany upgraded its Enigma machine as the second world war started, the head of the Government Code and Cypher School (soon to become GCHQ) said it would be "a waste of time and public money" to even try to crack the new codes. But Alan Turing and others took up the challenge, and proved them wrong. As the Cold War started, Soviet codes proved near impossible to break. But the spies instead carried out massive traffic analysis on the externals of communications to extract useful intelligence. By establishing what normal patterns of Soviet military communications were, GCHQ and NSA would look for any change -- this might be an indicator of troops on the move, and potentially war. This was the real -- and secret -- birth of today's buzz word of "big data". Finally, when fibre-optic cables spread in the 90s, the spies again thought their satellite-based collection model was over, but they adapted (as Edward Snowden soon revealed). The point about end-to-end encryption is that there is still an endpoint where the message is clear and readable. And so the spies at GCHQ and NSA will likely shift

towards greater exploiting of target endpoints by what they call Computer Network Exploitation -- what everyone else calls hacking. This may also be done on a much larger scale than in the past, with references in some recent reports to something called "bulk" computer network exploitation. There are indications from the Snowden leaks that the US may be able to pre-install large numbers of implants in computers, ready to be activated. Spies will also do what they have done in the past by looking for weaknesses in encryption protocols (as they discovered with Enigma machines) and for any human failings in implementation. These may offer the chink in the armour which clever mathematicians and machines can together work on, as happened again at Bletchley. Other forms of surveillance may also play a role -- after all, a covertly placed camera above your PC can catch you type in your password and outwit the very best forms of encryption. This kind of activity needs to be authorised if the state wants to do it, however, and new laws planned for the UK are expected to overhaul the entire surveillance system to make it clearer what can and cannot be done ,and who should sign it off (perhaps soon a judge, rather than a minister). One of Whit Diffie's reflections about why he was mistaken back in the 70s is that, while much of the emphasis is on what proportion of traffic the state can read, there is another part of the equation for signals intelligence. And that is the overall volume of communications that are out there. The trend over the years has been for almost exponential growth and all the signs are that this will continue as we connect up more and more internet of things devices. And not everything will be properly encrypted. In other words, even if a smaller proportion of the communications is readable, there is still more out there overall. The connected devices in our household, like our fridges and those that we wear and carry, like our watches, are likely to be potentially highly revealing sources of intelligence. The shift towards encryption may also increase the pressure to carry out traffic analysis and extract meaning from metadata rather than the unreadable content. More will also be made of open source forms of intelligence (information searchable from the web and social media like Twitter which might reveal connections, links or locations) -- this is already proving increasingly valuable. The smartest spies know encryption is coming -- and that they risk being on the wrong side of the argument if they oppose it, as the public increasingly understands its value in protecting their data from a range of malevolent actors like criminals and foreign hackers. The spread may mean spies have a lean period as existing intelligence flows do, in fact, go dark. But history suggests that if they are as smart in the future as they have been in the past, then they will find new ways to do their job.

We can crack encryptions now, “Going Dark” not an issue – local information, metadata, and new databases are happening now

Swire July 15th

(Peter Swire is the Huang professor of law and ethics at the Georgia Institute of Technology, senior counsel with Alston & Bird LLP, and a cyber-fellow with New America, Slate Magazine, “The Golden Age of Surveillance”, http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html, TMP)

In recent months, law enforcement, led by FBI Director James Comey, has waged war against the “going dark” problem—criminals using secure communications technologies, particularly encryption, to evade justice. Its solution to this problem is to encourage or require technology

companies to build in back doors to allow the government to circumvent, say, encryption on your iPhone. But in reality, we are currently in a golden age of surveillance. The “going dark” argument should not be used as a reason to support back doors or other special access by law enforcement to encrypted communications.¹ Last Wednesday I had the privilege of testifying before the Senate Judiciary Committee on the balance between public safety and encryption. I have been researching and writing on encryption for two decades, including serving on President Obama’s Review Group on Intelligence and Communications Technology. My testimony stressed three arguments. First, I agree that law there are indeed specific ways that enforcement and national security agencies lose specific previous capabilities due to changing encryption technology. These specific losses, however, are more than offset by massive gains, including: **(1)** location information; **(2)** information about contacts and confederates; and **(3)** an array of new databases that create digital dossiers about individuals’ lives.² The adoption in the past 20 years of text messaging, an area highlighted by law enforcement as an example of “going dark,” specifically shows enormous gains to law enforcement. Although relatively few text messages were sent 20 years ago, by 2010 the number exceeded 6 trillion texts per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the metadata.³ Being able to access texts and other metadata is enormously helpful in mapping the social graphs of suspects. Before we all communicated online, most of our social interactions (except our phone calls) left no records, and the content of communications left no trace unless law enforcement happened to have an active wiretap on a phone call. Today, however, metadata leaves traces of every electronic communication a suspect has, showing whom they speak to, how often, how long, and from where. Identifying these other confederates gives law enforcement the opportunity to use a number of other tools to access encrypted content, ranging from confidential informants, to surveillance on the co-conspirators, to offering immunity to one participant to gain access to the content of communications with the others.⁴ Law enforcement has expressed particular concern about encrypted text messaging services, such as WhatsApp. For text messages, it might be tempting to say that law enforcement could call the glass half empty (some texts are encrypted) or half full (some texts are in the clear). With more than 6 trillion messages filling the cup, though, it takes chutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.⁵ Second, government-mandated vulnerabilities would threaten severe harm to cybersecurity, privacy, human rights, and U.S. technological leadership while not preventing effective encryption by adversaries. As occurred in the 1990s, a diverse coalition of cybersecurity experts, technology companies, privacy experts, human rights activists, and others has expressed vociferous and united opposition to government-mandated encryption vulnerabilities. These concerns include:⁶ Technology companies, even before Edward Snowden, had multiple reasons to deploy strong encryption to enhance cybersecurity and customer trust. The ongoing development of encryption should thus not be seen primarily as a short-term response to Snowden’s revelations.⁷ Overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption.⁸ U.S. government support for encryption vulnerabilities increases cybersecurity problems in the “least trusted countries” and globally, and undermines U.S. human rights policies. The United States should be a strong example for cybersecurity and human rights, rather than an excuse used by repressive regimes to surveil U.S.-based businesses and individuals and clamp down on political dissent.⁹ Mandated vulnerabilities are bad industrial policy—they threaten U.S. technological leadership without preventing bad actors from using strong encryption.¹⁰ An impressive new technical study by a group of experts was released on July 6 just before the hearing, titled “Keys Under Doormats:

Mandating Insecurity by Requiring Government Access to All Data and Communications.” The new study highlights three general problems. Providing mandated access “would force a U-turn from the best practices now being deployed to make the Internet more secure.” Furthermore, building in exceptional access would substantially increase system complexity, “making security testing difficult and less effective.” Finally, exceptional access would create concentrated targets for bad actors: “Recent attacks on the United States Government Office of Personnel Management show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities.”¶ One might perhaps wonder whether the technical experts are stretching a point by making such definitive statements. Based on my two decades of work on these issues, the technical experts say the same things in private as are written in blue ribbon reports. The passion that the most eminent technical experts show here is due to their conviction based on hard-fought experience, and not a lobbying ploy.¶ Third, the Review Group on Intelligence and Communications Technology report, released in December 2013, unanimously and clearly recommended that the U.S. government vigorously encourage the use of strong encryption, stating:¶ We recommend that, regarding encryption, the US Government should:(1) fully support and not undermine efforts to create encryption standards;¶ (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and¶ (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.¶ With full awareness of the “going dark” concerns, we sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administrationwide scrutiny. Based on the top-secret briefings and our experience, we found these policies would best fight cybercrime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.¶ At heart, providing access exceptions for U.S. law enforcement and intelligence agencies will be harmful, rather than helpful, to national security. The inability to directly access the content of a small fraction of these communications does not warrant the subsequent damage that would result to privacy and to U.S. economic, diplomatic, and security interests.¶ Special thanks to Justin Hemmings for assistance with this project.This article is part of Future Tense, a collaboration among Arizona State University, New America, and Slate. Future Tense explores the ways emerging technologies affect society, policy, and culture. To read more, visit the Future Tense blog and the Future Tense home page. You can also follow us on Twitter.

FT false positives (hay stack/puzzle)

False positives are wrong – meta-data eliminates scenarios and increases efficiency

Lewis 14 [James Andrew Lewis, Director and Senior Fellow of the Technology and Public Policy Program at the CSIS, December 2014, "Underestimating Risk in the Surveillance Debate", Center for Strategic and International Studies,

http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf, pg 2 jf]

NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but **assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence.**

Intelligence does not work as it is portrayed in films—solitary agents do not

make startling discoveries that lead to dramatic, last-minute success. **Success is the product of the efforts of teams** of

dedicated individuals **from many agencies**, using many tools and techniques, **working together to assemble**

fragments of data from many sources into a coherent picture. In practice, **analysts must**

simultaneously explore many possible scenarios. A collection program contributes by not

only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 **domestic** bulk

telephony **metadata program provided information that allowed analysts to rule out some**

scenarios and suspects. The consensus view from interviews with current and former intelligence officials is that while metadata

collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they

had to give up, it would be 215, but this would not come without an increase in risk. **Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.** Spying on Allies NSA's mass

surveillance programs for counterterrorism were carried out in cooperation with more than 30 countries. Unilateral U.S. collection programs focused on national security problems: nonproliferation, counterintelligence (including Russian covert influence operations in Europe), and arms sales to China. The United States failed to exercise sufficient oversight over intelligence collection, but the objectives set for NSA reflect real security problems for the United States and its allies. The notion that "friends don't spy on friends" is naive. The United States has friends that routinely spy on it and yet are strong security partners. Relations among powerful states are complex and not explained by simple bromides drawn from personal life. The most startling thing about U.S. espionage against Germany was the absence of a strategic calculation of risk and benefit. There are grounds for espionage (what other major power has a former leader on Russia's payroll?), but the benefits were outweighed by the risk to the relationship. The case for spying on Brazil is even weaker. While Brazil is often antagonistic, it poses no risk to national security. If economic intelligence on Brazil is needed, the private sector has

powerful incentives and legitimate means to obtain information and usually has the best data. Risk Is Not Going Away **Broad surveillance of communications is the least intrusive and most effective method for discovering terrorist**

and espionage activity. Many countries have expanded surveillance programs since the 9/11 attacks to detect and prevent terrorist activity,

often in cooperation with other countries, including the United States. **Precise metrics on risk and effectiveness do not**

exist for surveillance, and we are left with conflicting opinions from intelligence officials and civil libertarians as to what makes

counterterrorism successful. Given resurgent authoritarianism and continuing jihad, the new context for the surveillance debate is that **the**

likelihood of attack is increasing. Any legislative change should be viewed through this lens.

FT “New Technology for searches will solve the Terror Disad”

**Aff’s call for a new technology is bad – makes counter-terror less effective.
Branda ‘14**

(et al; JOYCE R. BRANDA, Acting Assistant Attorney General, BRIEF FOR THE APPELLEES - Amicus Brief for Smith v. Obama – before the United States Ninth Circuit Court of Appeals. “Amici” means “friend of the court” and – in this context - is legal reference to the Reporters Committee – October 2nd - <https://www.eff.org/document/governments-smithanswering-brief>)

In addition, the declarations in the record establish that a preliminary injunction against the program, even one limited to telephony metadata about plaintiff, would be burdensome. It would require the government to develop a new capability to segregate metadata associated with plaintiff’s call records from the rest of the information, and remove that metadata from each new batch of metadata received on a daily basis (assuming the government received any in the first place). SER 27. Those tasks could consume considerable resources, and any technological solution could degrade the program’s overall effectiveness by eliminating or cutting off potential call chains that might otherwise reveal connections between individuals associated with terrorist activity. SER 27.

Moreover, requiring the government to refrain from collecting and to destroy records regarding plaintiff’s calls, as her motion for a preliminary injunction requests, SER 2, would be irreversible, and hence is improper preliminary injunctive relief, because it would grant plaintiff full relief on the merits prematurely. See Dorfmann v. Boozer, 414 F.2d 1168, 1173 n.13 (D.C. Cir. 1969).

FT Zero sum

Funding divided between 15+ agencies, not a funding tradeoff

Sahadi 13 (Jeanne Sahadi 13, 6-7-2013, "What the NSA costs taxpayers," CNNMoney, <http://money.cnn.com/2013/06/07/news/economy/nsa-surveillance-cost/> CCC)

As a result, it's impossible to say exactly how much money the NSA is given to conduct its surveillance efforts -- which Americans learned this week has recently included collecting phone call data and monitoring online activities. That's because the NSA, a Defense Department agency created in 1952, falls under the category of a "black" program in the federal budget, a term applied to classified efforts. The NSA is one of at least 15 intelligence agencies, and combined the total U.S. intelligence budget in 2012 was \$75 billion, said Steve Aftergood, director of the government secrecy program at the Federation of American Scientists, a nonpartisan think tank that analyzes national and international security issues. The intelligence budget includes funding for both classified and unclassified activities. Funding for classified programs has tracked the upward trend in defense spending over the past decade, according to an analysis of fiscal year 2012 Defense Department budget request by Todd Harrison of the Center for Strategic and Budgetary Assessments. Aftergood estimates about 14% of the country's total intelligence budget -- or about \$10 billion -- goes to the NSA.

FT Recruitment

NSA recruiting is going extremely well

Libicki et al 14 [Libicki, Martin C., 2014, "Hackers Wanted: An Examination of the Cybersecurity Labor Market," RAND, http://www.rand.org/pubs/research_reports/RR430.html jf]

The NSA is the country's largest and leading employer of cybersecurity professionals. In the face of the current stresses in the market for such professionals, **officials there believe they are doing quite well—fewer than 1 percent of their positions are vacant for any significant length of time,** and **supervisors**, queried after their new hires have been working for six months, **report being very happy with the personnel they get.** NSA also has a very low turnover rate (losing no more to voluntary quits than to retirements). One reason is that it pays attention to senior technical development programs to ensure that employees stay current and engaged.

Yet, to get to that point, our interview indicates that NSA must and does pay a great deal of attention to workforce issues. If not its primary focus, then it is still very high up on the list. Although only 80 people have recruitment as their full-time occupation, another 300 have recruitment as an additional duty, and another 1,500 beyond that are involved in the whole recruitment and employment process. All told, that is a great deal of effort—suggesting, from our perspective, that **the difficulties of finding enough cybersecurity professionals can be largely met if sufficient energy is devoted to the task.**

NSA has outreach into many universities, not simply those designated its Centers of Academic Excellence (CAE),² although it pays attention to supporting cybersecurity curricula development in the CAE schools, as noted. In some cases it has people teaching in schools to encourage potential cybersecurity professionals at the pre-college levels, particularly, for obvious reasons, in the state of Maryland.

For the most part, our interview suggests that the **NSA makes rather than buys cybersecurity professionals.** although its recruitment process is very sensitive to the importance of determining those qualities that predispose people to make good employees. Recruiters also look hard at schools that have a reputation for educating people that go into the military. Fully 80 percent of their hires are entry level, the vast majority of whom have bachelor's degrees. They could conceivably draw deeper by finding particularly talented junior college graduates, but the latter would have to undergo a much longer training program as a result. Furthermore, they are not inclined to look for the brilliant non-degreed hacker.³

NSA has a very intensive internal schooling system, lasting as long as three years for some. This too, would be difficult for other institutions to duplicate. NSA can take advantage not only of its size, but also of its low turnover rate. The latter means that it reaps the benefits of its investments in people rather than seeing the benefits accrue to other organizations after NSA has paid the costs of the training (not least of which is the time that such students spend off the job to be trained). Employers with more turnover may logically deem it not worthwhile investing that much to educate their employees.

In all fairness, **only one organization can be the most prestigious place to work, and for this line of work** (and for this size of organization), **NSA is hard to beat.** It consistently absorbs a third of all Scholarship for Service graduates, as shown in Figure 3.1,4 in part because it has the most job openings but also because **it has a reputation for hiring the best hackers.**

Silicon valley jobs are comparatively a much bigger challenge for NSA recruitment -- the NSA has already had to deal with recruitment issues in the past

Brumfiel, science correspondent for NPR, 3/31/15 (Geoff Brumfiel, NPR, MARCH 31, 2015, "After Snowden, The NSA Faces Recruitment Challenge", <http://www.npr.org/2015/03/31/395829446/after-snowden-the-nsa-faces-recruitment-challenge>, accessed 7/17/15 JH @ DDI)

But Ziring says **there's a much bigger problem:** "I was at a Dartmouth career fair a few months ago," he says, "and our table was right across from Facebook. And we are looking for some of the

same things that they are." Ever since the Snowden leaks, cybersecurity has been hot in Silicon Valley. In part that's because the industry no longer trusts the government as much as it once did. Companies want to develop their own security, and they're willing to pay top dollar to get the same people the NSA is trying to recruit. Students like Swann. Last summer Microsoft paid him \$7,000 a month to work as an intern. The company even rented him a car. "It was actually really nice," Swann says. "It was a Subaru Legacy." Ziring says the agency can't compete on money, so he tries to sell it in other ways: "You know we have good health benefits, and we're government, right? So we have a huge scope of insurance to choose from," he says.

FT Targeted Surveillance Turn

Metadata is necessary and targeted searches prevent the ability to identify networks and halt terrorist activities

Posner, 8. [Richard A., Judge, United States Court of Appeals for the Seventh Circuit; Senior Lecturer in Law, The University of Chicago. "Privacy, Surveillance, and Law," 75 University of Chicago Law Review 245, http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2808&context=journal_articles.

What is most notable about the amendments, as indeed of the Terrorist Surveillance Program to which they seem addressed, is their backing away from reliance on warrants to prevent abuses of electronic surveillance. The warrant is a poorly designed means for balancing the security and liberty interests involved in counterterrorist surveillance. It is true that instead of requiring probable cause to believe that the target of an interception is a terrorist, FISA could be amended to require merely reasonable suspicion. But even that would be too restrictive from the standpoint of effective counterterrorism; effective surveillance cannot be confined to suspected terrorists when the object is to discover who may be engaged in terrorism or ancillary activities. Further attenuation of FISA's standard for obtaining a warrant might be possible without running afoul of the Fourth Amendment. Conceivably the issuance of a warrant could be authorized on the basis of a showing that while the target was probably not a terrorist, national security required making assurance doubly sure by intercepting some of his electronic communications. A model might be the criterion for issuing a search warrant to the Canadian Security Intelligence Service, where a warrant can be issued on the basis of a factually supported "belief, on reasonable grounds, that [it] ... is required to enable the Service to investigate a threat to the security of Canada." 9 Such a criterion might pass muster under the Fourth Amendment, which requires probable cause for the issuance of a warrant but does not state what it is that there must be probable cause to believe. The Supreme Court has said that there must be probable cause to believe that the search will yield contraband or evidence of crime when the search is part of a criminal investigation." The Constitution binds the government more tightly when it is exerting its powers to convict people of crimes than in other areas of government activity. A search intended not to obtain evidence of crime but to obtain information about terrorism might, as under Canadian law, require only probable cause to believe that the search would yield such information. The lower the standard for getting a warrant, however, the more porous the filter that the requirement of a warrant creates, bearing in mind the ex parte character of a warrant proceeding. If all the application need state is that an interception might yield data having value as intelligence, judges would have no basis for refusing to issue the warrant. Alternatively, reliance on warrants could invite legislation to expand the reach of the criminal laws relating to terrorism in order to make it easier to establish probable cause to believe that a search will reveal evidence of a crime. That expansion could raise issues under the First Amendment, since the natural route for expanding criminal laws against terrorism is to criminalize extremist speech or even attendance at extremist (though peaceful) speeches and rallies, as activities that may be preparatory to or encouraging of terrorism. Warrants that satisfy FISA's standard as traditionally understood should continue to be required for all physical searches, because they are far greater intrusions on privacy than electronic interceptions, and for all electronic surveillance for which FISA's existing probable cause requirement can reasonably be satisfied (mainly cases in which the government wanted to intercept communications of a person who they had probable cause to believe was a terrorist). With these exceptions, civil libertarians' preoccupation with warrants is not only harmful to national security (and possibly to civil liberties if it induces legislation to expand the reach of the criminal law) but also anachronistic. The government's ready access to the vast databases that private and public entities compile for purposes unrelated to national security has enabled it to circumvent much of the protection of privacy that civil libertarians look to warrant requirements to secure. There are a number of possible measures, apart from requiring warrants, that Congress could adopt in order to minimize abuses of domestic surveillance. If all were adopted, the risk of such abuses would be slight. The temporary FISA amendments take tiny steps in this direction. Bolder steps would include the following: 1. Congress could create a steering committee for national security electronic surveillance, composed of the attorney general, the director of national intelligence, the secretary of homeland security, and a retired federal judge or justice appointed by the chief justice of the Supreme Court. The committee would monitor all such surveillance to assure compliance with the Constitution and federal statutes. The requirement in the temporary amendments that the attorney general and the director of national intelligence devise procedures for a new warrantless surveillance program is one of the tiny steps to which I referred." The other, and legally dubious one, is requiring submission of the procedures for approval by the Foreign Intelligence Surveillance Court; that court becomes in effect the steering committee. 2. The NSA could be required to submit to the steering committee, to departmental inspectors general, to the Privacy and Civil Liberties Oversight Board (a White House agency created by the

Intelligence Reform Act), to the congressional intelligence and judiciary committees, and to an independent watchdog agency of Congress modeled on the GAO every six months a list of the names and other identifying information of all persons whose communications had been intercepted in the previous six months without a warrant, with a brief statement of why these persons had been targeted. 3. The responsible officials of the NSA could be required to certify annually to the watchdog groups that there had been no violations of the statute during the preceding year. False certification would be punishable as perjury. But lawsuits challenging the legality of the Terrorist Surveillance Program should be precluded. Such lawsuits would distract officials from their important duties to no purpose if the kind of statute that I am suggesting were enacted. The statute should sunset after five years. 4. The use of intercepted information for any purpose other than investigating threats to national security would be forbidden. Information could not be used as evidence or leads in a prosecution for ordinary crime-this to alleviate concern that wild talk bound to be picked up by electronic surveillance would lead to criminal investigations unrelated to national security. Violations of this provision would be made felonies punishable by substantial prison sentences and heavy fines. But the punishments must not be made too severe lest they cause intelligence officers to steer so far clear of possible illegality that they fail to conduct effective surveillance. The risk of abuses is not great enough to justify savage penalties in order to deter them, because intelligence officers have no interest in assisting in the enforcement of criminal laws unrelated to national security. A neglected point is that violations of privacy and civil liberties tend to emanate from the White House and the top management level of executive branch agencies rather than from the working or middle-management levels. 5. To limit the scope of surveillance, "threats to national security" should be narrowly defined as threats involving a potential for mass deaths or catastrophic damage to property or to the economy. That would exclude, for the time being anyway, ecoterrorism, animal-rights terrorism, and other political violence that, though criminal, does not threaten catastrophic harm (yet). Congressional action is also needed to protect the phone companies that cooperated with the NSA's surveillance program from potentially immense liability for allegedly having violated federal law protecting the privacy of telephone records; a number of suits are pending. The intelligence system is enormously dependent on informal assistance from private companies in communications, banking, and other industries. At times such assistance is made a legal duty, as in the federal law requiring banks to report cash transactions of \$10,000 or more; and this is also a feature of the new amendments to FISA. Were it not for the threat of liability, which the amendments do not address, voluntary assistance would probably as in the past be all the government needed. But if voluntary assistance-even when tendered in a national emergency, as in the wake of the 9/11 terrorist attacks- places companies in legal jeopardy, such assistance will dry up. FISA needs to be amended not only to authorize more extensive domestic surveillance than its anachronistic terms permit but also to insulate from liability conduct that may have violated the Act or some other statute but that would be permitted under the amended regime. Until the temporary amendments were enacted, the type of approach that I am advocating (call it the "nonwarrant" approach) for regularizing domestic surveillance was getting little attention from Congress and the Bush Administration, possibly because the Administration wanted to retain a completely free hand and thought it could fend off the sort of restrictions that I have sketched. (It is remarkable how tepid the public reaction to the Terrorist Surveillance Program has been.) A related possibility is that the Administration's aggressive claims of presidential power prevented it from acknowledging the legitimacy of congressional controls over intelligence and hence of a legislative solution to the controversy over the program. Still another possibility was (and is) that because no one is in charge of domestic intelligence, authority over which is divided among the attorney general, the FBI director, the Department of Homeland Security, and the director of national intelligence (among others), no one is formulating a comprehensive legislative and public relations strategy for ending the controversy over the role of electronic surveillance in such intelligence. (At this writing, the only confirmed senior official in the Justice Department is the solicitor general.) And another possibility is the grip of our legalistic culture, which makes us think that the regulation of national security must be modeled on the regulation of criminal law enforcement. The temporary amendments suggest, however, that the logjam may be breaking, though one of the reasons, it appears, is that the Administration's decision to bring the Terrorist Surveillance Program under FISA resulted in a paper jam at the Foreign Intelligence Surveillance Court as the number of warrant applications soared. We should be playing to our strengths, and one of the greatest of them is technology. We may not be able to prevail against terrorism with one hand tied behind our back. Critics of surveillance argue that since our enemies know that we monitor electronic communications, they will foil us by simply ceasing to use such communications. That is wrong. We know it is wrong because we do intercept terrorist communications. 24 But if it were true that our monitoring caused the terrorists to abandon the telephone and the internet, that would be an enormous victory for counterterrorism, as it is extremely difficult to coordinate and execute a major terrorist attack if all communications among the plotters must be face to face to avoid detection. The greater danger is that encryption and other relatively

cheap and simple countermeasures will defeat our surveillance. Opponents of efforts to amend FISA point out that the Foreign Intelligence Surveillance Court has almost never turned down an application for a warrant. In 2005, for example, although more than 2,000 applications were filed, not a single one was denied in whole or in part. 5 The inference the critics wish drawn is that FISA is not inhibiting surveillance. The correct inference is that the Justice Department is too conservative in seeking warrants. The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time. The effect of our legalistic culture is to cause law enforcement agencies, notably the FBI, to avoid not only violating the law but also steering so close to the wind that they might be accused, albeit groundlessly, of violating the law or of being "insensitive" to values that inform the law, even when those values have not been enacted into law.

No replacement for Metadata

Sessions 15 [Jeff, U.S. Senator, May 20, “Why Should Terrorists Be Harder to Investigate than Routine Criminals?”<http://www.nationalreview.com/article/418675/why-should-terrorists-be-harder-investigate-routine-criminals-jeff-sessions>]

The 9/11 attacks exposed the dangerous wall separating the intelligence and law-enforcement communities. In response, Congress developed a number of tools to eliminate those barriers so that critical information could be timely and appropriately shared to address radical Islamic terrorism. Among them was Section 215 of the USA Patriot Act. In 2006, the National Security Agency transitioned the bulk telephone-metadata acquisition program authorized under the president’s Terrorist Surveillance Program to the business-records court-order authority of Section 215. Since shortly after 9/11, this program has been helping to keep Americans safe by acquiring non-content call records, i.e., telephone numbers and the date, time, and duration of a call. This program has yielded invaluable intelligence that has helped prevent attacks and uncovered terrorist plots. Nevertheless, the Obama administration has built up unnecessary barriers that sacrifice the fragile operational efficiency of the program without actually accomplishing anything in terms of data security. Meanwhile, the threat level has only increased. On the heels of an ISIS-inspired attack in Texas, the administration has greatly increased security at military bases, airports, railroads, and other potential targets. Just this year, the FBI has so far arrested at least 30 Americans for planning ISIS-inspired attacks in the U.S. FBI director James Comey recently issued this chilling warning: The siren song sits in the pockets, on the mobile phones, of the people who are followers [of ISIS] on Twitter . . . It’s almost as if there’s a devil sitting on the shoulder, saying “Kill! Kill! Kill! Kill!” all day long. Most people would agree it should not be more difficult to investigate a terrorist plot than check fraud. As the National Academy of Sciences noted in its recent report, Section 215 of the Patriot Act simply “allow[s] the [Foreign Intelligence Surveillance Court] to require production of documents and other tangible things determined relevant to national security investigations, much like other courts do in criminal and grand jury investigations.” But unlike in the criminal context, Section 215 is subject to extraordinary oversight by the Executive and Judicial branches, as well as minimization procedures to protect Americans’ civil liberties. Moreover, information acquired under Section 215 can be accessed by only a limited number of trained intelligence professionals and only after the government has demonstrated to the court that there is a reasonable, articulable suspicion that a number or identifier is associated with a specific foreign-terrorist organization. Compare this with how a local district attorney can obtain the same type of information in a routine criminal case. He issues a grand-jury subpoena for phone records, which requires only a showing that the records are relevant to an investigation. The subpoena could require the production of much more detailed information than is acquired under Section 215, such as names and addresses of the callers. Indeed, the U.S. Drug Enforcement Agency and Internal Revenue Service can obtain telephone call records and bank records with an administrative subpoena without even a prosecutor’s approval, much less approval by a judge. The Supreme Court has long held this process constitutional under the Fourth Amendment because such information is already in the hands of a third-party — the phone companies — and therefore, a customer has no reasonable expectation of privacy in that information. But legislation known as the USA Freedom Act would prevent our intelligence officers from obtaining information in this manner at all. As former federal judge and attorney general Michael Mukasey said: The bill’s imposition of the warrant requirement on the NSA would be more burdensome than what any assistant U.S. attorney must do to get metadata in a routine criminal case, which is simply to aver that the information is needed in connection with a criminal investigation — period. The bill would also eliminate entirely the database through which the NSA is able to quickly access information to “connect the dots” in order to prevent terror attacks. This is significant because, as the National Academy of Sciences explained, in contrast to domestic law enforcement . . . the world of intelligence analysis has many fewer tools available for investigation. In hostile foreign environments, personal interviews and observations and records review are much more limited. Accordingly, the role of bulk data as a

way to understand the significance of past events is important, and the loss of this tool becomes more serious. Instead, the USA Freedom Act relies on a nonexistent, untested system and the hope that private companies will agree to retain records long enough for the NSA to obtain data when it may be critical to preventing an imminent attack. But as the National Academy of Sciences noted, “there is no technological magic . . . that will fully substitute for bulk collection” and service providers “have no incentive to cooperate, even if paid; indeed, their customers may object to such cooperation.” Moreover, requiring the government to obtain a court order every time it seeks to search data held by private companies would significantly delay investigations, giving terrorists a substantial operational advantage. In short, the USA Freedom Act would make it vastly more difficult for the NSA to stop a terrorist than it is to stop a tax cheat. Why make it much harder to investigate terrorists than common criminals?

FT Perception Turn

The plan is perceived as weakness – invites attacks

Daily Mail 15. “Head of CIA warns that US is at risk of lone wolf terror attack after NSA powers to monitor all phone calls expired – as Isis ‘watch carefully’ for security gaps,” 5-31-2015, <http://www.dailymail.co.uk/news/article-3105089/Senate-makes-ditch-bid-extend-NSA-s-bulk-collection-phone-records-Rand-Paul-swears-block-legislation-let-Patriot-Act-expire.html>.

The head of the CIA has warned that Americans are now at risk after the Senate was unable to extend laws giving authorities special powers to fight terrorists.¶ Politicians in the upper house were unable to come to an agreement to extend key parts of the Patriot Act - that legalize controversial methods of surveillance by the National Security Agency (NSA) - which expired on Sunday.¶ Attempts were frustrated by Presidential candidate Rand Paul, who has taken a firm stance against the extension of powers allowing the mass collection of phone records, wire taps and warrants without evidence.¶ But the Head of the CIA John Brennan claims ordinary Americans, who expect the NSA to do their jobs, have been put at risk by 'political grandstanding and crusading for ideological causes' that fueled the debate.¶ Speaking on CBS show Face The Nation, he warned that the US - and Europe - is now in danger from technologically 'sophisticated' terrorists who are watching developments carefully and 'looking for the seams to operate' within.¶ He claimed that the authorities do not abuse the powers, extended in 2011 to help fight lone wolf terror suspects not connected to a specific group, and that without them, it's difficult for the NSA to protect America.¶ Mr Brennan said: 'I think terrorist elements have watched very carefully what has happened here in the United States, whether or not it's disclosures of classified information or whether it's changes in the law and policies. They are looking for the seams to operate within.'¶ And this is something that we can't afford to do right now, because if you look at the horrific terrorist attacks and violence that is being perpetrated around the globe, we need to keep our country safe. And our oceans are not keeping us safe the way they did a century ago.¶ The Patriot Act was passed in 2001 in the wake of the 9/11 terror attacks. Now that the provisions have expired, government agents will need to subpoena phone companies for the records.¶ The White House previously justified collecting the records because of the Patriot Act's Section 215, which expired on Sunday.¶ Two other provisions, added in 2011, also expired with it. The first is a 'roving wiretap' provision which allows government agencies to keep tracking suspects as they switch devices.¶ The second is a 'lone wolf' clause which allows warrants to be granted without any evidence linking a suspect to a foreign power or terrorist group.¶ Political struggles over the NSA and its data collection have become a national issue since whistleblower Edward Snowden revealed the extent of government programs in 2013. ¶ The senate's efforts to pass a replacement bill were frustrated by Kentucky's junior senator Rand Paul, who has spoken at length against the NSA's activities, which he has excoriated as illegal and unconstitutional.¶ Paul, a Republican who is running for president, came up against members of his own party, as well as the Obama administration.¶ With his presidential campaign waning, he has been accused of irresponsible political opportunism by opponents, by fighting a bill on ideological grounds that may put ordinary people at risk.¶ He was criticized by the White House Sunday night, which called the Patriot Act expiration an 'irresponsible lapse'. ¶ While Brennan didn't mention Paul by name, he said on Face The Nation: 'Unfortunately I think there is a little too much political grandstanding and crusading for ideological causes that have really fuelled the debate on this issue.'¶ He added: 'These are authorities that have been used by the government to make sure that we're able to safeguard Americans. And the sad irony is that most Americans expect the government to protect them. And so although there's a lot of debate that goes on, on the Congress and the Hill on this issue, I think, when you go out to Boise or Tampa or Louisville, Americans are expecting their law enforcement and homeland security and intelligence professionals to do their work. And these authorities are important.' ¶ Paul argued 'there must be another way' but even he agrees that the lapse in these powers are likely to be temporary as politicians work on the USA Freedom Act, which is expected to pass within the next week.¶ Republican Senate Majority Leader Mitch McConnell called a rare Sunday session to try to pass the replacement law, but was unable to push it through in time.¶ And although the replacement is set to pass this week, Paul said the expiration was 'a victory no matter how you look at it'. ¶ In a statement, he said: 'It might be short lived, but I hope that it provides a road for a robust debate, which will strengthen our intelligence community, while also respecting our Constitution.'¶ He added: 'The expiration of the NSA's sweeping, all-encompassing and ineffectual powers will not relinquish functions necessary for protecting national security. The expiration will instead do what we should have done all along - rely on the Constitution for these powers.'¶ According to a top lawmaker, as of 8pm Sunday no NSA employee could access their enormous phone records database, which holds metadata on millions of phone conversations handed over by telecoms companies like Verizon and AT&T.¶ Senate Intelligence Committee chairman Richard Burr said on Sunday: 'There is no way to get any type of agreement tonight -- either an extension or passage of a bill. So at 8pm tonight, NSA employees can not query the database'. ¶ In a statement issued Sunday night, Obama's press secretary Josh Earnest, urged action to pass the USA Freedom Act as quickly as possible.¶ He said: 'The Senate took an important - if late - step forward tonight. We call on the Senate to ensure this irresponsible lapse in authorities is as short-lived as possible.'¶ On a matter as critical as our national security, individual Senators must put aside their partisan motivations and act swiftly. The American people deserve nothing less.¶ Some lawmakers have said the lapse raises

alarming questions about how US authorities can keep the homeland safe with a diminished security toolbox.¶ 'I think it's very very unfortunate that we're in this position,' said Senator Mike Lee, a conservative Republican who supports the reform bill.¶ 'We've known this date was coming for four years. Four years. And I think it's inexcusable that we adjourned' for a weeklong break last week without resolving the issue.¶ Lee, too, conceded that the reform bill would most likely pass in the coming week.¶ With the clock ticking, CIA chief John Brennan warned Sunday that allowing vital surveillance programs to lapse could increase terror threats, and argued that the phone metadata dragnet has not abused civil liberties and only serves to safeguard citizens.¶ 'This is something that we can't afford to do right now,' Brennan said of allowing the counterterrorism provisions to expire.¶ 'Because if you look at the horrific terrorist attacks and violence being perpetrated around the globe, we need to keep our country safe, and our oceans are not keeping us safe the way they did century ago,' he said on CBS talk show Face the Nation.¶ Brennan added that online threats from groups like Isis would continue to grow over the next five to ten years. He said: 'Isis has been very sophisticated and adept at using the Internet to propagate its message and reach out to individuals. We see what is happening as far as thousands upon thousands of individuals, including many thousands from the West, that have traveled into Syria and Iraq. And a number of these individuals are traveling back.¶ And what we see, they're also using the Internet as a way to incite and encourage individuals to carry out acts of violence.¶ 'So as the director of FBI says, you know, this use of these websites and their Internet capabilities is something of great concern. So yes, I think ISIS is a threat not just in the Middle East and South Asia and African regions but also to Europe as well as to the United States.'

NSA programs are reasonable, legal, and key to stopping the rising terrorist threat

Bolton 4/28/15 (John R. Bolton, former U.S. permanent representative to the United Nations, "NSA activities key to terrorism fight", 4/28/15, <http://www.aei.org/publication/nsa-activities-key-to-terrorism-fight/>) -LL

Congress is poised to decide whether to re-authorize programs run by the National Security Agency that assess patterns of domestic and international telephone calls and emails to uncover linkages with known terrorists. These NSA activities, initiated after al-Qaeda's deadly 9/11 attacks, have played a vital role in protecting America and our citizens around the world from the still-metastasizing terrorist threat. The NSA programs do not involve listening to or reading conversations, but rather seek to detect communications networks. If patterns are found, and more detailed investigation seems warranted, then NSA or other federal authorities, consistent with the Fourth Amendment's prohibition against unreasonable searches and seizures, must obtain judicial approval for more specific investigations. Indeed, even the collection of the so-called metadata is surrounded by procedural protections to prevent spying on U.S. citizens. Nonetheless, critics from the right and left have attacked the NSA for infringing on the legitimate expectations of privacy Americans enjoy under our Constitution. Unfortunately, many of these critics have absolutely no idea what they are talking about; they are engaging in classic McCarthyite tactics, hoping to score political points with a public justifiably worried about the abuses of power characteristic of the Obama administration. Other critics, following Vietnam-era antipathies to America's intelligence community, have never reconciled themselves to the need for robust clandestine capabilities. Still others yearn for simpler times, embodying Secretary of State Henry Stimson's famous comment that "gentlemen don't read each others' mail." The ill-informed nature of the debate has facilitated scare-mongering, with one wild accusation about NSA's activities after another being launched before the mundane reality catches up. And there is an important asymmetry at work here as well. The critics can say whatever their imaginations conjure up, but NSA and its defenders are significantly limited in how they can respond. By definition, the programs' success rests on the secrecy fundamental to all intelligence activities. Frequently, therefore, explaining what is not happening could well reveal information about NSA's methods and capabilities that

terrorists and others, in turn, could use to stymie future detection efforts. After six years of President Obama, however, trust in government is in short supply. It is more than a little ironic that Obama finds himself defending the NSA (albeit with obvious hesitancy and discomfort), since his approach to foreign and defense issues has consistently reflected near-total indifference, except when he has no alternative to confronting challenges to our security. Yet if harsh international realities can penetrate even Obama's White House, that alone is evidence of the seriousness of the threats America faces. In fact, just in the year since Congress last considered the NSA programs, the global terrorist threat has dramatically increased. ISIS is carving out an entirely new state from what used to be Syria and Iraq, which no longer exist within the borders created from the former Ottoman Empire after World War I. In already-chaotic Libya, ISIS has grown rapidly, eclipsing al-Qaeda there and across the region as the largest terrorist threat. Boko Haram is expanding beyond Nigeria, declaring its own caliphate, even while pledging allegiance to ISIS. Yemen has descended into chaos, following Libya's pattern, and Iran has expanded support for the terrorist Houthi coalition. Afghanistan is likely to fall back under Taliban control if, as Obama continually reaffirms, he withdraws all American troops before the end of 2016. This is not the time to cripple our intelligence-gathering capabilities against the rising terrorist threat. Congress should unquestionably reauthorize the NSA programs, but only for three years. That would take us into a new presidency, hopefully one that inspires more confidence, where a calmer, more sensible debate can take place.

Aggressive anti-terrorism creates a new security paradigm – hardens the public to government intrusions – scaling back surveillance eliminates that paradigm and creates vulnerability

Givens 13 -- Austen D. Givens is a PhD student in the Department of Political Economy at King's College London. His forthcoming book with Nathan E. Busch, The Business of Counterterrorism: Public-Private Partnerships in Homeland Security, will be published by Peter Lang. [“The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws”](#)
<http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/>

The ratchet effect can occur because anti-terrorism laws create a new security paradigm. An aggressive anti-terrorism law can fundamentally alter societal approaches to terrorism. Surveillance may increase. Police powers can expand. Intelligence efforts may grow. Public expectations of privacy can diminish. In the aggregate, these types of changes can represent a drastic change in a government's approach to terrorism, and effectively create a “new normal” level of security. Because this “new normal” is linked to the law itself, reversing the law begins to dismantle the new security paradigm. From the public's perspective, this might be an unacceptable option because it may increase societal vulnerability to terrorism. Government agencies also risk losing resources—personnel, money, and political support—by returning to the status quo ante.

Violent war on terror is the only way to win – history proves non-violent strategies fail

Hanson 10 – senior fellow @ Hoover Institute

Victor, “The Tragic Truth of War” [<http://www.nationalreview.com/node/229152/print>] February 17 //mtc

Victory has usually been defined throughout the ages as forcing the enemy to accept certain political objectives. “Forcing” usually meant killing, capturing, or wounding men at arms. In

today's polite and politically correct society we seem to have forgotten that nasty but eternal truth in the confusing struggle to defeat radical Islamic terrorism. What stopped the imperial German army from absorbing France in World War I and eventually made the Kaiser abdicate was the destruction of a once magnificent army on the Western front — superb soldiers and expertise that could not easily be replaced. Saddam Hussein left Kuwait in 1991 when he realized that the U.S. military was destroying his very army. Even the North Vietnamese agreed to a peace settlement in 1973, given their past horrific losses on the ground and the promise that American air power could continue indefinitely inflicting its damage on the North. When an enemy finally gives up, it is for a combination of reasons — material losses, economic hardship, loss of territory, erosion of civilian morale, fright, mental exhaustion, internal strife. But we forget that central to a concession of defeat is often the loss of the nation's soldiers — or even the threat of such deaths. A central theme in most of the memoirs of high-ranking officers of the Third Reich is the attrition of their best warriors. In other words, among all the multifarious reasons why Nazi Germany was defeated, perhaps the key was that hundreds of thousands of its best aviators, U-boaters, panzers, infantrymen, and officers, who swept to victory throughout 1939–41, simply perished in the fighting and were no longer around to stop the allies from doing pretty much what they wanted by 1944–45. After Stalingrad and Kursk, there were not enough good German soldiers to stop the Red Army. Even the introduction of jets could not save Hitler in 1945 — given that British and American airmen had killed thousands of Luftwaffe pilots between 1939 and 1943. After the near destruction of the Grand Army in Russia in 1812, even Napoleon's genius could not restore his European empire. Serial and massive Communist offensives between November 1950 and April 1951 in Korea cost Red China hundreds of thousands of its crack infantry — and ensured that, for all its aggressive talk, it would never retake Seoul in 1952–53. But aren't these cherry-picked examples from conventional wars of the past that have no relevance to the present age of limited conflict, terrorism, and insurgency where ideology reigns? Not really. We don't quite know all the factors that contributed to the amazing success of the American "surge" in Iraq in 2007–08. Surely a number of considerations played a part: Iraqi anger at the brutish nature of al-Qaeda terrorists in their midst; increased oil prices that brought massive new revenues into the country; General Petraeus's inspired counterinsurgency tactics that helped win over Iraqis to our side by providing them with jobs and security; much-improved American equipment; and the addition of 30,000 more American troops. But what is unspoken is also the sheer cumulative number of al-Qaeda and other Islamic terrorists that the U.S. military killed or wounded between 2003 and 2008 in firefights from Fallujah to Basra. There has never been reported an approximate figure of such enemy dead — perhaps wisely, in the post-Vietnam age of repugnance at "body counts" and the need to create a positive media image. Nevertheless, in those combat operations, the marines and army not only proved that to meet them in battle was a near death sentence, but also killed thousands of low-level terrorists and hundreds of top-ranking operatives who otherwise would have continued to harm Iraqi civilians and American soldiers. Is Iraq relatively quiet today because many who made it so violent are no longer around? Contemporary conventional wisdom tries to persuade us that there is no such thing as a finite number of the enemy. Instead, killing them supposedly only incites others to step up from the shadows to take their places. Violence begets violence. It is counterproductive, and creates an endless succession of the enemy. Or so we are told. We may wish that were true. But military history suggests it is not quite accurate. In fact, there was a finite number of SS diehards and kamikaze suicide bombers even in fanatical Nazi Germany and imperial Japan. When they were attrited, not only were their acts of terror curtailed, but it turned out that far fewer than expected wanted to follow the dead to martyrdom. The Israeli war in Gaza is considered by the global community to be a terrible failure — even

though the number of rocket attacks against Israeli border towns is way down. That reduction may be due to international pressure, diplomacy, and Israeli goodwill shipments of food and fuel to Gaza — or it may be due to the hundreds of Hamas killers and rocketeers who died, and the thousands who do not wish to follow them, despite their frequently loud rhetoric about a desire for martyrdom.⁴ Insurgencies, of course, are complex operations, but in general even they are not immune from eternal rules of war. Winning hearts and minds is essential; providing security for the populace is crucial; improving the economy is critical to securing the peace. But all that said, we cannot avoid the pesky truth that in war — any sort of war — killing enemy soldiers stops the violence. For all the much-celebrated counterinsurgency tactics in Afghanistan, note that we are currently in an offensive in Helmand province to “secure the area.” That means killing the Taliban and their supporters, and convincing others that they will meet a violent fate if they continue their opposition.⁵ Perhaps the most politically incorrect and Neanderthal of all thoughts would be that the American military’s long efforts in both Afghanistan and Iraq to kill or capture radical Islamists has contributed to the general safety inside the United States. Modern dogma insists that our presence in those two Muslim countries incited otherwise non-belligerent young Muslims to suddenly prefer violence and leave Saudi Arabia, Yemen, or Egypt to flock to kill the infidel invader.⁶ A more tragic view would counter that there was always a large (though largely finite) number of radical jihadists who, even before 9/11, wished to kill Americans. They went to those two theaters, fought, died, and were therefore not able to conduct as many terrorist operations as they otherwise would have, and also provided a clear example to would-be followers not to emulate their various short careers. That may explain why in global polls the popularity both of bin Laden and of the tactic of suicide bombing plummeted in the Middle Eastern street — at precisely the time America was being battered in the elite international press for the Iraq War.⁷ Even the most utopian and idealistic do not escape these tragic eternal laws of war. Barack Obama may think he can win over the radical Islamic world — or at least convince the more moderate Muslim community to reject jihadism — by means such as his Cairo speech, closing Guantanamo, trying Khalid Sheikh Mohammed in New York, or having General McChrystal emphatically assure the world that killing Taliban and al-Qaeda terrorists will not secure Afghanistan.⁸ Of course, such soft- and smart-power approaches have utility in a war so laden with symbolism in an age of globalized communications. But note that Obama has upped the number of combat troops in Afghanistan, and he vastly increased the frequency of Predator-drone assassination missions on the Pakistani border.⁹ Indeed, even as Obama damns Guantanamo and tribunals, he has massively increased the number of targeted assassinations of suspected terrorists — the rationale presumably being either that we are safer with fewer jihadists alive, or that we are warning would-be jihadists that they will end up buried amid the debris of a mud-brick compound, or that it is much easier to kill a suspected terrorist abroad than detain, question, and try a known one in the United States.¹⁰ In any case, the president — immune from criticism from the hard Left, which is angrier about conservative presidents waterboarding known terrorists than liberal ones executing suspected ones — has concluded that one way to win in Afghanistan is to kill as many terrorists and insurgents as possible. And while the global public will praise his kinder, gentler outreach, privately he evidently thinks that we will be safer the more the U.S. marines shoot Taliban terrorists and the more Hellfire missiles blow up al-Qaeda planners.

FT Link Turn – Public/Law Enforcement Cooperation

Poll shows public support PRISM

Logiurato, Business Insider's politics editor, 6/7/13, (Brett, (Degree in International Politics), "The NSA's PRISM Program Is Shockingly Uncontroversial With The American Public" Business Insider, <http://www.businessinsider.com/prism-surveillance-poll-nsa-obama-approval-2013-6>)

President Barack Obama's approval rating is sinking like a stone in a new CNN/ORC poll — but it's not because of Americans' reactions to the National Security Agency surveillance program known as "PRISM." In fact, the public overwhelmingly approves of the program. The poll found that 66 percent of Americans say the Obama administration was right to gather and analyze information from major internet companies to help locate suspected terrorists. Here's the full wording of the question posed in the poll: [F]or the past few years the Obama administration has reportedly been gathering and analyzing information from major internet companies about audio and video chats, photographs, e-mails and documents involving people in other countries in an attempt to locate suspected terrorists. The government reportedly does not target internet usage by U.S. citizens and if such data is collected, it is kept under strict controls. Do you think the Obama administration was right or wrong in gathering and analyzing that internet data? Overall, according to the poll, the public has exhibited a collective shrug to new revelations detailing the scope of the NSA's surveillance efforts. On its collection of phone data, the public is less gung-ho about the program, but still supportive — 51 percent say the Obama administration is right, while 48 percent say it's wrong. Incidentally, partisans on both sides of the aisle are most likely to support the programs. Self-identified Republicans and Democrats approve of both programs, while Independents are much less enthusiastic. They disapprove of the NSA's phone surveillance program by a 40-58 split, and their approval of PRISM (58-41) significantly trails both Republicans (67-31) and Democrats (76-24)

Polls show public supports PRISM's actions

Moseley, 10/6/13 (Tom, (reporter for the Huffington Post), "Please Spy On Us: Poll Finds Public Support For "Snooping" Plans Despite NSA Prism Scandal", Huffington Post, http://www.huffingtonpost.co.uk/2013/06/10/poll-finds-public-support-snooping-plans_n_3415724.html)

A majority of Britons support the government's controversial 'snooping' proposals - despite the growing NSA/Prism data-sharing scandal, an exclusive poll for The Huffington Post UK reveals. And more than four in 10 people think the security services should be able to break data laws in order to prevent terrorism. The first major survey carried out since the leaking of details of the US Prism surveillance programme found that 51% of voters either backed the coalition's draft Communications Data Bill, or thought it did not go far enough. The Bill would allow the security services access to mobile phone and internet records. Civil liberties campaigners had hoped the ongoing data-mining revelations involving Google, Apple and Facebook would serve as a "wake-up call" on the plans. But just 38% of people polled agreed that the Bill "goes too far" and "undermines our privacy". Meanwhile, 42% of people said the police and security agencies should be able to go "beyond the law" to obtain information if it is necessary to fight serious crime and terrorism, while 45% said they should "always obey the law". Foreign Secretary William Hague told MPs it was "baseless" to suggest GCHQ could circumvent UK laws by using personal data gathered by foreign agencies. But 46% would be happy with such a measure, the YouGov poll found. By comparison, 39% said would be "sorry that the UK agencies might be getting round British law to undermine our right to privacy". YouGov President Peter Kellner said the "simmering dispute" over the Communications Data Bill had "roared to life" following the leak, by 29-year-old Edward Snowden. Women were far more likely to back the Bill than men, dividing by almost two to one. However, despite the overall backing for the 'snooping' measures, support was far smaller than for previous civil liberties battlegrounds, 90-day detention and control orders, Kellner said. "These are early days in an argument that may well rumble on for months, even years," he said. "Indeed, the trade-off

between security-driven rules and individual liberty will, and should, be something that we never stop debating." Giving a statement to Parliament on Monday afternoon, Hague said he "deplored" the leaking of US intelligence data that sparked the Prism scandal. And he insisted that any data on British citizens would be "subject to proper UK statutory controls and safeguards". The Foreign Secretary admitted he could not say "everything is definitely perfect at all times" in the way the intelligence services operate, but said he only had praise for the way they work. Counter terror activity reached peak during the 2012 Olympics, he said, and added: "The methods we use to combat these threats have to be secret". Emphasising the importance of the measures to the struggle against terrorism makes political sense, according to YouGov's Kellner: "One thing that is likely to sway public attitudes is evidence that electronic 'snooping' either has, or has not, managed to stop terrorism and/or serious crime."

FT Bruce Schneier

Schneier is wrong about mass surveillance — it's a vital counter-terror tool.

Knee 15 — Jonathan A. Knee, Professor of Professional Practice at Columbia Business School, Senior Adviser at Evercore Partners—a U.S. investment bank, holds a J.D. from Yale Law School and an M.B.A. from the Stanford Business School, 2015 (“Looking at the Promise and Perils of the Emerging Big Data Sector: Book Review of ‘Data and Goliath’ by Bruce Schneier,” *Deal Book*—a *New York Times* blog, March 16th, Available Online at <http://www.nytimes.com/2015/03/17/business/dealbook/book-review-of-data-and-goliath-by-bruce-schneier.html>, Accessed 07-12-2015)

When it comes to his specific policy recommendations, however, Mr. Schneier becomes significantly less compelling. And the underlying philosophy that emerges — once he has dispensed with all pretense of an evenhanded presentation of the issues — seems actually subversive of the very democratic principles that he claims animates his mission.

The author is at his most vehement in his opposition of all forms of government mass surveillance. He claims that data mining of undifferentiated bulk communications sucked up by our national security apparatus is “an inappropriate tool for finding terrorists.” “Whenever we learn about an N.S.A. success,” Mr. Schneier informs us, “it invariably comes from targeted surveillance rather than from mass surveillance.”

Like the claim that waterboarding failed to yield actionable intelligence that thwarted terrorist plots, it is impossible for a citizen without access to classified information to assess its validity.

Even if Mr. Schneier is correct that “traditional investigative police work” is ultimately responsible for successfully identifying the truly dangerous, there are still reasons that the public would want our spies to have access to a ready cache of metadata. As soon as the bad guy is found using old-fashioned methods, data-mining of previous communications would still presumably allow the speedy identification of known associates with a potentially lifesaving efficiency.

FT New America Foundation Report

The NAF report is wrong about the NSA's role in preventing terrorism.

Wittes 14 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2014 (“A Critique of the New America Foundation’s Recent NSA Report,” *Lawfare*—a national security blog curated by the Brookings Institution, January 23rd, Available Online at <http://www.lawfareblog.com/2014/01/a-critique-of-the-new-america-foundations-recent-nsa-report/>, Accessed 04-20-2015)

I am a big fan of Peter Bergen. His book, *Manhunt*, about the search for Osama Bin Laden is one of the most useful and informative and gripping reads on a counterterrorism matter I have come across in a long time. So it’s with a bit of a heavy heart that I say that his recent New America Foundation report, entitled “Do NSA’s Bulk Surveillance Programs Stop Terrorists?” is fatally flawed. Written with David Sterman, Emily Schneider, and Bailey Cahall, the report has grabbed headlines for its arresting conclusion that “the government’s claims about the role that NSA ‘bulk’ surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading.” The report examines the cases of 225 individuals and finds that “Section 215 of the USA PATRIOT Act appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases” and “Section 702 of the FISA Amendments Act played a role in 4.4. percent of the terrorism cases we examined.” Other NSA surveillance “played a role in 1.3 percent of the cases we examined.” In total, “NSA surveillance of any kind, whether bulk or targeted of U.S. persons or foreigners, played an initiating role in only 7.5 percent of cases.”

There are a number of problems with the New America Foundation report, mostly relating to the composition of the dataset it examines. That dataset includes 225 individuals but importantly, it includes many fewer events, since a terrorist plot or fundraising scheme will often involves several different individuals. The individuals in the dataset include people “in the United States, as well as U.S. persons abroad, who have been indicted, convicted or killed since the terrorist attacks on September 11, 2001.” The dataset “seeks to include all American citizens and residents indicted for crimes who were inspired by or associated with al-Qaeda and its affiliated groups, as well as those citizens and residents who were killed before they could be indicted, but have been widely reported to have worked with or been inspired by al-Qaeda and its affiliated groups.”

Here are four problems:

First, if you’re looking for NSA impact, a database of US citizens is the wrong place to look. NSA, after all, is a foreign intelligence agency that isn’t allowed to operate domestically, as a general matter. The 702 program specifically bars the targeting of US persons, requiring that targets be reasonably believed to be non-US persons overseas. Yes, the bulk telephony metadata program involves domestic and one-end-in-US acquisition of metadata, but that is specifically to assess whether domestic plots might have a foreign nexus and whether foreign plots may have an agent operating in the US. This is not an agency that investigates US nationals. So looking at a large database of US nationals and finding limited NSA involvement says very little about the effectiveness of the programs in question.

Second, NSA is not a law enforcement agency, so looking at a group of criminal cases is also the wrong haystack in which to find the needles at issue here. The perfect NSA operation would be

focused on identifying and disrupting some activity overseas and might never result in an indictment in a US court. So looking at a bunch of criminal cases and finding a minimal NSA footprint is a little bit like looking at a bunch of criminal cases and finding that the local fire department has been ineffective because its work only shows up in a few arson cases. Arson is only one small part of firefighting. And the criminal case is only one possible disposition for an intelligence agency—and not necessarily the most prized disposition. This problem is compounded by the fact that NSA material will generally not be admissible evidence (there are exceptions to that rule, but it's a good rule of thumb) and the government generally won't want to release it in the context of criminal cases (there are exceptions to that rule too, but it's also a good rule of thumb), so by the time you have a criminal case developed, the prosecutors will typically be presenting evidence that the FBI generated. This may follow a tip or lead from NSA, but the those tracks—at least when all goes well—will tend to be covered.

Third, the New America Foundation report is focused on how a criminal case gets initiated—that is, how authorities first learn of a particular plot. I'm not sure what the right metric is here, but I'm sure that's the wrong one. Information can be critical at many different stages of an investigation—whether a criminal or a national security investigation. If I were, say, the FBI, and a bomb went off at the Boston Marathon, it would be very useful and important to me to run the Tsarnaev brothers' telephone numbers through a database that could offer a window into whether they were having significant overseas contacts. It would be important even after I had identified them as the likely perpetrators, because it could provide insight into whether the bombing was a domestic matter or involved international terrorist groups. It might address the question of whether the AUMF applied—a deeply important in its own right. It might also address the question of whether confederates were still active. None of this has anything to do with how the investigation initiated, but it could be critical important to how it proceeds. Information—both in the form of evidence in criminal cases and in the form of intelligence in non-criminal investigations—is cumulative, not binary.

Finally, large numbers of the events in the New America Foundation database predate the authorities whose impact the group is studying. The list of events, available here, includes 105 separate incidents (as opposed to individuals). Of these, 24 predate 2006, when the law first enabled the current iteration of the 215 program. And quite a number more predate 2008, when Congress passed the FAA (including Section 702). This is not in and of itself devastating to the report, since metadata collection was taking place prior to 2006, as was overseas targeting of the communications contents of non-US persons overseas. But it does indicate a certain carelessness about what cases the database includes and excludes.

To put the matter simply, the New America report is evaluating intelligence programs mostly directed at non-US persons overseas on the basis of the initiation only of law enforcement cases directed at US citizens, and it is looking at a body of cases that don't correspond temporally to the existence of the programs it seeks to evaluate. As I say, I have a lot of respect for Peter Bergen, but this seems to me a serious misfire.

FT White House Panel Report

Their authors *misinterpret* the report — NSA domestic surveillance is a vital counter-terrorism tool.

Morell 13 — Michael Morell, Former Acting Director and Deputy Director of the Central Intelligence Agency, Member of President Obama's Review Group on Intelligence and Communications Technologies, 2013 ("Correcting the record on the NSA recommendations," *Washington Post*, December 27th, Available Online at http://www.washingtonpost.com/opinions/michael-morell-correcting-the-record-on-the-nsa-recommendations/2013/12/27/54846538-6e45-11e3-aecc-85cb037b7236_story.html, Accessed 07-12-2015)

Another misperception involved the review group's view of the efficacy of the Section 215 program; many commentators said it found no value in the program. The report accurately said that the program has not been "essential to preventing attacks" since its creation. But that is not the same thing as saying the program is not important to national security, which is why we did not recommend its elimination.

Had the program been in place more than a decade ago, it would likely have prevented 9/11. And it has the potential to prevent the next 9/11. It needs to be successful only once to be invaluable. It also provides some confidence that overseas terrorist activity does not have a U.S. nexus. The metadata program did exactly that during my last days at the CIA this summer, in the midst of significant threat reports emanating from Yemen. By examining the metadata, we were able to determine that certain known terrorists were most likely not in phone contact with anyone in the United States during this specific period of concern.

FT Glenn Greenwald

Greenwald isn't even worth responding to.

Wittes 11 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2011 (“My Non-Response to Glenn Greenwald,” *Lawfare*—a national security blog curated by the Brookings Institution, January 14th, Available Online at <http://lawfareblog.com/my-non-response-glenn-greenwald>, Accessed 07-12-2015)

Believe it or not, this blog does have a higher purpose than to send Glenn Greenwald into paroxysms of rage—though I confess that such paroxysms are great fun when we happen to provoke them, and they seem to be very good for traffic. That said, enraging Greenwald is not why I write the blog, and neither is engaging him. As Lawfare readers know, I define the universe of people with whom I feel privileged to argue exceptionally broadly. But Greenwald is not part of the same conversation as I am. His pose of moral purity has yielded both a committed simple-mindedness with respect to wrenchingly difficult questions and a very ugly eagerness to attack honorable people in government, in the press, and in public life more generally who are trying to do their jobs or to express views that differ from his. Greenwald seems to like to quote the founders, but his style actually reminds me more of their French contemporaries.

Lawfare readers will thus, I trust, pardon me if I don't treat Greenwald's admittedly amusing howls of rage as arguments warranting response.

To Greenwald's readers who find themselves on Lawfare for the first time: welcome; stick around; you might learn something. We have no purity tests here—just a preference for civility and decency.

Greenwald doesn't deserve a response — he's not civil.

Wittes 11 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2011 (“Why I Won't Engage Glenn Greenwald,” *Lawfare*—a national security blog curated by the Brookings Institution, January 16th, Available Online at <http://lawfareblog.com/why-i-wont-engage-glenn-greenwald>, Accessed 07-12-2015)

A few weeks ago, I received an email from a producer inviting me to participate in a “debate+discussion with Glenn [Greenwald] about the legality of the Predator strikes.” I responded, “I would be happy to discuss the subject . . . but I'm afraid I am unwilling to appear alongside Glenn Greenwald on any subject in any forum. I don't consider us as participating in remotely the same conversation.”

This exchange took place before Greenwald's and my back-and-forth this past week—in which he attacked me for faux centrism, for being on the take from lavish funders, and for servilely worshiping power, and in which I somewhat archly refused to engage him and compared him to the Jacobins.

The volume of email I have received following my non-response to Greenwald has been a genuine testament to the size of his readership. Almost all of the emails have been abusive. On Twitter, too, I am taking my lumps. The themes are remarkably consistent. I am a coward for

ducking an argument. Greenwald has made a substantive case which I am avoiding with a fake insistence on civility—even as I defend torturers. My refusal to engage proves the merits of Greenwald's positions.

I have tried to answer each of the emails, some of which have yielded substantive and valuable exchanges. And while none of this correspondence has convinced me that I should respond to Greenwald, it has collectively convinced me that I should explain more clearly why I do not do so—a decision that, as the email above reflects, I made long before his post of this week.

Tellingly, with a single exception, no regular reader of Lawfare has urged me to respond or has written to question my refusal to do so. People who spend time reading this blog—and it's not a huge group—have wide-ranging political sensibilities, but they share a tendency to insist on civility and common politeness. A while back, a human rights activist sent in some very cutting remarks about my views and asked me to post them. As I was getting ready to do so, he emailed and asked me to change a sentence that, he worried, could be construed as a personal attack. That's the sensibility of this blog—the idea that one can criticize ideas, even quite harshly, without questioning people's motives, accusing them of corruption, or pretending they do not believe what they say.

My problem with Greenwald is not his politics. I engage with people of his politics all the time. It is the pervasive suggestion in his work of the corruption and ill-motive of his opponents, whom he serially fails to credit with believing the arguments they are making. His post about me is a case in point. In his first paragraph, he purports to know my "overarching purpose." He insinuates—all but states, really—that I am a paid shill of the powerful. And throughout his piece, he casually casts aspersions on my motives and integrity ("dutifully fulfilling his function," "devote themselves to serving those in power," "That's not whose interests they're funded to defend," etc.).

This is by no means unusual for him. Consider this attack on Bobby (which begins by asserting falsely that Bobby had been dispatched by the White House to make the argument Glenn was criticizing) or this attack on Bob Litt (which actually calls Litt's argument "corrupt" and goes on to imply without quite saying that Litt was making it in support of intelligence community clients). This is Greenwald's modus operandi.

I don't see any reason either to engage with someone who begins with the premise that people who disagree with him are arguing in bad faith, are on the take, or are evil. My life is too short for that. When people on the right attacked Obama administration lawyers for their former representation in private life of Guantanamo detainees, I organized a group of centrist and conservative lawyers and policy folks to take a very strong position against it. My refusal to engage with Greenwald is rooted in the same sensibility: Civility is important to me in this debate--and no less so when I happen to be the object of the incivility. If that makes me look like a coward to some of Greenwald's readers, so be it.

One of Greenwald's readers, after hearing me out on this, responded as follows, "I still believe that his argument is persuasive enough, and based enough on sound reason and fact, that it merits an equally considered response." Fair enough. For Greenwald's readers who are genuinely interested in my views, I have written at great length about both interrogation and, particularly, detention. My views on these subjects are hardly a secret. Anyone who reads the interrogation chapter of *Law and the Long War* or the paper I wrote with Stuart Taylor Jr. in *Legislating the War on Terror* will not have any trouble figuring out why I think prosecution is a terrible idea.

For those who want a more explicit treatment of the specific question of prosecution, this oped by Jack speaks for me pretty completely. For those interested in an introduction to my rather voluminous writings on detention, my new book, *Detention and Denial*, is brief and written for the general interest reader. And interested readers should use the search function on Lawfare or simply browse it; many of the substantive points Greenwald raises we have addressed often.

But don't hold your breath waiting for me to reply to Greenwald. It isn't going to happen.

Crime

Links

Encryption transforms the internet into an ungovernable space. Law enforcement would become powerless.

Wittes 15 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2015 (“Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits,” *Lawfare*—a national security blog curated by the Brookings Institution, July 12th, Available Online at <http://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-ii-debate-merits>, Accessed 07-13-2015)

Consider the conceptual question first. Would it be a good idea to have a world-wide communications infrastructure that is, as Bruce Schneier has aptly put it, secure from all attackers? That is, if we could snap our fingers and make all device-to-device communications perfectly secure against interception from the Chinese, from hackers, from the FSB but also from the FBI even wielding lawful process, would that be desirable? Or, in the alternative, do we want to create an internet as secure as possible from everyone except government investigators exercising their legal authorities with the understanding that other countries may do the same?

Conceptually speaking, I am with Comey on this question—and the matter does not seem to me an especially close call. The belief in principle in creating a giant world-wide network on which surveillance is technically impossible is really an argument for the creation of the world's largest ungoverned space. I understand why techno-anarchists find this idea so appealing. I can't imagine for moment, however, why anyone else would.

Consider the comparable argument in physical space: the creation of a city in which authorities are entirely dependent on citizen reporting of bad conduct but have no direct visibility onto what happens on the streets and no ability to conduct search warrants (even with court orders) or to patrol parks or street corners. Would you want to live in that city? The idea that ungoverned spaces really suck is not controversial when you're talking about Yemen or Somalia. I see nothing more attractive about the creation of a worldwide architecture in which it is technically impossible to intercept and read ISIS communications with followers or to follow child predators into chatrooms where they go after kids.

Encryption empowers criminals and terrorists — it makes prosecution impossible.

Vance 14 — Cyrus Vance Jr., District Attorney of Manhattan, holds a J.D. from the Georgetown University Law Center, 2014 (“Apple and Google threaten public safety with default smartphone encryption,” *Washington Post*, September 26th, Available Online at http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html, Accessed 07-05-2015)

Apple and Google, whose operating systems run a combined 96.4 percent of smartphones worldwide, announced last week that their new operating systems will prevent them from complying with U.S. judicial warrants ordering them to unlock users' passcode-protected mobile devices.

Each company tweaked the code of its new and forthcoming mobile operating systems — iOS 8 and Android “L,” respectively — for this explicit purpose. “Apple cannot bypass your passcode and therefore cannot access this data. So it’s not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession,” reads a new section of Apple’s Web site. “Keys are not stored off of the device, so they cannot be shared with law enforcement,” a Google spokeswoman stated.

While these maneuvers may be a welcome change for those who seek greater privacy controls, the unintended victors will ultimately be criminals, who are now free to hide evidence on their phones despite valid warrants to search them.

On the losing end are the victims of crimes — from sexual assault to money laundering to robbery, kidnapping and homicide — many of whom undoubtedly are these companies’ own loyal customers.

When news of these changes was reported, I did a brief survey of my office’s recent cases to see which defendants Apple and Google would have protected had their passcode-locked smartphones been running iOS 8 or Android “L” at the time of their arrests. I found:

- * Multiple violent gang members who discussed in a smartphone video their plans to shoot a rival. The video was taken shortly before the members mistakenly shot an innocent bystander. The evidence would later be used to implicate two dozen of the gang’s members in additional murders and shootings.
- * A vile “up-skirter” who was observed by police inside a major subway station walking up and down stairs behind women wearing skirts, with two iPhones angled upward in his hands. A warrant allowed us to search the phones, which revealed exactly what you would think, as recorded by the perpetrator at multiple stations throughout New York.
- * An identity thief whose smartphone contained the bank account numbers, blank check images, account activity screen shots and tax return information of several individuals.

Today, nearly every criminal case has a digital component. Much of the evidence required to identify, locate and prosecute criminals is stored on smartphones. None of the above cases could be prosecuted as effectively if the perpetrators had smartphone software incorporating Apple and Google’s privacy guarantees.

Apple and Google have brought their products to a new level of privacy, and of course privacy is critically important to our society. But the protection of privacy is found in the Constitution, which requires warrants issued by neutral, detached judges and supported by probable cause before law enforcement can obtain information from a mobile device. Absent certain narrow exceptions, my office cannot search a mobile device without a warrant. Neither can the other thousands of state and local prosecutors offices throughout the country. The warrant requirement assures that peoples’ possessions and privacy remain secure in all but exceptional circumstances.

Apple’s and Google’s software updates, however, push mobile devices beyond the reach of warrants and thus beyond the reach of government law enforcement. This would make mobile devices different from everything else. Even bank security boxes — the “gold standard” of the pre-digital age — have always been searchable pursuant to a judicial warrant. That’s because banks keep a key to them.

I am aware of no plausible reason why these companies cannot reverse these dangerous maneuvers in their next scheduled updates to iOS 8 and Android “L.” Apple’s and Google’s software should not provide aid and comfort to those who commit crimes. This is not a matter of good or bad corporate citizenship. It is a matter of national public safety.

When threats to the common public safety arise, we ask Congress to do everything within its constitutional authority to address them. The provision of cloaking tools to murderer, sex offenders, identity thieves and terrorists constitutes such a threat.

Absent remedial action by the companies, Congress should act appropriately.

Encryption could get us all killed.

Hosko 14 — Ronald T. Hosko, President of the Law Enforcement Legal Defense Fund, Former Assistant Director of the Criminal Investigative Division at the Federal Bureau of Investigation, 2014 (“Don’t Create Virtual Sanctuaries for Criminals,” *Room for Debate*—a *New York Times* expert blog, October 1st, Available Online at <http://www.nytimes.com/roomfordebate/2014/09/30/apple-vs-the-law/dont-create-virtual-sanctuaries-for-criminals>, Accessed 07-05-2015)

When the director of the F.B.I. recently voiced his concerns about the impact of newly designed smartphone encryption systems on our security, the unsurprising, reflexive response of many was, “Too bad, government. We can’t trust you.” But, like most issues that divide our nation, it’s more complicated than that.

As a former insider, I watched the painful flow of Snowden disclosures with dismay – those leaks, I’m confident, have weakened our national security. It is no leap to suggest that those who already aim to harm us are bolstered by the information they have learned from the revelations. Even a moderately savvy criminal will closely observe the actions taken by law enforcement during their pursuit or conviction, later using such tactics themselves in future, often more dangerous crimes.

Popular culture has also skewed the public’s view of how law enforcement actually solves crimes. As happy as we would all be to close complex cases within a 60-minute time slot using cutting-edge technology, fighting crime nearly always requires exhaustive investigation and not simply the use of fancy gadgetry. In fact, investigators are limited in their technological capabilities, and I’m concerned that the gap between public perception and reality could only make matters worse.

The virtual sanctuaries constructed and marketed by certain companies will not only attract ordinary Americans seeking to protect their private communications, but also criminals and conspirators who wish to destroy our nation or to do great harm to others. Creating these technological fortresses will have our intelligence and law enforcement communities scurrying to penetrate them. On occasion, they’ll succeed. But on others, time or cost will defeat them, and people will be hurt or killed. While we debate the delicate balance of privacy and the lawful need to intrude, we leave American lives at risk.

Encryption exponentially increases the risk of catastrophic crime and terrorism.

Hosko 14 — Ronald T. Hosko, President of the Law Enforcement Legal Defense Fund, Former Assistant Director of the Criminal Investigative Division at the Federal Bureau of Investigation, 2014 (“Apple and Google’s new encryption rules will make law enforcement’s job much harder,” *Washington Post*, September 23rd, Available Online at <http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>, Accessed 07-05-2015)

Last week, Apple and Google announced that their new operating systems will be encrypted by default. Encrypting a phone doesn’t make it any harder to tap, or “lawfully intercept” calls. But it does limit law enforcement’s access to a data, contacts, photos and email stored on the phone itself.

That kind information can help law enforcement officials solve big cases quickly. For example, criminals sometimes avoid phone interception by communicating plans via Snapchat or video. Their phones contain contacts, texts, and geo-tagged data that can help police track down accomplices. These new rules will make it impossible for us to access that information. They will create needless delays that could cost victims their lives.*

Law enforcement officials rely on all kinds of tools to solve crimes and bring criminals to justice. Most investigations don’t rely solely on information from one source, even a smartphone. But without each and every important piece of the investigative puzzle, criminals and those who plan acts destructive to our national security may walk free.

In my last FBI assignments, I was privy to information that regularly demonstrated how criminal actors adapted to law enforcement investigative techniques – how drug conspirators routinely “dropped” their cellphones every 30 days or so, estimating the time it takes agents to identify and develop probable cause on a new device before seeking interception authority; how child predators migrated to technologies like the Onion Router to obfuscate who’s posting and viewing online posting and viewing online images and videos of horrific acts of child abuse.

We shouldn’t give them one more tool.

But the long-used cellular service selling points of clarity and coverage have been overtaken by a new one – concealment. Capitalizing on post-Snowden disclosures fears, Apple and Android have pitched this as a move to protect consumers’ privacy. Don’t misunderstand me — I, too, place a great value on personal privacy. I have little interest in the government collecting and storing all of my texts and e-mails or logging all of my calls.

But Apple’s and Android’s new protections will protect many thousands of criminals who seek to do us great harm, physically or financially. They will protect those who desperately need to be stopped from lawful, authorized, and entirely necessary safety and security efforts. And they will make it impossible for police to access crucial information, even with a warrant.

As Apple and Android trumpet their victories over law enforcement efforts, our citizenry, our Congress, and our media ought to start managing expectations about future law enforcement and national security success. We’ve lived in an era where the term “connecting the dots” is commonly used. If our cutting edge technologies are designed to keep important dots out of the

hands of our government, we all might start thinking about how safe and secure we will be when the most tech-savvy, dedicated criminals exponentially increase their own success rates.

* Editors note: This story incorrectly stated that Apple and Google's new encryption rules would have hindered law enforcement's ability to rescue the kidnap victim in Wake Forest, N.C. This is not the case. The piece has been corrected.

This turns the affirmative case — people will demand backdoors in response to horrible crimes.

Wittes 15 — Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution, Editor in Chief of Lawfare, Member of the Task Force on National Security and Law at the Hoover Institution, 2015 ("Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits," *Lawfare*—a national security blog curated by the Brookings Institution, July 12th, Available Online at <http://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-ii-debate-merits>, Accessed 07-13-2015)

There's a final, non-legal factor that may push companies to work this problem as energetically as they are now moving toward end-to-end encryption: politics. We are at very particular moment in the cryptography debate, a moment in which law enforcement sees a major problem as having arrived but the tech companies see that problem as part of the solution to the problems the Snowden revelations created for them. That is, we have an end-to-end encryption issue, in significant part, because companies are trying to assure customers worldwide that they have their backs privacy-wise and are not simply tools of NSA. I think those politics are likely to change. If Comey is right and we start seeing law enforcement and intelligence agencies blind in investigating and preventing horrible crimes and significant threats, the pressure on the companies is going to shift. And it may shift fast and hard. Whereas the companies now feel intense pressure to assure customers that their data is safe from NSA, the kidnapped kid with the encrypted iPhone is going to generate a very different sort of political response. In extraordinary circumstances, extraordinary access may well seem reasonable. And people will wonder why it doesn't exist.

Circumvention

Circumvention – bulk collection

The government will restart other bulk collection programs in response to the plan

Toomey 15 [Patrick, Patrick Toomey is a Staff Attorney in the ACLU's National Security Project, where he works on issues related to electronic surveillance, national security prosecutions, whistle-blowing, and racial profiling. Mr. Toomey is a graduate of Harvard College and Yale Law School. , Has the CIA Asked the FISC to Restart Its Bulk Collection Program?, <http://justsecurity.org/24216/cia-asked-fisc-restart-bulk-collection-program/>] Schloss BR 15-76 is a proposal to renew interception and storage of data in regards to businesses

And now it appears, the government may be seeking to restart another one of the very bulk collection programs that many people understood the USA Freedom Act was meant to prohibit.

There are a few reasons to think the missing application relates to one of these still-secret bulk collection programs and is not just another targeted request. First, in issuing the opinion related to BR 15-77 and BR 15-78, the FISC made a deliberate decision to split off the questions it considered no-brainers from the more difficult statutory and constitutional questions raised by the government's application to renew its bulk call records program in BR 15-75. The legal authority for that program has been deeply undermined by the Second Circuit's decision in ACLU v. Clapper, and at least based on the public record today, the FISC still has not resolved those questions. But in the meantime, as Judge Saylor's opinion makes clear, the FISC chose to skip ahead to several subsequent applications that presented only "relatively simple" questions. The FISC's decision to leave BR 15-76 out of Judge Saylor's opinion suggests that it involves more complicated questions on par with the bulk call records application — i.e., that it involves a different bulk collection program, one the government wants to restart but the FISC must now analyze more closely.

Second, it's very unlikely that BR 15-76 is a targeted application that the FISC simply went ahead and silently granted. That's because the FISC would have had to address the same questions raised by BR 15-77 and BR 15-78 in order to grant virtually any application under Section 215 — namely, which version of Section 215 is currently in effect. The temporary expiration of Section 215 on June 1 left it unclear, at least as a technical matter, what remained of the law when Congress decided to amend it. If the missing application were also a targeted one, why didn't the FISC resolve this question and announce its decision in the context of that earlier application? The better conclusion is that BR 15-76 isn't a targeted application at all, but concerns a bulk collection program the government continues to hide from the public.

They'll reinstate CIA bulk collection in response to the plan

Toomey 15 [Patrick, Patrick Toomey is a Staff Attorney in the ACLU's National Security Project, where he works on issues related to electronic surveillance, national security prosecutions, whistle-blowing, and racial profiling. Mr. Toomey is a graduate of Harvard College and Yale Law School. , Has the CIA Asked the FISC to Restart Its Bulk Collection Program?, <http://justsecurity.org/24216/cia-asked-fisc-restart-bulk-collection-program/>] Schloss

The more likely scenario is that the government has asked the FISC to reinstate the CIA's bulk collection program or one of its still-secret brethren. If that's right, the public should know about this program. The government's application goes directly to one of the key questions in the USA Freedom Act debate: whether the legislation would prove effective in halting the bulk collection of Americans' sensitive information. Perhaps the government is simply seeking to "transition" this program over the coming 180 days, as it has said of its effort to restart the NSA call records program — but of course we don't know. So long as the government continues to keep the public in the dark about its efforts to collect their data en masse, we can't judge whether the USA Freedom Act really put an end to bulk collection under Section 215.

2nc – redundant capabilities

Redundant means and justifications make circumvention easy

Brenner, 15 - Senior Fellow, the Center for Transatlantic Relations; Professor of International Affairs, University of Pittsburgh (Michael, Huffington Post, “The NSA's Second Coming” 6/8,

http://www.huffingtonpost.com/michael-brenner/the-nsas-second-coming_b_7535058.html

11. United States Intelligence agencies have multiple, **redundant** methods for acquiring bulk data or specific data. They also have multiple legal justifications, however **contrived** they might be; **those justifications are extremely difficult to challenge in the federal courts who have pretty much neutered themselves on these types of security issues**. Where top officials, including the President, feel it necessary, **they have few qualms about skirting the law.**

State and local governments will give data to the federal government – circumvents more restrictive federal rules

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

Outside of the federal government, a lot more surveillance and analysis of surveillance data is going on. Since 9/11, **the US has set up “fusion centers” around the country. These institutions are generally run by state and local law enforcement, and are meant to serve as an information bridge between those groups and national agencies like the FBI and DHS.**

They give local police access to previously unavailable surveillance capabilities and data. They were initially supposed to focus on terrorism, but increasingly they're used in broader law enforcement. And **because they're run locally, different fusion centers have different rules**—and different levels of adherence to those rules. **There's minimal oversight, probably illegal military involvement, and excessive secrecy.** For example, **fusion centers are known to have spied on political protesters.**

Joint Terrorism Task Forces are also locally run, nebulously defined, and shrouded in extreme secrecy. They've been caught investigating political activists, spreading anti- Islamic propaganda, and harassing innocent civilians.

They'll just use National Security Letters

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of

the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

That said, unlike NSA surveillance, FBI surveillance is traditionally conducted with judicial oversight, through the warrant process. Under the Fourth Amendment to the US Constitution, the government must demonstrate to a judge that a search might reasonably reveal evidence of a crime. However, the FBI has the authority to collect, without a warrant, all sorts of personal information, either targeted or in bulk through the use of National Security Letters (NSLs). These are basically administrative subpoenas, issued by the FBI with no judicial oversight. They were greatly expanded in scope in 2001 under the USA PATRIOT Act (Section 505), although the initial legal basis for these letters originated in 1978. Today, NSLs are generally used to obtain data from third parties: email from Google, banking records from financial institutions, files from Dropbox.

NSA circumvention

Redundant capabilities from other agencies circumvent

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

The NSA might get the headlines, but the US intelligence community is actually composed of 17 different agencies. There's the CIA, of course. You might have heard of the NRO—the National Reconnaissance Office—it's in charge of the country's spy satellites. Then there are the intelligence agencies associated with all four branches of the military. The Departments of Justice (both FBI and DEA), State, Energy, the Treasury, and Homeland Security all conduct surveillance, as do a few other agencies. And there may be a still-secret 18th agency. (It's unlikely, but possible. The details of the NSA's mission remained largely secret until the 1970s, over 20 years after its formation.)

After the NSA, the FBI appears to be the most prolific government surveillance agency. It is tightly connected with the NSA, and the two share data, technologies, and legislative authorities. It's easy to forget that the first Snowden document published by the Guardian—the order requiring Verizon to turn over the calling metadata for all of its customers—was an order by the FBI to turn the data over to the NSA. We know there is considerable sharing amongst the NSA, CIA, DEA, DIA, and DHS. An NSA program code-named ICReach provides surveillance information to over 23 government agencies, including information about Americans.

Domestic constraints cause a foreign shift – turns the case

Chandler and Le, 15 - * Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND **Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, "DATA NATIONALISM" 64 Emory L.J. 677, lexis)

First, the United States, like many countries, concentrates much of its surveillance efforts abroad. Indeed, the Foreign Intelligence Surveillance Act is focused on gathering information overseas, limiting data gathering largely only when it implicates U.S. persons. n174 The recent NSA surveillance disclosures have revealed extensive foreign operations. n175 Indeed, constraints on domestic operations may well have spurred the NSA to expand operations abroad. As the Washington Post reports, "Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight." n176 Deterred by a 2011 ruling by the Foreign Intelligence Surveillance Court barring certain broad domestic surveillance

of Internet and telephone traffic, n177 the NSA may have increasingly turned its attention overseas.

Allied cooperation circumvents domestic restrictions

Brenner, 15 - Senior Fellow, the Center for Transatlantic Relations; Professor of International Affairs, University of Pittsburgh (Michael, Huffington Post, “The NSA’s Second Coming” 6/8, http://www.huffingtonpost.com/michael-brenner/the-nsas-second-coming_b_7535058.html

7. The NSA coordinates its spying closely with Intelligence agencies of the four other English-speaking countries that participate in "Five Finger" alliance: the UK, Canada, Australia and New Zealand. Their data sharing does not stop at that acquired by legal means. They do each other favors by relying on a partner to circumvent domestic restrictions in any one of them. There are credible reports that NSA has assisted Britain's GCHQ in this respect. Both have assisted the German NBD in spying on German targets- as has been revealed within the past few weeks. Therefore, the significance of last week legislation is undercut by this close collaboration.

Creative lawyering guarantees circumvention

Redmond, 14 – J.D. Candidate, 2015, Fordham University School of Law (Valerie, “I Spy with My Not So Little Eye: A Comparison of Surveillance Law in the United States and New Zealand” FORDHAM INTERNATIONAL LAW JOURNAL [Vol. 37:733]

In the United States, the current state of surveillance law is a product of FISA, its amendments, and its strictures. An evaluation of US surveillance law proves that inherent loopholes undercut FISA’s protections, which allows the US Government to circumvent privacy protections.¹⁸² The main problems are the insufficient definition of surveillance, the ability to spy on agents of foreign powers, the lack of protection against third party surveillance, and the ability to collect incidental information.¹⁸³

First, a significant loophole arises in the interpretation of the term “surveillance.”¹⁸⁴ In order for information collection to be regulated by FISA, it must fall under FISA’s definition of surveillance.¹⁸⁵ This definition does not apply to certain National Security Letters, which are secret authorizations for the Federal Bureau of Investigation (“FBI”) to obtain records from telephone companies, credit agencies, and other organizations if they merely certify that the information is relevant to an international terrorism investigation.¹⁸⁶ National Security Letters are regularly used to circumvent FISA’s warrant procedures.¹⁸⁷

Additionally, FISA’s definition of surveillance is antiquated because it distinguishes between data acquired inside of the United States and outside of the United States.¹⁸⁸ This distinction allows the NSA to process surveillance that is received from other countries irrespective of whether the target is a US citizen.¹⁸⁹ Therefore, the NSA is unrestrained when a communication is not physically intercepted within the United States.¹⁹⁰

Second, an issue arises when US citizens are construed to be agents of foreign powers under FISA because a warrant can be issued to engage in surveillance against them.¹⁹¹ According to FISA's procedures, the only way to spy on a US citizen is when they can be considered to be an agent of a foreign power, or engaged in information gathering, aiding, or abetting a foreign power.¹⁹² However, this limitation does not result in total privacy protection because it only requires probable cause that a person is an agent of a foreign power, not that a crime is being committed.¹⁹³ The effect of this ability is that the US Government can conduct surveillance on a US citizen with no ties to terrorism such as a suburban mother telling her friend that her son "bombed" a school play.¹⁹⁴

2nc – domestic only limit

The domestic-only limit prevents solvency

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

It appears that little consideration was given over the past decade to the potential economic repercussions if the NSA’s secret programs were revealed.³⁸ This failure was acutely demonstrated by the Obama Administration’s initial focus on reassuring the public that its programs primarily affect non-Americans, even though non-Americans are also heavy users of American companies’ products. Facebook CEO Mark Zuckerberg put a fine point on the issue, saying that the government “blew it” in its response to the scandal. He noted sarcastically: “The government response was, ‘Oh don’t worry, we’re not spying on any Americans.’ Oh, wonderful: that’s really helpful to companies [like Facebook] trying to serve people around the world, and that’s really going to inspire confidence in American internet companies.”³⁹ As Zuckerberg’s comments reflect, certain parts of the American technology industry are particularly vulnerable to international backlash since growth is heavily dependent on foreign markets. For example, the U.S. cloud computing industry has grown from an estimated \$46 billion in 2008 to \$150 billion in 2014, with nearly 50 percent of worldwide cloud-computing revenues coming from the U.S.⁴⁰ R Street Institute’s January 2014 policy study concluded that in the next few years, new products and services that rely on cloud computing will become increasingly pervasive. “Cloud computing is also the root of development for the emerging generation of Web-based applications—home security, outpatient care, mobile payment, distance learning, efficient energy use and driverless cars,” writes R Street’s Steven Titch in the study. “And it is a research area where the United States is an undisputed leader.”⁴¹ This trajectory may be dramatically altered, however, as a consequence of the NSA’s surveillance programs.

The domestic-only limit wrecks solvency

Kehl, 14 – Policy Analyst at New America’s Open Technology Institute (Danielle, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July, <https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>

The U.S. government has already taken some limited steps to mitigate this damage and begin the slow, difficult process of rebuilding trust in the United States as a responsible steward of the Internet. But the reform efforts to date have been relatively narrow, focusing primarily on the surveillance programs’ impact on the rights of U.S. citizens. Based on our findings, we recommend that the U.S. government take the following steps to address the broader concern that the NSA’s programs are impacting our economy, our foreign relations, and our cybersecurity:

1. Strengthen privacy protections for both Americans and non-Americans, within the United States and extraterritorially.
2. Provide for increased transparency around government surveillance, both from the government and companies.
3. Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance, including moving toward international human-rights based standards on surveillance.
4. Begin the process of restoring trust in cryptography standards through the National Institute of Standards and Technology.
5. Ensure that the U.S. government does not undermine cybersecurity by inserting surveillance backdoors into hardware or software products.
6. Help to eliminate security vulnerabilities in software, rather than stockpile them.
7. Develop clear policies about whether, when, and under what legal standards it is permissible for the government to secretly install malware on a computer or in a network.
8. Separate the offensive and defensive functions of the NSA in order to minimize conflicts of interest.

The NSA doesn't comply with foreignness designation requirements

Gellman, 14 – staff writer for the Washington Post; won 3 Pulitzer Prizes (Barton, Washington Post, “In NSA-intercepted data, those not targeted far outnumber the foreigners who are” 7/5, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

When NSA and allied analysts really want to target an account, their concern for U.S. privacy diminishes. The rationales they use to judge foreignness sometimes stretch legal rules or well-known technical facts to the breaking point.

In their classified internal communications, colleagues and supervisors often remind the analysts that PRISM and Upstream collection have a “lower threshold for foreignness ‘standard of proof’ than a traditional surveillance warrant from a FISA judge, requiring only a “reasonable belief” and not probable cause.

One analyst rests her claim that a target is foreign on the fact that his e-mails are written in a foreign language, a quality shared by tens of millions of Americans. Others are allowed to presume that anyone on the chat “buddy list” of a known foreign national is also foreign.

In many other cases, analysts seek and obtain approval to treat an account as “foreign” if someone connects to it from a computer address that seems to be overseas. “The best foreignness explanations have the selector being accessed via a foreign IP address,” an NSA supervisor instructs an allied analyst in Australia.

Apart from the fact that tens of millions of Americans live and travel overseas, additional millions use simple tools called proxies to redirect their data traffic around the world, for business or pleasure. World Cup fans this month have been using a browser extension called Hola to watch live-streamed games that are unavailable from their own countries. The same trick is routinely used by Americans who want to watch BBC video. The NSA also relies routinely on locations embedded in Yahoo tracking cookies, which are widely regarded by online advertisers as unreliable.

Circumvention – allied intel sharing

Allied info sharing makes circumvention inevitable

Donohue, 15 - Professor of Law, Georgetown University Law Center (Laura, “SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT” 38 Harv. J.L. & Pub. Pol'y 117, Winter, lexis)

With GCHQ in mind, it is worth noting an additional exception to both FISA and Executive Order 12,333: to the extent that it is not the United States engaged in the collection of information, but, rather, one of our allies, rules that otherwise limit the U.S. intelligence community may not apply. From the language of the order, it appears that the United States may receive or benefit from other countries' collection of information on U.S. citizens, where it does not actively participate in the collection or specifically request other countries to carry out the collection at its behest. n142 In turn, the United States can provide information about foreign citizens to their governments that their intelligence agencies, under their domestic laws, might otherwise be unable to collect. To the extent that the programs underway are extended to the closely allied "Five Eyes" (Australia, Canada, the United Kingdom, the United States, and New Zealand), structural demarcations offer a way around the legal restrictions otherwise enacted to protect citizen rights in each region.

Information sharing is a loophole they can't fiat out of – it doesn't constitute 'its' surveillance but the government will get the info anyway

Redmond, 14 – J.D. Candidate, 2015, Fordham University School of Law (Valerie, “I Spy with My Not So Little Eye: A Comparison of Surveillance Law in the United States and New Zealand” FORDHAM INTERNATIONAL LAW JOURNAL [Vol. 37:733]

Furthermore, FISA is limited to protecting against surveillance by the US Government; it does not create a reasonable expectation of privacy for individuals from surveillance by a third party.¹⁹⁵ This rule is exploited by the United States' participation in Echelon.¹⁹⁶ Because US law generally does not regulate information sharing, the United States essentially violates the privacy rights of US citizens by accepting information from foreign intelligence agencies about potential threats involving US citizens.¹⁹⁷ Thus, the lack of privacy rights when US citizens are spied on by agencies outside of the United States creates a loophole for spying on US citizens without the government restrictions created by existing law.¹⁹⁸

Lastly, US law allows for the collection of incidental information.¹⁹⁹ It is predicted that Echelon collects nearly all communications, many of which can be considered incidental.²⁰⁰ Therefore, the fact that FISA allows for the collection of incidental information suggests that privacy rights can be violated by its involvement in Echelon.²⁰¹

Allied surveillance inevitable and information sharing is routine

Chandler and Le, 15 - * Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School AND **Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law (Anupam and Uyen, "DATA NATIONALISM" 64 Emory L.J. 677, lexis)

Third, while governments denounce foreign surveillance on behalf of their citizens, governments routinely share clandestinely intercepted information with each other. n182 The Guardian reports that Australia's intelligence agency collects and shares bulk data of Australian nationals with its partners - the United States, Britain, Canada, and New Zealand (collectively known as the "5-Eyes"). n183 Even while the German government has been a forceful critic of NSA surveillance, the German intelligence service has been described as a "prolific partner" of the NSA. n184 Der Spiegel reports that the German foreign intelligence agency Bundesnachrichtendienst (BND) has been collaborating with the NSA, passing about 500 million pieces of metadata in the month of December 2012 alone. n185 The NSA has collaborated with the effort led by the British intelligence agency Government Communications Headquarters (GCHQ) to hack into Yahoo!'s webchat service to access unencrypted webcam images of millions of users. n186 A German computer expert observes, "We know now that data was intercepted here on a large scale. So limiting traffic to Germany and Europe doesn't look as promising as the government and [Deutsche Telekom] would like you to believe." n187

2nc – circumvention turns the case

Circumvention turns their perception arguments

Seamon 8 – Professor, University of Idaho College of Law (Richard, “Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits”, Hastings Constitutional Law Quarterly, Spring 2008,
<http://www.hastingsconlawquarterly.org/archives/V35/I3/seamon.pdf>)//DBI

Conversely, allowing the President to ignore statutory restrictions on surveillance encourages executive lawlessness. Courts should discourage such behavior by preferring Fourth Amendment interpretations that encourage the executive branch to collaborate with the legislature to frame such rules, rather than defy them. After all, how is the public to feel when an Act of Congress supposedly provides the "exclusive" authority for a specified type of surveillance, yet it learns that a program exists "outside" that authority and has been going on for years? 20 8 Such a situation is likely to undermine public confidence that the nation's leaders obey the rule of law. It undermines faith in the legislative branch's willingness and ability to check executive abuse, and in the President's willingness to abide by legislative restrictions.^{20 9}

Circumvention – FBI specific

The FBI will empirically circumvent the plan

Schneier, 15 - fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient Systems, Inc (Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)//AK

Technology has greatly enhanced the FBI's ability to conduct surveillance without a warrant. For example, the FBI (and also local police) uses a tool called an IMSI-catcher, which is basically a fake cell phone tower. If you've heard about it, you've heard the code name StingRay, which is actually a particular type of IMSI-catcher sold by Harris Corporation. By putting up the tower, it tricks nearby cell phones into connecting to it. Once that happens, IMSI-catchers can collect identification and location information of the phones and, in some cases, eavesdrop on phone conversations, text messages, and web browsing. The FBI is so scared of explaining this capability in public that the agency makes local police sign nondisclosure agreements before using the technique, and instructs them to lie about their use of it in court. When it seemed possible that local police in Sarasota, Florida, might release documents about StingRay cell phone interception equipment to plaintiffs in civil rights litigation against them, federal marshals seized the documents.

Circumvention – section 702

Section 702 fails to limit domestic surveillance—legal loopholes and circumventions

Arnbak and Goldberg 14- cybersecurity and information law research at the Institute for Information Law, LL.M degree from Leiden University, A Competitive Strategy and Game Theory degree from London School of Economics University of Amsterdam; Associate professor in the Computer Science Department at Boston University, phD from Princeton University, B.A.S.c from University of Toronto (Axel and Sharon, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad”, Working Paper, June 27, 2014)//TT

For years, FISA and especially its s. 702 have been criticized for providing legal loopholes for warrantless political and economic surveillance on U.S. lawyers, NGOs, journalists and corporations communicating internationally through U.S. Internet companies [33]; the media reports in December 2005, around warrant-less wiretapping in bulk from the Internet backbone at an AT&T switch [28], have highlighted some of this tension. Nonetheless, U.S. Congress passed FAA after the AT&T revelations and extended the validity of the FAA for another five years on 31 December 2012, one day before the sunset deadline. Two months later, on 26 February 2013 in the case ‘Clapper v. Amnesty International’, the U.S. Supreme Court denied several U.S. organizations a right to claim that the privacy of their international communications was violated by s. 702 on procedural grounds. In what appeared to be the final ruling on the constitutionality of s. 702 for the foreseeable future, a 5-4 majority argued that these organizations were merely ‘speculating’, and could not prove that their communications had actually been intercepted [6]. Justice Breyer, on behalf of the minority, noted in his dissent that s. 702 prohibits the same applicants to actually gain knowledge of the surveillance itself because of national security secrecy, and that the broad authorities probably existed for a reason.

The political debate and the issue of legal standing have shifted considerably since June 2013, when it became clear that s. 702 indeed serves as the legal basis for many operations, among them ‘UPSTREAM’ and ‘PRISM’ [13]. Moreover, several of the classified targeting and minimization procedures under s. 702 have been leaked or declassified [2, 3]. Both revelations have spurred the N.S.A. to confirm that a principle use of s. 702 is compelling assistance from U.S. Internet companies for warrantless surveillance [5, p. 4].

This new dynamic enables a unique insight into classified and generous interpretations of the legal provisions in FISA made by the intelligence community and the FISA Court [13]. Before we dive into the details of FISA, we mention that FISA also contains s. 703 and s. 704, that regulate surveillance intentionally targeting U.S. persons located abroad. These sections are outside the scope of this paper, since our focus is on surveillance operations on Americans located in the U.S., with surveillance conducted on foreign soil. As an aside, Donohue has observed that the warrant requirements in these sections have been circumvented by applying s. 702 criteria to the collection phase, and then seeing whether collected data is of use for further processing after the fact [13, p.26].

2.2.2 Scope of the Second Regulatory Regime under FISA: The 1978 ‘Electronic Surveillance’ Definition

All communications surveillance operations that constitute ‘electronic surveillance’, as defined s. 1801(f) of FISA, fall within the scope of FISA (cf. 18 U.S.C. s.2511(2)(f); 50 U.S.C. s.1812(a)). The definition has largely remained intact since 1978. To acquire the content of ‘wired communications’, surveillance only falls within the FISA definition when authorities ‘intentionally target a U.S. person’ (s. 1801(f)(1)), or when the acquisition is conducted on U.S. soil (s. 1801(f)(2)). Importantly, when authorities conduct targeted surveillance from abroad, even if they know that both ‘sender and all intended recipients are located in the U.S.’, then only ‘radio’ (i.e., wireless) communications fall within the FISA definition of ‘electronic surveillance’ (s. 1801(f)(3)). The FISA definition only mentions communications ‘content’, but not ‘metadata’ (location, time, duration, identity of communicants, etc.), which in itself gives rise to privacy concerns that we will not further discuss here. Relevant for our purposes, is the observation that operations on ‘wired communications’, when conducted abroad, only fall within the scope of FISA if they ‘intentionally target a U.S. person’.

Intentionally Targeting U.S. Persons. ‘Intentionally targeting a U.S. person’ constitutes ‘electronic surveillance’ under FISA (s. 1801(f)(1)). However, ‘intention’ and ‘targeting’ are not defined in FISA, leaving the concepts open to generous interpretation by authorities in classified ‘targeting’ and ‘minimization’ procedures. Apart from providing clarity that bulk surveillance is not regarded as intentional targeting (we discuss this further when we look at legal protections from U.S. persons under FISA), the disclosure of these procedures has revealed two important new facts related to surveillance operations conducted abroad. Firstly, conducting the surveillance abroad creates the presumption that the surveillance targets a non-U.S. person [2, p. 3-4]. Secondly, the ‘targeting procedures’ do not provide any due diligence requirement or duty of care to establish the identity of parties on either side of a communication [2, p.3-4] [3]. This implies that unless a communicant is known to be a U.S. person, the procedures consider the communicant to be a non-U.S. person. In other words, authorities have a strong incentive to conduct surveillance abroad: legal protections offered to U.S. persons under FISA can be circumvented, and a more generous legal regime applies to the data collection itself.

702 fails—serious loopholes exist to circumvent protections

Arnbak and Goldberg 14- cybersecurity and information law research at the Institute for Information Law, LL.M degree from Leiden University, A Competitive Strategy and Game Theory degree from London School of Economics University of Amsterdam; Associate professor in the Computer Science Department at Boston University, PhD from Princeton University, B.A.S.c from University of Toronto (Axel and Sharon, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad”, Working Paper, June 27, 2014)//TT

Applicability of FISA to a surveillance operation is relevant for Americans, because the statute contains some important legal protections for U.S. persons intentionally targeted. For instance, the statute explicitly states that the 4th Amendment applies to surveillance operations under FISA (cf. s.1881(b)(5)) and a narrow set of four surveillance operations is explicitly prohibited. As discussed, surveillance under s. 702 may not intentionally target a U.S. person; for those operations s. 703 exists. Another example is the ‘reverse-targeting’ prohibition of s.1881(b)(2), which holds that authorities may not intentionally target a non-U.S. person under a s. 702 if the actual purpose of the operation is to target a U.S. person. By contrast, the third legal regime under

EO 12333 explicitly allows for intentional targeting of U.S. persons, when certain conditions discussed in the next section are met.

Nonetheless, serious loopholes exist for surveillance conducted within the bounds of FISA. One of the most-discussed loopholes is when U.S. persons have not been ‘intentionally targeted’ but instead affected by a surveillance operation, e.g., a bulk intercepts on the Internet backbone on U.S. soil under the ‘UPSTREAM’ program. Instead of promptly destroying such data, generous ex- emptions exist to nonetheless use the ‘incidentally’ or ‘inadvertantly’ collected information of the affected U.S. person, including when a ‘foreign intelligence’ interest is created in the data sometime after its collection, or when the information could be relevant for cybersecurity (incl. cyber-offense) purposes [3].

More generally, the targeting and minimization procedures seem to have introduced a new category of surveillance specifically aimed acquiring information about persons. (For example, two communicants that chat *about* a subject, like Angela Merkel, which is part of an N.S.A. ‘selector’.) Such surveillance is not considered to intentionally target specific communicating parties, and hardly enjoys protection even if it affects U.S persons. The information collected through such operations may be further analyzed and disseminated to other agencies as long as the identity of U.S. persons implicated are redacted in a way ‘that the information cannot be reasonably connected with an identifiable U.S. person’ [3, s.6]).³ A more complete analysis of the targeting and minimization procedures can be found in [13], along with a critical assessment of the role of the FISA Court.

Security

Security First

Security comes first—privacy is never absolute

Himma 7—Kenneth Himma, Associate Professor of Philosophy, Seattle Pacific University, holds JD and PhD and was formerly a Lecturer at the University of Washington in Department of Philosophy, the Information School, and the Law School, 2007 (“Privacy vs. Security: Why Privacy is Not an Absolute Value or Right,” Available online at <http://ssrn.com/abstract=994458>, accessed on 7/17/15)

Although an account that enables us to determine when security and privacy come into conflict and when security trumps privacy would be of great importance if I am correct about the general principle, my efforts in this essay will have to be limited to showing that the various theories of legitimacy presuppose or entail that, other things being equal, security is, as a general matter, more important than privacy. Among the moral rights most people believe deserve legal protection, none is probably more poorly understood than privacy. What exactly privacy is, what interests it encompasses, and why it deserves legal protection, are three of the most contentious issues in theorizing about information ethics and legal theory. While there is certainly disagreement about the nature and importance of other moral rights deserving legal protection, like the right to property, the very concept of privacy is deeply contested. Some people believe that the various interests commonly characterized as privacy interests have some essential feature in common that constitutes them as privacy interests; others believe that there is no such feature and that the concept of privacy encompasses a variety of unrelated interests, some of which deserve legal protection while others do not. Notably, many people tend to converge on the idea that privacy rights, whatever they ultimately encompass, are absolute in the sense that they may not legitimately be infringed for any reason. While the various iterations of the USA PATRIOT Act are surely flawed with respect to their particulars, there are many people who simply oppose, on principle, even a narrowly crafted attempt to combat terrorism that infringes minimally on privacy interests. There is no valid justification of any kind, on this absolutist conception, for infringing any of the interests falling within the scope of the moral right to privacy.

National security is a prerequisite for human security—the DA comes first

Edward C. Luck, director of a new center on international organization of the School of International and Public Affairs at Columbia University, January 2002, Global Governance

In this respect, it should be recognized that the recent emphasis on human security, though welcome, cannot be conceptually or operationally divorced from the parallel pursuit of national security. The latter may not be a sufficient condition to ensure the former, but it tends to be a necessary one. Secure states, it appears, are less likely to abuse their citizens or to permit others to do so than are insecure ones. In an age of intrastate and transnational conflicts in which civilian casualties are abhorrently high, it is generally where states are weakest that human security is most gravely threatened. In most cases, the first steps toward restoring human security will involve rebuilding or reshaping national institutions so that they are more capable, democratic, inclusive, responsive, transparent, and tolerant. Both international institutions and transnational civil society can play important supporting parts in these efforts--but again as supplements, not substitutes, for the state. For one thing, they can begin by acknowledging the need for stronger, not weaker, states. An underappreciation of the centrality of the state has also encouraged exaggerated rhetoric about the capacities and purposes of international organization and of civil society, as well as about the nature of their relationship. Most serious students of international organization, myself included, are also its advocates. As such, we need to take care not to confuse what we are seeking with what we are assessing. In our fascination with what is new in the world, we must not neglect the enduring importance of what is not. Nonstate actors matter, for example, largely because of the ways they influence the priorities and behavior of states. Likewise, international institutions play a critical role in many fields today precisely because we are still in the midst of the nation-state era. In a time of weapons of mass destruction and of economic globalization, the capacity of states for good or ill is such that the moderating influences of transnational civil society, global norms, and international organization can sometimes make a critical difference. But they cannot substitute for the state or for the domestic political processes that ultimately determine its policy choices. The powers of nonstate actors are derivative, their operational capacities limited, and their legitimacy compromised by their lack of accountability, sovereignty, and democratic structures.

A state centered conception of security is the only way to improve human well-being

Yuen Foong **Khong**, a fellow of Nuffield College, Oxford University, and senior research adviser at the Institute of Defence and Strategic Studies, **2001**, Vol. 7, Global Governance

However, too many individuals in the twenty-first century reside in makeshift shelters and thatched homes. What difference will it make to their lives for us to insist that they have become the referents of security? Not very much. It would be more advisable for them to cast their lot with their government--and their state--if they want a way out of their privation, which need not be seen in security terms. In the late 1970s, when Deng Xiaoping regained control of the reins of state power, he freed the Chinese peasant from the dictates of central economic planning and set in motion the virtuous cycle of economic growth that continues to this day. No amount of securitizing of the Chinese peasant could have secured for them what Deng, who saw the issue in terms of improving their livelihoods and making China strong, did. It has to be acknowledged that states in turmoil and those controlled by bad leaders are capable of despicable acts against their own citizens. However, to label the misery of citizens as a security problem that deserves international attention and response is not the wisest way to go, lest it gives citizens false hopes premised on false priorities and causal assumptions. Therefore, without the capacity and willingness to prioritize the countless human security dilemmas and devote the requisite human, economic, and military resources to make a dent in ameliorating these problems, it is probably not remiss to caution against the uncritical extension of the concept of security to the individual.

We have to solve large-scale violent conflicts before we can focus on everyday forms of violence – they’re a key barrier to peace

Joshua **Goldstein**, Int'l Rel Prof @ American U, **2001**, War and Gender, p. 412

First, peace activists face a dilemma in thinking about causes of war and working for peace. Many peace scholars and activists support the approach, “if you want peace, work for justice.” Then, if one believes that sexism contributes to war one can work for gender justice specifically (perhaps among others) in order to pursue peace. This approach brings strategic allies to the peace movement (women, labor, minorities), but rests on the assumption that injustices cause war. The evidence in this book suggests that causality runs at least as strongly the other way. War is not a product of capitalism, imperialism, gender, innate aggression, or any other single cause, although all of these influence wars’ outbreaks and outcomes. Rather, war has in part fueled and sustained these and other injustices.⁹ So, “if you want peace, work for peace.” Indeed, if you want justice (gender and others), work for peace. Causality does not run just upward through the levels of analysis, from types of individuals, societies, and governments up to war. It runs downward too. Enloe suggests that changes in attitudes towards war and the military may be the most important way to “reverse women’s oppression.” The dilemma is that peace work focused on justice brings to the peace movement energy, allies, and moral grounding, yet, in light of this book’s evidence, the emphasis on injustice as the main cause of war seems to be empirically inadequate.

Security Trumps Constitution

The counter-terror benefits of mass surveillance outweigh privacy and the Constitution.

Posner 5 —

Richard A. Posner, Senior Lecturer in Law at the University of Chicago, Judge on the United States Court of Appeals for the Seventh Circuit in Chicago, was named the most cited legal scholar of the 20th century by *The Journal of Legal Studies*, 2013 “Our Domestic Intelligence Crisis,” *Washington Post*, December 21st, <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>

These programs are criticized as grave threats to civil liberties. They are not. Their significance is in flagging the existence of gaps in our defenses against terrorism. The Defense Department is rushing to fill those gaps, though there may be better ways. The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer. The data that make the cut are those that contain clues to possible threats to national security. The only valid ground for forbidding human inspection of such data is fear that they might be used to blackmail or otherwise intimidate the administration's political enemies. That danger is more remote than at any previous period of U.S. history. Because of increased political partisanship, advances in communications technology and more numerous and competitive media, American government has become a sieve. No secrets concerning matters that would interest the public can be kept for long. And the public would be far more interested to learn that public officials were using private information about American citizens for base political ends than to learn that we have been rough with terrorist suspects – a matter that was quickly exposed despite efforts at concealment. The Foreign Intelligence Surveillance Act makes it difficult to conduct surveillance of U.S. citizens and lawful permanent residents unless they are suspected of being involved in terrorist or other hostile activities. That is too restrictive. Innocent people, such as unwitting neighbors of terrorists, may, without knowing it, have valuable counterterrorist information. Collecting such information is of a piece with data-mining projects such as Able Danger. The goal of national security intelligence is to prevent a terrorist attack, not just punish the attacker after it occurs, and the information that enables the detection of an impending attack may be scattered around the world in tiny bits. A much wider, finer-meshed net must be cast than when investigating a specific crime. Many of the relevant bits may be in the e-mails, phone conversations or banking records of U.S. citizens, some innocent, some not so innocent. The government is entitled to those data, but just for the limited purpose of protecting national security. The Pentagon's rush to fill gaps in domestic intelligence reflects the disarray in this vital yet neglected area of national security. The principal domestic intelligence agency is the FBI, but it is primarily a criminal investigation agency that has been struggling, so far with limited success, to transform itself. It is having trouble keeping its eye on the ball; an FBI official is quoted as having told the Senate that environmental and animal rights militants pose the biggest terrorist threats in the United States. If only that were so. Most other nations, such as Britain, Canada, France, Germany and Israel, many with longer histories of fighting terrorism than the United States, have a domestic intelligence agency that is separate from its national police force, its counterpart to the FBI. We do not. We also have no official with sole and comprehensive responsibility for domestic intelligence. It is no surprise that gaps in domestic intelligence are being filled by ad hoc initiatives. We must do better. The terrorist menace, far from receding, grows every day. This is not only because al Qaeda likes to space its attacks, often by many years, but also because weapons of mass destruction are becoming ever more accessible to terrorist groups and individuals.

Security Balance Good

The current balance between security and privacy is perfect

Karen J. Greenberg, [the executive director of the Center on Law and Security], APRIL 12, 2007

Karen J. Greenberg, Jeff Grossman, Sybil Perez, Joe Ortega, Jim Diggins, Wendy Bedenbaugh, [SECRECY AND GOVERNMENT: America Faces the Future PRIVACY IN THE AGE OF NATIONAL SECURITY] Pgs. 74-75

People often talk about the threats to our privacy under the Patriot Act and other Bush administration programs, but the actual notion of what privacy is – whether we have a right to it, why we think we have a right to it, and whether we even want it – seems to be somewhat up for grabs. The issue brings together the government, the corporate sector, the medical sector, and many diverse specialties that we do not usually combine in the same conversation. I see today's discussion as the beginning of a longterm dialogue about these ideas, which hopefully will come into focus as we talk about them. Privacy is a generational issue, and the way in which policymakers and commentators address it today may be irrelevant sooner than we think. My mother will not use her credit card at the supermarket because she does not want people to know what groceries she buys. That is her notion of privacy. One of my brothers will not go through the E-ZPass lane at the tollbooth because he does not like the idea of anybody knowing where he has been or where he is going. My daughter and her friends, however, post photos and trade notes on Facebook. They are an open book to one another and they do not care. They have a very different conception of what privacy should be. I think that the idea of protecting privacy, as we understand it, is already outdated. Over time, we should begin to understand a new concept of privacy that is very much within us. Prof. Burt Neuborne: We are going to ask difficult and theoretical questions about the nature of privacy and how it evolved as an idea. In thinking about the future, this panel will also discuss the notion of what privacy will look like in the technologically explosive world of the 21st century, why we should care, and what parameters should be imposed upon it. Valerie Caproni: Given my position as general counsel for the FBI, I suspect that few people will be surprised when I say that the primacy of privacy has not been sacrificed to the demands of national security or law enforcement. I do think that the topic needs to be discussed and that there must be public debate about it. I recognize that many of the panelists today feel that the accretion of power in the executive branch has endangered privacy and that we seem to have an endless desire to collect information on citizens. Nevertheless, it is my strong belief that the FBI is striking the correct balance between privacy and security (I do not have sufficiently in-depth knowledge to talk about other federal agencies). Too often, the debate is phrased in terms of an either/or proposition: you can either respect privacy or have national security, but not both. I reject that notion. The question is one of balance. From the Bureau's perspective, the notion of balancing security and privacy is nothing new. Benjamin Franklin said, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." I think we respect the notion of a middle ground. For all of our almost 100 years of existence, the FBI has been in the business of balancing national security and civil liberties. We view privacy as one element of civil liberties. There have admittedly been times in our history when we did not do a good job of balancing those equities. The abuses of the 1960s and '70s that led to the Church Committee in the Senate and the Pike Committee in the House are prime examples of the balance being askew, but things have changed since those days. The agents now working at the Bureau were children in the days of the counterintelligence programs known as "COINTELPRO." Those programs are not a part of any current agent's history.

Secret surveillance programs are necessary

Michael Sheehan was appointed a deputy assistant secretary of state in the Bureau of International Organizations . Secrecy and Government: America Faces the Future. April 12, 2007

so there are different levels of secrecy; the secracies involved in discrete acts and the secracies involved in entire state actions. But to get back to what we are concerned with today, we are talking about issues involv-

ing counterterrorism and some of the programs involved. I think that most people would agree that the government needs to keep certain secrets. The issues really revolve around programs, not secrets – secret programs. Three of them have been mentioned here today: the NSA wiretap program, which President Bush initiated after September 11th; the national security letter program that has been internally investigated by the FBI; and the NYPD programs looking at some of the actions prior to the Republican National Convention here in New York City. In my view, each one of these programs was justified in itself and was generally well-needed. But each of them probably suffered a little from not getting the proper legislative action and oversight to prevent abuse. The NSA wiretap program, which we wrote about here at the Center on Law and Security, was in my view well-warranted, and the president should have gotten the proper authority from the Congress. And he would have gotten it. I believe that if he had partnered with the Congress to give them aggressive oversight, he would have gotten that also. I believe that both sides of the aisle would have been able to provide constructive oversight of that program, and it would have worked much better. Perhaps the program would not have been in the jeopardy that it is in right now, although it still is going on. You do not hear a lot of squawking from the Democratically-controlled Congress because they recognize its value. Now, with proper oversight, I think they are a little bit more comfortable with it.

Privacy relations self-correct to balance harms – empirics prove

Etzioni 15 Amitai, "The New Normal – Finding a Balance between Individual Rights and the Common Good, Transaction Publishers – New Brunswick, NJ, Senior Advisor to the Carter White House; taught at Columbia, Harvard Business, Copyright 2015, ISBN 978-1-4128-5477-1)

Moreover, given that societal steering mechanisms are rather

loose, societies tend to over-steer and must correct their corrections with still further adjustments. For example, in the mid-1970s, the Church and Pike Committees investigated abuses by the CIA, FBI and NSA, uncovering "domestic spying on Americans, harassment and disruption of targeted individuals and groups, assassination plots targeting foreign leaders, infiltration and manipulation of media and business.³² As a result, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) and created the Foreign Intelligence Surveillance Court to limit the surveillance of American citizens by the US government.³³ After 9/11, several reports concluded that the reforms had gone too far by blocking the type of interagency intelligence sharing that could have forestalled the terrorist attacks.³⁴ As a result, the Patriot Act was enacted in a great rush and, according to its critics, sacrificed privacy excessively in order to enhance security and "correct" what are considered the excesses of the reforms the Church and Pike committees set into motion. Since then, the Patriot Act itself has been recalibrated.³⁵

At each point in time, one must hence ask whether society is tilting too far in one direction or the other. Civil libertarians tend to hold that rights in general and privacy in particular are not adequately protected. The government tends to hold that national security and public safety require additional limitations on privacy. It is the mission of legal scholars, public intellectuals, and concerned citizens to nurture dialogues that help sort out in which direction corrections must next be made.³⁶ Note that often some tightening in one area ought to be combined with some easing in others. For instance, currently a case can be made that TSA screening regulations are too tight, while the monitoring of whether visitors and temporary residents committed to leaving the US actually do so is too loose.

<?rin Kerr and Peter Swire engage in an important dialogue on whether the issues presented above are best suited for treatment by the courts or by Congress, and whether they are largely

viewed through the prism of the Fourth Amendment or Congressional acts. The following discussion treats both as if they were an amalgam.

National Security Protection Generally Good

National security is a prerequisite for human security—the DA comes first

Edward C. Luck, director of a new center on international organization of the School of International and Public Affairs at Columbia University, January 2002, Global Governance

In this respect, it should be recognized that the recent emphasis on human security, though welcome, cannot be conceptually or operationally divorced from the parallel pursuit of national security. The latter may not be a sufficient condition to ensure the former, but it tends to be a necessary one. Secure states, it appears, are less likely to abuse their citizens or to permit others to do so than are insecure ones. In an age of intrastate and transnational conflicts in which civilian casualties are abhorrently high, it is generally where states are weakest that human security is most gravely threatened. In most cases, the first steps toward restoring human security will involve rebuilding or reshaping national institutions so that they are more capable, democratic, inclusive, responsive, transparent, and tolerant. Both international institutions and transnational civil society can play important supporting parts in these efforts--but again as supplements, not substitutes, for the state. For one thing, they can begin by acknowledging the need for stronger, not weaker, states. An underappreciation of the centrality of the state has also encouraged exaggerated rhetoric about the capacities and purposes of international organization and of civil society, as well as about the nature of their relationship. Most serious students of international organization, myself included, are also its advocates. As such, we need to take care not to confuse what we are seeking with what we are assessing. In our fascination with what is new in the world, we must not neglect the enduring importance of what is not. Nonstate actors matter, for example, largely because of the ways they influence the priorities and behavior of states. Likewise, international institutions play a critical role in many fields today precisely because we are still in the midst of the nation-state era. In a time of weapons of mass destruction and of economic globalization, the capacity of states for good or ill is such that the moderating influences of transnational civil society, global norms, and international organization can sometimes make a critical difference. But they cannot substitute for the state or for the domestic political processes that ultimately determine its policy choices. The powers of nonstate actors are derivative, their operational capacities limited, and their legitimacy compromised by their lack of accountability, sovereignty, and democratic structures.

A state centered conception of security is the only way to improve human well-being

Yuen Foong Khong, a fellow of Nuffield College, Oxford University, and senior research adviser at the Institute of Defence and Strategic Studies, 2001, Vol. 7, Global Governance

However, too many individuals in the twenty-first century reside in makeshift shelters and thatched homes. What difference will it make to their lives for us to insist that they have become the referents of security? Not very much. It would be more advisable for them to cast their lot with their government--and their state--if they want a way out of their privation, which need not be seen in security terms. In the late 1970s, when Deng Xiaoping regained control of the reins of state power, he freed the Chinese peasant from the dictates of central economic planning and set in motion the virtuous cycle of economic growth that continues to this day. No amount of securitizing of the Chinese peasant could have secured for them what Deng, who saw the issue in terms of improving their livelihoods and making China strong, did. It has to be acknowledged that states in turmoil and those controlled by bad leaders are capable of despicable acts against their own citizens. However, to label the misery of citizens as a security problem that deserves international attention and response is not the wisest way to go, lest it gives citizens false hopes premised on false priorities and causal assumptions. Therefore, without the capacity and willingness to prioritize the countless human security

dilemmas and devote the requisite human, economic, and military resources to make a dent in ameliorating these problems, it is probably not remiss to caution against the uncritical extension of the concept of security to the individual.

We have to solve large-scale violent conflicts before we can focus on everyday forms of violence – they're a key barrier to peace

Joshua **Goldstein**, Int'l Rel Prof @ American U, **2001**, War and Gender, p. 412

First, peace activists face a dilemma in thinking about causes of war and working for peace. Many peace scholars and activists support the approach, “if you want peace, work for justice.” Then, if one believes that sexism contributes to war one can work for gender justice specifically (perhaps among others) in order to pursue peace. This approach brings strategic allies to the peace movement (women, labor, minorities), but rests on the assumption that injustices cause war. The evidence in this book suggests that causality runs at least as strongly the other way. War is not a product of capitalism, imperialism, gender, innate aggression, or any other single cause, although all of these influence wars' outbreaks and outcomes. Rather, war has in part fueled and sustained these and other injustices.⁹ So, “if you want peace, work for peace.” Indeed, if you want justice (gender and others), work for peace. Causality does not run just upward through the levels of analysis, from types of individuals, societies, and governments up to war. It runs downward too. Enloe suggests that changes in attitudes towards war and the military may be the most important way to “reverse women’s oppression.” The dilemma is that peace work focused on justice brings to the peace movement energy, allies, and moral grounding, yet, in light of this book’s evidence, the emphasis on injustice as the main cause of war seems to be empirically inadequate.

Utilitarianism Best

Evaluate consequences – allowing violence for the sake of moral purity is evil

Isaac 2 (Jeffrey C., Professor of Political Science – Indiana-Bloomington, Director – Center for the Study of Democracy and Public Life, Ph.D. – Yale, Dissent Magazine, 49(2), “Ends, Means, and Politics”, Spring, Proquest)

As writers such as Niccolo Machiavelli, Max Weber, Reinhold Niebuhr, and Hannah Arendt have taught, an unyielding concern with moral goodness undercuts political responsibility. The concern may be morally laudable, reflecting a kind of personal integrity, but it suffers from three fatal flaws: (1) It fails to see that the purity of one's intention does not ensure the achievement of what one intends. Abjuring violence or refusing to make common cause with morally compromised parties may seem like the right thing; but if such tactics entail impotence, then it is hard to view them as serving any moral good beyond the clean conscience of their supporters; (2) it fails to see that in a world of real violence and injustice, moral purity is not simply a form of powerlessness; it is often a form of complicity in injustice. This is why, from the standpoint of politics--as opposed to religion--pacifism is always a potentially immoral stand. In categorically repudiating violence, it refuses in principle to oppose certain violent injustices with any effect; and (3) it fails to see that politics is as much about unintended consequences as it is about intentions; it is the effects of action, rather than the motives of action, that is most significant. Just as the alignment with “good” may engender impotence, it is often the pursuit of “good” that generates evil. This is the lesson of communism in the twentieth century: it is not enough that one’s goals be sincere or idealistic; it is equally important, always, to ask about the effects of pursuing these goals and to judge these effects in pragmatic and historically contextualized ways. Moral absolutism inhibits this judgment. It alienates those who are not true believers. It promotes arrogance. And it undermines political effectiveness.

Looking at consequences is the only way to evaluate policy

Dan W. Brock, Professor of Philosophy and Biomedical Ethics at Brown University, **1987**
("Truth or Consequences: The Role of Philosophers in Policy-Making," *Ethics*, Volume 97, July, Available Online via JSTOR, p. 787)

When philosophers become more or less direct participants in the policy-making process and so are no longer academics just hoping that an occasional policymaker might read their scholarly journal articles, this scholarly virtue of the unconstrained search for the truth—all assumptions open to question and follow the arguments wherever they lead—comes under a variety of related pressures. What arises is an intellectual variant of the political problem of "dirty hands" that those who hold political power often face. I emphasize that I do not conceive of the problem as one of pure, untainted philosophers being corrupted by the dirty business of politics. My point is rather that the different goals of academic scholarship and public policy call in turn for different virtues and behavior in their practitioners. Philosophers who steadfastly maintain their academic ways in the public policy setting are not to be admired as islands of integrity in a sea of messy political compromise and corruption. Instead, I believe that if philosophers maintain the academic virtues there they will not only find themselves often ineffective but will as

well often fail in their responsibilities and act wrongly. Why is this so? The central point of conflict is that the first concern of those responsible for public policy is, and ought to be, the consequences of their actions for public policy and the persons that those policies affect. This is not to say that they should not be concerned with the moral evaluation of those consequences—they should; nor that they must be moral consequentialists in the evaluation of the policy, and in turn human, consequences of their actions—whether some form of consequentialism is an adequate moral theory is another matter. But it is to say that persons who directly participate in the formation of public policy would be irresponsible if they did not focus their concern on how their actions will affect policy and how that policy will in turn affect people. The virtues of academic research and scholarship that consist in an unconstrained search for truth, whatever the consequences, reflect not only the different goals of scholarly work but also the fact that the effects of the scholarly endeavor on the public are less direct, and are mediated more by other institutions and events, than are those of the public policy process. It is in part the very impotence in terms of major, direct effects on people's lives of most academic scholarship that makes it morally acceptable not to worry much about the social consequences of that scholarship. When philosophers move into the policy domain, they must shift their primary commitment from knowledge and truth to the policy consequences of what they do. And if they are not prepared to do this, why did they enter the public domain? What are they doing there?

Civil Liberties/Rights Infringements Justified in The War on Terror

Constitution requires the President to preserve security even if rights are violated

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 79-80

Initially, it is impossible to say with any certainty whether or not Presidents like Abraham Lincoln and Franklin Roosevelt had to infringe constitutional liberties the way they did in order to win their wars. Perhaps they could have achieved the same results with fewer intrusions. But maybe greater solicitude for personal freedoms would have led to defeat, or to a victory that exacted a far greater cost in blood and money. Speculating about such matters is an academic exercise. All we know for sure is that these Presidents took the actions they deemed necessary prevail, and they did. For better or worse, the Constitution commits to the President almost unbridled discretion to determine what must be done to meet a military emergency. These decisions must be made quickly and with imperfect information, and they are then judged by Congress, voters, and posterity

Civil liberties violations necessary to prevent terror attacks

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 80

[Incorporating the lessons of history] has several implications for the War on Terrorism. Most importantly, although President Bush asserted aggressive unilateral executive powers, his response to al Qaeda's September 11, 2001 attacks was fairly mild in comparison with the actions of Lincoln, Roosevelt, and other Presidents. Furthermore, like his predecessors, Bush can defend his infringements on civil liberties as necessary to achieve his avowed objective: preventing another terrorist assault. In the past, such success has usually been sufficient for a President to deflect charges that he went overboard. Indeed, the majority of Americans have always solidly supported antiterrorism efforts. Although the legal and media intelligentsia have been outraged by conditions at Guantanamo Bay, average people do not appear to feel widespread regret that will result in a compensatory increase in civil rights.

Civil liberties yield to the national imperative of winning wars

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 83

In implementing the Constitution, all three branches have determined that sometimes individual rights and liberties must yield to the national imperative of winning a war. The primary actor has been the President, who has had to make swift decisions based on a constantly shifting military situation and imperfect intelligence. As long as they acted reasonably under the circumstances, strong Presidents who have forcefully and successfully responded to military crises have always enjoyed the support of Congress, the courts, and the American people. Thus, modern laments that these Presidents have gone "too far" often smack of Monday-morning quarterbacking. The examples of Lincoln and Roosevelt are especially illuminating.

Presumption favors security, not rights

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 88

The overall picture, however, is best captured by America's decision to build a monument honoring Roosevelt, as it did for Lincoln. These marble symbols send the clear message that, in a high-stakes war, Presidents should err on the side of using too much force (including intrusions on constitutional liberties) to win, rather than risk defeat by showing greater sensitivity for individual rights.

War on terror requires innovative tactics

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 88

Since September 11, 2001, America has been engaged in a unique conflict. Unlike past wars, America is not fighting a nation-state for a finite time period in a series of battles. Rather, we are confronting shadowy worldwide private terrorist groups like al Qaeda, which strike indiscriminately in a struggle that will probably never end. Accordingly, the Bush Administration responded with equally innovative strategies and tactics. The War on Terrorism raises difficult constitutional questions concerning how to strike the optimum balance between national defense and individual rights.

Authorization to Use Military Force (AUMF) and the PATRIOT Act provide legal authority for the President's actions in the war on terror

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 89

First, Congress authorized the President to use "all necessary and appropriate force" against those who planned, committed, or aided the terrorist attacks.

Invoking this "Authorization for Use of Military Force" (AUMF) and his independent Article II powers, Bush deployed troops to Afghanistan (whose government had backed al Qaeda) and beefed up antiterrorism efforts both at home and abroad. Among other things, Bush claimed the power to indefinitely detain "enemy combatants" (a status determined by the executive branch) and, at his discretion, to try them by military commissions appointed by the Secretary of Defense.

Second, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act increased surveillance of suspected terrorists, especially by reducing restrictions on domestic gathering of foreign intelligence; facilitated the deportation of immigrants suspected of involvement with terrorism; authorized law enforcement officials to search homes and businesses without prior notice to the owners ("sneak and peek"); permitted government searches of telephone, internet, financial, and other records; and enhanced the Treasury Secretary's power to regulate and monitor financial transactions involving suspected terrorists and their allies.

Bush's actions in the war on terror less restrictive than Lincoln's or Roosevelt's

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 90

First, unlike Lincoln and Wilson, Bush did not censor speech or the press or criminally prosecute his critics, despite their vehement and often vicious verbal attacks on him and his antiterrorism policies. Admittedly, the USA PATRIOT Act has raised legitimate First Amendment concerns, but they are of a far smaller magnitude than those that resulted from previous Presidents' flagrant suppression of valid opposition to their wartime actions.

Second, in contrast to FDR's treatment of Japanese Americans, President Bush worked with Congress to specifically prohibit and condemn discrimination against Arab and Muslim Americans and to ensure review of all allegations of civil rights abuses. Such sensitivity was welcome in the emotionally charged aftermath of the September 11 attacks.

Third, Lincoln suspended the writ of habeas corpus unilaterally and broadly, whereas Bush and Congress left it intact. The only exception was for a few hundred foreign suspected terrorists imprisoned at the U.S. Naval Base in Guantanamo Bay, Cuba, who were given extensive administrative and judicial review as a substitute.

Public supported Bush's actions in the war on terror

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 91

My preliminary assessment, then, is that Bush consistently took strong actions to fight terrorism; that Americans (and their representatives in Congress) always supported these efforts; but that the Iraq War and the economic downturn fatally weakened his Presidency. Bush did not, however, adopt many of the liberty-infringing policies of his predecessors, such as censoring the press or imprisoning members of a particular ethnic group.

Conditions of war and insecurity justify actions that infringe on civil liberties. Modern infringements are mild by historical comparison

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 92

War is hell. Winning one requires many hard decisions based on constantly changing military circumstances and incomplete information. Presidents in the midst of a national security crisis often conclude that they have to do unspeakably awful things, as when Lincoln ordered that Union Army deserters be shot and Truman chose to drop atomic bombs. Keeping in mind the emergency conditions that actually existed and the facts the President had available, it is usually difficult to conclude with certitude that his specific infringement of civil liberties was unnecessary for military success. It is equally speculative to assert that regret over wartime excesses has directly resulted in enhanced protection of civil rights. Similarly, no one can objectively determine whether such a tradeoff (if one existed) was worth it. As with all armed conflicts, reasonable people can disagree about the optimum balance between individual rights and collective security in the War on Terrorism. In evaluating the response of the Bush and Obama Administrations to this threat, it is important to recognize the validity of a range of possible responses and to compare Presidents to their real-life predecessors, not to some idealized leader.

FISA requirements reflect need for surveillance in a war time environment

Yohn Yoo, Summer 2014, Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute, Harvard Journal of Law & Public Policy, THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS,
<http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Yoo1.pdf>, DOA: 1-1-15, p. 905

As explained above, FISA does not reflect a general attitude against government surveillance; rather, it creates a balance between the criminal system's restrictions on government searches and the broader acceptance of information-gathering during wartime. Although FISA does lay out a probable cause requirement, that requirement is more in line with

wartime information gathering than with evidence gathering in the criminal system. And, although the FISC does check the government's ability to conduct surveillance, it only does so shrouded in complete confidentiality--reflecting the wartime, rather than criminal, system of information gathering. This blend of the criminal and wartime information gathering schemes negates the assertion that FISA broadly protects against government surveillance. **Although FISA's criminal components restrict government searches, the wartime components recognize the government's need to engage in robust information gathering during times of conflict.**

Collection of intelligence necessary enables US military readiness

John **McLaughlin** teaches at the Johns Hopkins School of Advanced International Studies. He was deputy director and acting director of the CIA from 2000 to 2004, January 2, 2014, Washington Post, "NSA Intelligence-Gathering Programs Keep us Safe," http://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html

It's time we all came to our senses about the National Security Agency (NSA). If it is true, as many allege, that the United States went a little nuts in its all-out pursuit of al-Qaeda after the Sept. 11, 2001, attacks, it is equally true that we are going a little nuts again in our dogged pursuit of the post-Snowden NSA. Those who advocate sharply limiting the agency's activities ought to consider that its work is the very foundation of U.S. intelligence. I don't mean to diminish the role of other intelligence agencies, and I say this as a 30-year veteran of the Central Intelligence Agency who is "CIA" through and through. But in most cases, **the NSA is the starting point for determining what holes need to be filled through other means of intelligence-collection.** That's because its information on foreign developments is so comprehensive and generally so reliable. **It is the core of intelligence support to U.S. troops in battle. Any efforts to "rein in" the agency must allow for the possibility that change risks serious damage to U.S. security and the country's ability to navigate in an increasingly uncertain world.**

Rights not Absolute

An appropriate moral theory considers both rights and outcomes

Thomas Nagel, Professor of Philosophy, New York University, 'READING NOZICK, Jeffrey Paul, ed., 1981, p200.

A political theory that reflected these moral complexities would assign society the function of promoting certain goods and preventing certain evils, within limits set by the differing constraints of different individual rights. It would not judge processes and procedures solely by their tendency to produce certain outcomes, nor would it judge outcomes solely by the processes that had produced them. Social institutions and the procedures defining them would be assessed by reference both to their respect for individual rights and liberty, and to their tendency to promote desirable ends like the general welfare.

Rights carry different weights

Thomas Nagel, Professor of Philosophy, New York University, READING NOZICK, Jeffrey Paul, ed., 1981, p199.

There is no reason to think that either in personal life or in society the force of every right will be absolute or nearly absolute, i.e., never capable of being overridden by consequential considerations. Rights not to be deliberately killed, injured, tormented, or imprisoned are very powerful and limit the pursuit of any goal. More limited restrictions of liberty of action, restrictions on the use of property, restrictions on contracts, are simply less onerous and therefore provide less powerful constraints.

Rights can be overridden

Thomas Nagel, Professor of Philosophy, New York University, READING NOZICK, Jeffrey Paul, ed., 1981, p 196.

The sources of morality are not simple but multiple; therefore its development in political theory will reflect that multiplicity. Rights limit the pursuit of worthwhile ends, but they can also sometimes be overridden if the ends are sufficiently important.

Nozickian rights must be weighed against other interests

Jeffrey Paul, Professor of Philosophy, Bowling Green State University, READING NOZICK, 1981, p13.

Moreover, Nagel argues, the desirability of living a meaningful life cannot by itself imply as Nozick suggests it does, an absolute right against interference by others. For the effect of such non-interference upon those others who must, according to Nozick, forswear from intrusive activity has to be weighed against the interests of persons whose alleged rights are transgressed.

Rights aren't absolute

Ronald Dworkin, New York University Law School, TAKING RIGHTS SERIOUSLY, 1978,
p354

I conceded, moreover, that even the grand individual rights are not absolute, but will yield to especially powerful considerations of consequence, which I called, too dramatically, 'emergencies'. The argument of principle that establishes the individual right as an abstract right must recognize, in more concrete circumstances, negative arguments of principle from which it may follow, for example, that no one has a right to speak his mind freely when the result would be to cripple the defense capacity of the nation.

Rights can be overridden

C.E. Harris, philosopher, Texas A&M, APPLYING MORAL THEORIES, 1986, p137-38

Our first inclination might be to argue that we should never override the rights of others, but the preceding considerations have shown us that sometimes we must. In situations that involve criminal activity or a conflict of obligations, someone's freedom or well-being must be overridden.

Rights vary in importance

Ronald Dworkin, New York University Law School, TAKING RIGHTS SERIOUSLY, 1978,
p366

The theory of rights I offer does not deny that some rights are more important than others. No alleged right is a right (on my account) unless it overrides at least a marginal case of a general collective justification; but one right is more important than another if some especially dramatic or urgent collective justification, above that threshold, will defeat the latter but not the former.

It's permissible to risk rights violations

Charles Fried, Harvard Law School, RIGHT AND WRONG, 1978, p82

If my right against you to the security of my property means that you do me wrong if you take even a chance at damaging my property in pursuit of some other end, then that is right is too intrusive, potentially barring you from the pursuit of any goals--since everything carries some minuscule risk of producing the untoward result.

Rights aren't totally deontological

Ronald Dworkin, New York University Law School, TAKING RIGHTS SERIOUSLY, 1978, p313

Few people hold a rigidly deontological theory of rights. So most judges will think that, even when moral and political rights are in question, consequentialist arguments will play a role in defining the dimensions of these rights.

Abstract rights are meaningless

Mark Tushnet, Georgetown Law School, TEXAS LAW REVIEW, May 1 1984, p1364

It does not advance understanding to speak of rights in the abstract. It matters only that some specific right is or is not recognized in some specific social setting. It is, for example, literally incoherent to claim that women in neolithic societies ought to have had the right to choose not to bear children. Such a claim would have been meaningless to them.

Rights conflicts are irresolvable

Alan Hutchinson and Patrick Monehan, New York University Law School, TEXAS LAW REVIEW, May 1 1984, p1484-5

In any actual dispute, however, both parties can express their claims in the language of rights. Unless some meta-theory enables the adjudicator to choose between competing rights, a rights scheme will be meaningless. But liberalism possesses no such meta-theory. The various

argumentative techniques lawyers commonly employ provide equally plausible justifications for opposite results, depending on whether the initial emphasis is on freedom or on security.

Individual interests must be balanced with community interests

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.26-7

When Communitarians argue that the pendulum has swung too far toward the radical individualistic pole and it is time to hurry its return, we do not seek to push it to the opposite extreme, of encouraging a community that suppresses individuality. We aim for a judicious mix of self-interest, self-expression, and commitment to the commons--of rights and responsibilities, of I and we. Hence the sociological recommendation to move from 'I' to 'we' is but a form of shorthand for arguing that a strong commitment to the commons must now be added to strong commitments to individual needs and interests that are already well ensconced. Balancing the domestic forces with a fair measure of resumed wellness will bring our society closer to a balanced position, without a significant tilt toward either side, a society able to steer a stable course.

Individual rights and social needs must be balanced

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.182

At one extreme is the Radical Individualist position that no changes may be made whatsoever in Miranda, as if this legal measure, which did not take effect until 1966, was part of the Bill of Rights or carried the endorsement of the Founding Fathers. On the other hand, Authoritarians argue that Miranda, in toto, is but one of those many rights that accord criminals greater constitutional protection than is accorded to their victims. Indeed, former attorney general Edwin Meese wanted to do away with reading Miranda rights altogether. He believed that 'it provides incentives for criminals not to talk' and 'only helps guilty defendants.' The Office of Legal Policy of the US Attorney General under the Reagan administration issued a position paper that called for a wholesale overturning of Miranda. Here, as in many other matters, social wisdom and justice may well lie in third, intermediate positions, which balance individual rights with social needs.

Individual rights must inherently be balanced against public safety

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.264

The American moral and legal tradition has always acknowledged the need to balance individual rights with the need to protect the safety and health of the public. The Fourth Amendment, for example, guards against unreasonable searches but allows for reasonable ones.

Responsibilities need to be prioritized over rights

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p. 4

Correcting the current imbalance between rights and responsibilities requires a four-point agenda: a moratorium on the minting of most, if not all, new rights; reestablishing the link between rights and responsibilities; recognizing that some responsibilities do not entail rights; and most carefully, adjusting some rights to the changed circumstances.

Individual rights and social needs must be balanced

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.182

At one extreme is the Radical Individualist position that no changes may be made whatsoever in Miranda, as if this legal measure, which did not take effect until 1966, was part of the Bill of Rights or carried the endorsement of the Founding Fathers. On the other hand, Authoritarians argue that Miranda, in toto, is but one of those many rights that accord criminals greater constitutional protection than is accorded to their victims. Indeed, former attorney general Edwin Meese wanted to do away with reading Miranda rights altogether. He believed that 'it provides incentives for criminals not to talk' and 'only helps guilty defendants.' The Office of Legal Policy of the US Attorney General under the Reagan administration issued a position paper that called for a wholesale overturning of Miranda. Here, as in many other matters, social wisdom and justice may well lie in third, intermediate positions, which balance individual rights with social needs.

Individual rights must inherently be balanced against public safety

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.264

"The American moral and legal tradition has always acknowledged the need to balance individual rights with the need to protect the safety and health of the public. The Fourth Amendment, for example, guards against unreasonable searches but allows for reasonable ones.

Community needs prioritization over individual freedom

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.25

The eighties was a decade in which 'I' was writ large, in which the celebration of the self became a virtue. (The period was not unique, however, since such tendencies run far and deep in our national tradition.) Now is the time to push back the pendulum.

The times call for an age of reconstruction, in which we put a new emphasis on 'we' on values we share, an the spirit of the community.

Responsibilities need to be prioritized over rights

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.4

Correcting the current imbalance between rights and responsibilities requires a four-point agenda: a moratorium on the minting of most, if not all, new rights; reestablishing the link between rights and responsibilities; recognizing that some responsibilities do not entail rights; and most carefully, adjusting some rights to the changed circumstances.

Individual rights and social needs must be balanced

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.182

At one extreme is the Radical Individualist position that no changes may be made whatsoever in Miranda, as if this legal measure, which did not take effect until 1966, was part of the Bill of Rights or carried the endorsement of the Founding Fathers. On the other hand, Authoritarians argue that Miranda, in toto, is but one of those many rights that accord criminals greater constitutional protection than is accorded to their victims. Indeed, former attorney general Edwin Meese wanted to do away with reading Miranda rights altogether. He believed that 'it provides incentives for criminals not to talk' and 'only helps guilty defendants.' The Office of Legal Policy of the US Attorney General under the Reagan administration issued a position paper that called for a wholesale overturning of Miranda. Here, as in many other matters, social wisdom and justice may well lie in third, intermediate positions, which balance individual rights with social needs.

Individual rights must inherently be balanced against public safety

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.264

"The American moral and legal tradition has always acknowledged the need to balance individual rights with the need to protect the safety and health of the public. The Fourth Amendment, for example, guards against unreasonable searches but allows for reasonable ones.

Community needs prioritization over individual freedom

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.25

The eighties was a decade in which 'I' was writ large, in which the celebration of the self became a virtue. (The period was not unique, however, since such tendencies run far and deep in our national tradition.) Now is the time to push back the pendulum. The times call for an age of reconstruction, in which we put a new emphasis on 'we' on values we share, an the spirit of the community.

Responsibilities need to be prioritized over rights

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.4

Correcting the current imbalance between rights and responsibilities requires a four-point agenda: a moratorium on the minting of most, if not all, new rights; reestablishing the link between rights and responsibilities; recognizing that some responsibilities do not entail rights; and most carefully, adjusting some rights to the changed circumstances.

Rights are not trump cards; policy goals can outweigh the interests of rights

Harvey, J.D., Yale Law School, '02 (Philip Harvey, "Human Rights and Economic Policy Discourse: Taking Economic And Social Rights Seriously", Spring, 2002, 33 Colum. Human Rights L. Rev. 363, l/n)

A view frequently expressed by human rights advocates is that valid rights should "trump" other policy goals,¹⁵ but I argue that this prescription, if taken at face value, is inadequate. A genuine trump outweighs even the highest valued card in another suit, but rights-based claims are rarely treated that way. They are given added weight, but not a genuinely trumping value. For example, in American constitutional jurisprudence, even fundamental rights may be infringed; however, a "compelling state interest" is required to justify such actions.¹⁶ What I argue is needed, therefore, is not a social choice methodology that treats rights as absolute trumps, but one that treats them with appropriate deference. The level of deference owed a particular right may vary with the importance of the ultimate interests it protects and with the nature of the countervailing interests that oppose it. Whether the balance between human rights protection and other policy goals is struck appropriately in particular instances may not be easy to determine. It certainly will not be demonstrable with the mathematical precision to which welfare economics aspires. The most we can expect is persuasive argument.

Rights are not trump cards; policy goals can outweigh the interests of rights

Harvey, J.D., Yale Law School, '02 (Philip Harvey, "Human Rights and Economic Policy Discourse: Taking Economic And Social Rights Seriously", Spring, 2002, 33 Colum. Human Rights L. Rev. pp. 370-1)

A view frequently expressed by human rights advocates is that valid rights should "trump" other policy goals,¹⁵ but I argue that this prescription, if taken at face value, is inadequate. A genuine trump outweighs even the highest valued card in another suit, but rights-based claims are rarely treated that way. They are given added weight, but not a genuinely trumping value. For example, in American constitutional jurisprudence, even fundamental rights may be infringed; however, a "compelling state interest" is required to justify such actions.¹⁶ What I argue is needed, therefore, is not a social choice methodology that treats rights as absolute trumps, but one that treats them with appropriate deference. The level of deference owed a particular right may vary with the importance of the ultimate interests it protects and with the nature of the countervailing interests that oppose it. Whether the balance between human rights protection and other policy goals is struck appropriately in particular instances may not be easy to determine. It certainly will not be

demonstrable with the mathematical precision to which welfare economics aspires. The most we can expect is persuasive argument.

Once a counter-rights claim is established, rights are simply voided from consideration

John Hasnas, professor of Business Ethics, Georgetown, NORTHWESTERN UNIVERSITY LAW REVIEW, 1995, p. 932

But when fundamental rights conflict, as they can under the contemporary conception, the government will resolve the conflict on the basis of what will be most beneficial for society as a whole. In other words, it will employ precisely the same decision procedure as it would if there were no rights involved. Thus, when rights conflict, they play no substantive role. They simply drop from consideration.

Rights Threaten Community

Rights talk undermines community responsibility

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.7-8

To put it differently, we all now on one level that our liberties are limited by those of others and that we can do what we want only as long as we do not harm others. Rights talk, however, pushes us to disregard this crucial qualification, the concern for one another and for the community. Soon 'I: can do what I want as long as I do not hurt others' becomes 'I can do what I want, because I have a right to do it.'

Individual rights theory views humans atomistically

Charles Taylor, McGill University Philosopher, POWERS, POSSESSIONS AND FREEDOM, Ed. Alkis Kontos, 1979, p.41

Why do we even begin to find it reasonable to start a political theory with an assertion of individual rights and to give these primacy? I want to argue that the answer to this question lies in the hold on us of what I have called atomism. Atomism represents a view about human nature and the human condition which (among other things) makes a doctrine of the primacy of rights plausible; or to put it negatively, it is a view in the absence of which this doctrine is suspect to the point of being virtually untenable.

Rights can conflict with the value of community

Charles Taylor, McGill University Philosopher, POWERS, POSSESSIONS AND FREEDOM, Ed. Alkis Kontos, 1979, p.143

But just as the demands of utility and rights may diverge, so those of the citizen republic may conflict with both. For instance, the citizen republic requires a certain sense of community, and what is needed to foster this may go against the demands of maximum utility. Or it may threaten to enter into conflict with some of the rights of minorities.

Rights talk exaggerates conflict

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.7

Even if lawyers and judges realize among themselves that individual rights are limited by the rights of others and the needs of the community, as the language of rights penetrates into everyday discourse, the discourse becomes impoverished and confrontational. It is one thing to claim that you and I have different interests and see if we can work out a compromise; or, better yet, that we both recognize the merit or virtue of a common cause, say, a cleaner environment. The moment, however, that I claim a right to the same piece of land or property or public space as you, we start to view one another like the Catholics and Protestants in Northern Ireland or the Palestinians and Israelis in the

Rights talk undermines democratic compromise

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.6-7

Moreover, the expression of ever more wants, many quite legitimate, in the language of rights makes it difficult to achieve compromises and to reach consensus, processes that lie at the heart of democracy. A society that is studded with groups of true believers and special-interest groups, each brimming with rights, inevitably turns into a society overburdened with conflicts. Columnist John Leo of US NEWS AND WORLD REPORT declares: 'Rights talk polarizes debate; it tends to suppress moral discussion and consensus building. Once an agenda is introduced as a right sensible discussion and moderate positions tend to disappear.'

Rights undermine communitarian values

Roberto Unger, Harvard Law School, THE CRITICAL LEGAL STUDIES MOVEMENT, 1986, p36

The established system of rights presents another, less familiar obstacle to the aims of this institutional program: the absence of legal principles and entitlements capable of informing communal life--those areas of social existence where people stand in a relationship of heightened mutual vulnerability and responsibility toward each other.

Rights undermine communitarian values

Roberto Unger, Harvard Law School, THE CRITICAL LEGAL STUDIES MOVEMENT, 1986, p36-37

For one thing, our dominant conception of right imagines the right as a zone of discretion of the rightholder, a zone whose boundaries are more or less rigidly fixed at the time of initial definition of the right. The right is a loaded gun that the rightholder may shoot at will in his corner of town. Outside that corner the other licensed gunmen may shoot him down. But the give-and-take of communal life and its characteristic concern for the actual effect of any decision upon the other person are incompatible with this view of right and therefore, if this is the only possible view, with any regime of rights.

The procedural republic undermines community and democracy

Michael J. Sandel, Professor of Government-Harvard University., LIBERALISM AND THE LIMITS OF JUSTICE, 1982, p.93

A full account of this transition would take a detailed look at the changing shape of political institutions, constitutional interpretation, and the terms of political discourse in the broadest sense. But I suspect we would find in the practice of the procedural republic two broad tendencies foreshadowed by its philosophy: first a tendency to crowd out democratic possibilities; second, a tendency to undercut the kind of community on which it nonetheless depends.

Rights talk undermines community responsibility

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.7-8

To put it differently, we all now on one level that our liberties are limited by those of others and that we can do what we want only as long as we do not harm others. Rights talk, however, pushes us to disregard this crucial qualification, the concern for one another and for the community. Soon 'I can do what I want as long as I do not hurt others' becomes 'I can do what I want, because I have a right to do it.'

Individual rights theory views humans atomistically

Charles Taylor, McGill University Philosopher, POWERS, POSSESSIONS AND FREEDOM, Ed. Alkis Kontos, 1979, p.41

Why do we even begin to find it reasonable to start a political theory with an assertion of individual rights and to give these primacy? I want to argue that the answer to this question lies in the hold on us of what I have called atomism. Atomism represents a view about human

nature and the human condition which (among other things) makes a doctrine of the primacy of rights plausible; or to put it negatively, it is a view in the absence of which this doctrine is suspect to the point of being virtually untenable.

Procedural Rights Threaten Community

Rights can conflict with the value of community

Charles Taylor, McGill University Philosopher, POWERS, POSSESSIONS AND FREEDOM, Ed. Alkis Kontos, 1979, p.143

But just as the demands of utility and rights may diverge, so those of the citizen republic may conflict with both. For instance, the citizen republic requires a certain sense of community, and what is needed to foster this may go against the demands of maximum utility. Or it may threaten to enter into conflict with some of the rights of minorities.

Rawls Answers

Can't determine equality or the value of the risk in the original position

Ralph Ellis, philosophy professor, Florida, JUST RESULTS: ETHICAL FOUNDATIONS FOR POLICY ANALYSIS, p. 22

The most serious problem with the argument as Rawls originally proposed it is that there is no way to determine how safe or daring the person in the original position would want to be in her risk-taking behavior. As Kaye (1980) and other critics to be discussed later have shown, a very daring risk taker in the original position might be willing to risk the loss of some very necessary kinds of goods for the chance of gaining a very large amount of less necessary goods. We, therefore, cannot determine how much equality or inequality would be tolerated in a society from the standpoint of the original position.

The norms Rawls uses to justify the “original position” are utilitarian

Leonard Rattner, law professor, UCLA, HOFSTRA LAW JOURNAL, Spring 1984, p. 760-1

Despite his explicit rejection of utilitarian thought, Rawls intimates a utilitarian foundation for his equal-treatment conclusions by noting a sense of justice, moral feelings, and altruistic reciprocity may have evolutionary origins and by designating scarce resources, conflicting resource claims, and resulting collaborative arrangements as “circumstances of justice

Privacy Bad/Privacy Not Good

Privacy Generally Bad

Many benefits to limiting privacy

Heidi Reamer Anderson, Assistant Professor, Florida Coastal School of Law, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public," I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY v. 7 n. 3, 2012,
https://kb.osu.edu/dspace/bitstream/handle/1811/72997/ISJLP_V7N3_543.pdf?sequence=1

Just as we must "value privacy on the basis of the range of activities it protects" we also must consider the range of activities that protecting privacy would impede, i.e., the range of activities precluded by the privacy protections themselves.²²⁰ Although some scholars initially identify some of these benefits of exposure of public conduct or information,²²¹ there is no comprehensive recognition, categorization, and aggregation of exposure's benefits in the privacy literature. This section aims to fill that gap, beginning with a discussion of how exposure keeps government officials accountable.²²² Governmental accountability benefits Daniel Solove claims that "dog poop girl would have been just a vague image in a few people's memories if it hadn't been for the photo entering cyberspace and spreading around faster than an epidemic."²²³ While this may be true, and may be deemed a net gain for society in that one instance, this does not mean that legally preventing or discouraging exposures of people's public behavior always results in a net gain for society. Recall the police brutality story from the Introduction involving Officer Walsh. Do we want events like that to be "vague image[s] in a few people's memories?"²²⁴ Of course not, because exposure of such images holds our government officials accountable, inspires public debate, and often leads to real policy changes. However, such benefits could be sacrificed in that situation and others like it if the person who videotaped the event did not post it to YouTube because he had a legal duty to protect the obscurity of Officer Walsh or of other people at the scene. In trying to prevent harm suffered by the Dog Poop Girls of the world, we risk losing exposure of public behavior that should be further seen, heard, discussed, and addressed.²²⁵

Consider the many recent exposures of public officials at public events with other people nearby about which we may not have learned (or at least not seen) if the law protected people's obscurity in public: Anti-gay comments made by candidate for New York Governor, Carl Paladino, in a meeting with religious leaders:²²⁶ Then Governor of South Carolina, Mark Sanford's, emails to the woman with whom he was having an extra-marital affair, and suggestions to his staff to account for his absences during these affairs by falsely stating that he was "hiking the Appalachian trail";²²⁷ The reference by George Allen, a candidate for Virginia's U.S. Senate seat, to an opponent's aide as "Macaca," which many interpreted as a racist statement equating the aide to a Macaque monkey;²²⁸ Then Senate Majority Leader Trent Lott's birthday party statement suggesting that had civil-rights opponent and fellow Senator Strom Thurmond been elected president in 1948, on a pro-segregation platform, "we wouldn't have had all these problems over the years";²²⁹ and Pictures posted on a website by Ninth Circuit Judge Alex Kozinski, depicting nude women painted to look like farm animals.²³⁰ Any one of these or similar exposures of public conduct or statements may have been precluded or at least "chilled" if the law recognized a right to obscurity. As a result, the helpful discussions and consequences these exposures motivated may not have occurred. Thus, there is a risk that providing a general right to obscurity would sacrifice significant governmental accountability benefits. In the end, "keeping pertinent information about public affairs out of the hands of the public is equally problematic," regardless of whether the information's source is a "citizen journalist" or a more traditional journalist.²³¹ Behavioral improvement benefits There also is significant value in continuing to apply the "no privacy in public" rule to everyone instead of applying it only to public officials. Just as the possibility of getting caught and punished acts deters crime, the possibility of getting exposed for public statements or behavior deters non-criminal but still objectively-undesirable behavior.²³² Daniel Solove calls this type of exposure "norm policing," but this term is too pejorative for something that holds so much potential for benefitting society. Solove claims that "[w]e do not view the victims [of exposure] as blameworthy, and there is little social value in their suffering."²³³ I disagree. This alleged suffering, in the form of lost dignity and lost obscurity, can lead to significant social value-and even save lives. In Order Without Law, Robert Ellicksen discussed the behavioral benefits of exposure.²³⁴ In a more recent and more specific study, Lior Jacob Strahilevitz demonstrated how additional exposure of people's reckless driving habits could reduce deaths on our highways-the number one cause of death among those aged fifteen to twenty-nine.²³⁵ Strahilevitz first showed how protecting motorist obscurity leads to rude, dangerous, and even life-threatening behavior.²³⁶ Next, he demonstrated how reducing driver obscurity through exposure by fellow citizens, and holding drivers accountable for their actions, has led to better and safer driving among some "exposed" groups and promises such benefits for society should the exposed groups be expanded.²³⁷ Indeed, Strahilevitz has shown how facilitating closeness and more "norm policing" may work better than the tort system itself as a way of curtailing and punishing bad behavior.²³⁸ Fewer people cutting us off or tailgating us may save lives. On a more abstract level, additional exposure and less obscurity, promise to increase happiness as well, on the highways and elsewhere.²³⁹

Fewer instances of other bad behavior may make life more enjoyable in various other contexts-primarily those in which obscurity authorizes and perhaps encourages objectionable behavior.²⁴⁰ For example, exposing poor tippers online has made servers who felt cheated feel better simply by reporting them; such exposure, in turn, may make patrons more courteous and more generous. Similarly, exposure of unruly hotel, sports stadium, or airport patrons could make visiting such places more enjoyable for all.²⁴¹ If the potential for getting exposed for saying something extremely harmful to someone else actually changes someone's behavior-and prevents the harm that would have been caused-then this changed behavior is a benefit of the "no privacy in public" rule and is another benefit supporting the rule's retention. Criminal deterrence, reporting, and integrity benefits The fruits of exposure can be even more beneficial to society when it is a criminal act, versus happiness-reducing rudeness, that is subject to exposure.²⁴² Louis Brandeis's suggestion that sunlight is the best disinfectant permeates popular culture and legal discourse.²⁴³ Often forgotten, however, is the second part of Brandeis's sunlight quote: and "electric light the most efficient policeman."²⁴⁴ As Brandeis suggested, exposure that leads to reduced obscurity for would-be criminals can be quite efficient at deterring crime, improving the integrity of the criminal justice system, and increasing the reporting of crimes, as discussed below. As Daniel Solove has conceded, "social control can be beneficial... [f]or example, surveillance can serve as a deterrent to crime."²⁴⁴ In Great Britain, a government surveillance program using closed-circuit cameras (CCTV) reportedly has reduced street crimes in some areas by fifty percent or more.²⁴⁵ Although the Obscurity Problem includes, by definition, only exposure by private persons versus governments, it is possible if not likely that private exposure has a similar, albeit less comprehensive, deterrent effect on crime as more comprehensive, government-led surveillance would have. Further, if Britain's CCTV is any indication, the crime-deterring effects come burdened with minimal "thinking space" or other harms.²⁴⁶ The increased feeling of safety then improves citizen well-being across the board, leading to additional self-liberty, not less.²⁴⁷ For the many crimes that will occur despite the presence of citizen journalists, exposure of public conduct likely will continue to assist in the reporting of crimes as well as in the apprehension and prosecution of the correct perpetrators. For example, citizens have used their cell phone cameras to expose drivers involved in "hit and run" accidents in ways that led to their eventual arrest.²⁴⁸ Similarly, some citizens

reluctant to report crimes in-person have been willing to report crimes via cell phone text messages including photographs of the alleged perpetrators.²⁴⁹ Additionally, New York City residents now may report crimes via uploading their pictures or videos to a government website.²⁵⁰ The freedom to expose others' public actions even empowers some gutsy citizens to record and report the very criminals that have hurt them.²⁵¹ More broadly, social networks, chock-full of reports regarding others' activities and whereabouts, have been and could continue to be harnessed to locate and track criminals or lost children.²² These same networks of citizen journalists and their exposures provide reliable and truthful alibis for the wrongly-accused, thereby improving the integrity of the system and ensuring that the right person eventually is caught.²⁵³ Further, replacing notoriously unreliable eyewitness testimony with more reliable evidence of exposures documented via still- and video-cameras also improves reliability.²⁵⁴ Ultimately, the presence and use of what amounts to millions of mobile, citizen-directed security cameras could vastly improve the integrity and reliability of the criminal justice system, leading to improved safety and liberty for all citizens. Emotional and therapeutic benefits Although privacy scholars carefully have identified the emotional harms associated with the Obscurity Problem, they have not fully accounted for the emotional benefits associated with exposure. A person who exposes another's public behavior via distributing a video or story online often does so because sharing her take on the behavior with others makes her feel better.²⁵⁵ Some describe the emotional benefit of sharing a story via a personal blog as providing "a new kind of intimacy, a sense that they are known and listened to."²⁵⁶ For intensely personal autobiographical speech, the emotional benefits to the speaker are even more pronounced and heart-felt.²⁵⁷ In fact, even the performance of "Numa Numa Guy" has been described as a reason to promote webcam recordings because his video exhibited pure emotional enjoyment of a song.²⁵⁸ Thus, silencing one person to protect the obscurity of another likely ends up sacrificing the emotional interests of the one silenced. Exposure of public conduct also leads to emotional benefits for people similarly situated to the exposed person. When someone is exposed in public for supposedly shameful conduct-such as alcoholism-it often leads other people who engage in that conduct to feel connected and no longer alone. This powerful emotional benefit is why memoirs, a genre likely made impossible by a duty to protect others' obscurity, are so powerful.²⁵⁹ In turn, the readers of such truthful stories experience emotional benefits as well. Exposure even can help change a harmful social norm that wrongfully made a person feel "different" in the first place. For example, the "exposures" of certain celebrities as gay allegedly empowered others to come out and ultimately change the harmful social norm that made them feel ostracized.²⁶⁰ Even if the norm does not change, the exposure could lead to other emotional benefits such as a sense of community, relief, or forgiveness.²⁶¹ Exposing people's public actions and statements also brings certain issues, previously hidden at the expense of a certain segment of society, into the public sphere where they can be debated and addressed.²⁶² For example, some feminist scholars have argued that over-insistence on privacy kept many women's rights issues hidden from public scrutiny. In all of these ways, the increased pride, self-esteem, confidence and other emotional benefits likely offset dignity harms to the one being exposed or to people fearing exposure.²⁶³ Deception prevention benefits One reason some people vilify the Obscurity Problem is that they have something to hide and depend upon others' ignorance regarding this "something" in order to maintain their personal and professional relationships.²⁶⁴ Revealing this information may "correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fianc&e."²⁶⁵ Thus, exposing truthful facts about a person that he purposefully hides from others acts as a "deception prevention" device, which many view as a net benefit for society.²⁶⁶ Preventing deception leads to other societal benefits, both directly and indirectly, such as ensuring that one does not hire an irresponsible person to take care of one's children.²⁶⁷ Knowing more about someone also can help people make decisions based on real information rather than relying on inaccurate stereotypes.²⁶⁸ If we know more about people, and observe them benefitting society despite their past behavior, perhaps we will learn to be more forgiving and less judgmental.²⁶⁹ Legally barring or punishing the exposure of such information lets the deception and poor decision making continue in the interest of protecting a mythical right to obscurity.²⁷⁰

Innovation Turn

Privacy undermines the freedom to innovate

Adam Thierer, George Mason University - Mercatus Center, 2014, Maine Law Review, Privacy Law's Precautionary Problem,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2449308##

Privacy law today faces two interrelated problems. The first is an information control problem. Like so many other fields of modern cyberlaw — intellectual property, online safety, cybersecurity, etc. — privacy law is being challenged by intractable Information Age realities.¹ Specifically, it is easier than ever before for information to circulate freely and harder than ever to bottle it up once it is released.² This has not slowed efforts to fashion new rules aimed at bottling up those information flows. If anything, the pace of privacy-related regulatory proposals has been steadily increasing in recent years even as these information control challenges multiply.³ This has led to privacy law's second major problem: the precautionary principle problem. The precautionary principle generally holds that new innovations should be curbed or even forbidden until they are proven safe. Fashioning privacy rules based on precautionary principle reasoning necessitates prophylactic regulation that makes new forms of digital innovation guilty until proven innocent. This puts privacy law on a collision course with the general freedom to innovate that has thus far powered the Internet revolution, and privacy law threatens to limit innovations consumers have come to expect or even raise prices for services consumers currently receive free of charge.⁴ As a result, even if new regulations are pursued or imposed, there will likely be formidable push-back not just from affected industries but also from their consumers.

Strong privacy protection undermines innovation and investment

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

If creepiness were the standard by which information collection and distribution activities were regulated, it raises the question whether services like Gmail, and the entire commercial Internet for that matter, can continue to exist. Online advertising and data collection are the fuel that powers the modern information economy.⁴⁷ If claims of creepiness are converted into actionable legal trumps on commercial online activities, advertising and data collection will no longer be able to sustain online sites and services.⁴⁸ As a result, those online services will either need to raise prices significantly (most of them charge nothing today), cut back services, limit further innovation and investment, or go under entirely.⁴⁹ Regulation—especially arbitrary regulation of this sort—is not a costless exercise.

Adam Thierer, George Mason University, 2010, Privacy as an Information Control Regime: The Challenges, Ahead, <https://techliberation.com/2010/11/13/privacy-as-an-information-control-regime-the-challenges-ahead/>

Once they jump to the assumption that privacy is a “human right,” or must be protected in the name of “human dignity,” any discussion of enforcement hassles or the costs of regulation

seemingly goes right out the window. In reality, of course, privacy regulation will have profound consequences for online sites and services by potentially undermining the goose that lays the Internet's golden (and mostly free) eggs: online advertising and the data collection that powers it. Again, this is somewhat secondary to my point in this essay, which is just to suggest that the complexities associated with the mechanics of information control are not being fully considered in the privacy context. Either way, it's time we stop pretending privacy regulation is a free lunch.

Human advancement depends on innovation

Adam Thierer / Adam is a senior research fellow at the Mercatus Center at George Mason University. He previously served as President of the Progress & Freedom Foundation, Director of Telecom Studies at the Cato Institute, and Fellow in Economic Policy at the Heritage Foundation, March 10, 2013, Who Really Believes in Permissionless Innovation, <https://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation/>

I believe a strong case can be made that permissionless innovation should be our default position in public policy deliberations about technological change. Here's how I put it in the conclusion of my "Technopanics" article:

Resiliency and adaption strategies are generally superior to more restrictive approaches because they leave more breathing room for continuous learning and innovation through trial-and-error experimentation. Even when that experimentation may involve risk and the chance of mistake or failure, the result of such experimentation is wisdom and progress. As Friedrich August Hayek concisely wrote, "Humiliating to human pride as it may be, we must recognize that the advance and even preservation of civilization are dependent upon a maximum of opportunity for accidents to happen." I believe this is the more sensible default position toward technological innovation because the opposite default — a technological Precautionary Principle — essentially holds the “anything new is guilty until proven innocent,” as journalist Ronald Bailey has noted in critiquing the notion. When the law mandates “play it safe” as the default policy toward technological progress, progress is far less likely to occur at all. Social learning and adaptation become less likely, perhaps even impossible, under such a regime. In practical terms, it means fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living. Therefore, the default policy disposition toward innovation should be an “anti-Precautionary Principle.” Paul Ohm outlined that concept in his 2008 article, “The Myth of the Superuser: Fear, Risk, and Harm Online.” Ohm, who recently joined the Federal Trade Commission as a Senior Policy Advisor, began his essay by noting that “Fear of the powerful computer user, the ‘Superuser,’ dominates debates about online conflict,” but that this superuser is generally “a mythical figure” concocted by those who are typically quick to set forth worst-case scenarios about the impact of digital technology on society. Fear of the “superuser” and hypothetical worst-case scenarios prompts policy action, since as Ohm notes: “Policymakers, fearful of his power, too often overreact by passing overbroad, ambiguous laws intended to ensnare the Superuser but which are instead used against inculpable, ordinary users.” “This response is unwarranted,” Ohm argues “because the Superuser is often a marginal figure whose power has been greatly exaggerated.” (at 1327). Ohm correctly notes that Precautionary Principle policies are often the result. He prefers the “anti-Precautionary Principle” instead, which he summarized as follows: “when a conflict involves ordinary users in the main and Superusers only at the margins, the harms resulting from regulating the few cannot be justified.” (at 1394) In other words, policy should not be shaped by hypothetical fears and worst-case “boogeyman” scenarios. He elaborates as follows: Even if Congress adopts the Anti-Precautionary Principle and begins to demand better empirical evidence, it may conclude that the Superuser threat outweighs the harm from regulating. I am not arguing that Superusers should never be regulated or pursued. But given the checkered history of the search for Superusers — the overbroad laws that have ensnared non-Superuser innocents; the amount of money, time, and effort that could have been used to find many more non-Superuser criminals; and the spotty record of law enforcement successes — the hunt for the Superuser should be narrowed and restricted. Policymakers

seeking to regulate the Superuser can adopt a few strategies to narrowly target Superusers and minimally impact ordinary users. The chief evil of past efforts to regulate the Superuser has been the inexorable broadening of laws to cover metaphor-busting, impossible-to-predict future acts. To avoid the overbreadth trap, legislators should instead extend elements narrowly, focusing on that which separates the Superuser from the rest of us: his power over technology. They should, for example, write tightly constrained new elements that single out the use of power, or even, the use of unusual power. (at 1396-7)

To summarize, the Anti-Precautionary Principle generally holds the following answers to:

1. **society is better off when innovation is not preemptively restricted;**
2. **accusations of harm and calls for policy responses should not be premised on worst-case scenarios;** and,
3. remedies to actual harms should be narrowly tailored so that beneficial uses of technology are not derailed.

Slowing innovation kills

Eli Dourado is a research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program, February 6, 2013, “Permissionless Innovation” offline as well as on, <https://theumlaut.com/2013/02/06/permissionless-innovation-offline-as-well-as-on/>

Alternatively, look at the case of the Sensor Pad, a “medical device” barely worthy of the name. The device consists of two sheets of plastic with silicon lubricant in between. Despite its simplicity, the pad can help women detect breast lumps, potentially saving their lives. Yet the FDA demanded that costly clinical trials be conducted to determine the effect of the Sensor Pad on breast cancer mortality. The company that produced the Sensor Pad ultimately defied the FDA, resulting in a Congressional hearing that put pressure on the agency to approve the product, nine years after it was originally submitted.

These cases illustrate how the need to seek permission can harm innovation in the physical world, not just the virtual one. The costs of this forgone innovation are high. Left to tort-based regulation, the commercial drone industry might already be flourishing, resulting in new services, business models, companies, and jobs. And how many people died due to the unnecessary nine-year delay in approving the Sensor Pad? How many must die because other medical devices are never invented, because the existing regulatory model discourages innovation?

Data access pays for online content

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Second, and more broadly, there are social benefits to data analysis. As Professor Omer Tene and Jules Polonetsky note, the collection, use, and disclosure of personal data — even without consent — can lead to great benefits for individuals and society.⁷⁰ For example, many Internet companies that offer free web content use the analysis or sale of personal data as the main source of revenue.⁷¹ If many people refuse to

consent to the use of the data, these business models will fail. Thus, structurally, one of the benefits of data collection, use, and disclosure is that it pays for online content. There are deep problems with this state of affairs, as people are often not fully aware that they are paying for online content with their personal data,⁷² but legal restrictions on this business model would strike many as overly paternalistic.

Extensions – Targeted Advertising Good

Targeted advertising good for consumers

Berin Szoka / Berin is the founder and president of TechFreedom, a tech policy think tank based on pragmatic optimism about technology and skepticism about government, 2010, Privacy Trade-Offs: Comments on December 7 Privacy Workshop,
<https://techliberation.com/2009/11/11/privacy-trade-offs-pff-comments-on-december-7-ftc-privacy-workshop/>

The attached working paper I co-authored with PFF Visiting Fellow Mark Adams identifies five broad categories of benefits to users from targeted advertising:

1. More relevant, and potentially less annoying/interruptive advertising for consumers;
2. Higher-quality content and services supported by advertising;
3. Better correlation between the production of content and services, and consumer preferences;
4. A more vibrant media and improved political discourse and communities; and
5. Lower prices for consumers and greater innovation throughout the economy.

The paper explains how better targeting of advertising delivers these benefits by:

- Increasing the informational value of advertising to consumers;
- Increasing advertising funding for content and services that might not be sustainable on an ad-supported basis with untargeted or less targeted advertising; and
- Reducing the costs of buying and selling (“transaction costs”).

In particular, we note that, with behavioral targeting, the value of a site’s viewers depends less on the content associated with that site (keywords) and more on the viewers themselves. In this sense, behavioral advertising levels the playing field by allowing websites to sell access to viewers directly, rather than through the keywords associated with the website. Better targeting democratizes the ad-supported economy by empowering consumers to direct advertising revenues to the sites they spend time on. Targeting essentially increases the ability of Internet users to “vote with their clicks” for online content and services just as they “vote with their dollars” every time they make a purchase in the traditional economy.

Data on the precise “delta” between contextual and behavioral advertising is limited, but appears to indicate that behavioral advertising can produce significant increases in revenue for many publishers. In particular, we note the following increased measures of effectiveness

- Increased Click-Through-Rates 94% to 225% and conversion rates up to 3,000% (2005);[4]
- Increased CTR of 670-1000% (2009);[5] and
- Increased conversion rates of 400-900% (2008).[6]

There are a wide range of predictions on the potential value created by behavioral targeting. As with previous innovations in online advertising, it seems likely that the performance of behavioral targeting will

improve over time. Professor Tracy Tuten, author of **Advertising 2.0**, predicts that a twelvefold increase in the value of page views, from \$10 to \$120 per thousand views.^[7] Rich Karpinski calculates that Blue Kai, an ad network, is currently selling behaviorally targeted ads at a rate of \$4-15 per thousand views^[8]—a significantly lower rate than Ryan suggests but higher than the current performance of print advertising (\$5.50)^[9] and several times higher than the average price of non-premium display advertising (\$0.60-\$1.10).^[10] One experiment with re-targeting (showing users ads on one site based on actions taken towards making a purchase on one site but not completed) produced significantly higher returns: “retargeted impressions represented only 7% of all the banner impressions delivered, [but] were responsible for over 50% of the revenue and 25% of the sales generated by the campaign as a whole.”^[11] Hallerman concludes that “Behavioral targeting is more than hype.... For publishers, it can mean making more money from undersold or unsold ad inventory.”^[12]

Online world won't survive without advertising

Berin Szoka / Berin is the founder and president of TechFreedom, a tech policy think tank based on pragmatic optimism about technology and skepticism about government, 2010, Privacy Trade-Offs: Comments on December 7 Privacy Workshop,
<https://techliberation.com/2009/11/11/privacy-trade-offs-pff-comments-on-december-7-ftc-privacy-workshop/>

Traditionally, users “paid” for content by devoting part of their attention to ads, which have long funded the costs of generating content for radio, television, and newspapers (with subscriptions paying only for distribution).^[13] The basic reason is simple economics: In competitive markets, prices tend to fall to the marginal cost of production, which quickly converges on zero for information. The Internet has simply borne this theory out in full:

1. Producing the first unit of content (**e.g.**, a news story or video) remains costly, so while the **marginal** cost of every additional unit is essentially zero, **average** cost is not.
2. The failure of micropayments online seems to confirm that, no matter how low the technological transaction costs are, the mental transaction costs involved combined with even tiny payments will exceed the perceived value of most content.
3. The world of media scarcity in which consumers could choose from only a few sources of content (**e.g.**, news, entertainment) has given way to a world of staggering media abundance and the choices of users are no longer constrained by the tyranny of physical limitations like distance and printing costs.
4. Because pure information cannot be copyrighted (and fair use allows significant referencing and quotation), very little content is so unique that users cannot find a ready substitute elsewhere if a site (or even a group of sites) attempted to charge.

Thus, while policymakers should generally avoid preferring one business model over others, they must also recognize that the “economics of bits” will make advertising increasingly indispensable to the future of online content, services, media and culture. For that reason, they should take great care when tinkering with the economic engine that has made America the envy of the digital world as the fountainhead of online innovation and creativity.

Consumers do value targeted advertising

Berin Szoka / Berin is the founder and president of TechFreedom, a tech policy think tank based on pragmatic optimism about technology and skepticism about government, 2010, Privacy

Trade-Offs: Comments on December 7 Privacy Workshop,
<https://techliberation.com/2009/11/11/privacy-trade-offs-pff-comments-on-december-7-ftc-privacy-workshop/>

While many consumers said, in a recent poll, that they don't want ads, content and news "tailored" to their interests,[14] their actions in the real world speak louder than words: The increased click through rates and conversion rates mentioned above are evidence that consumers do, in fact, value more relevant advertising.[15] Whatever Americans tell pollsters about "tailored" ads, they also complain about irrelevant ads: A previous poll found that 72% of consumers "find online advertising intrusive and annoying when the products and services being advertised are not relevant to [their] wants and needs" and 85% say that less than 25% of the ads they see while browsing online are relevant to their wants and needs.[16]

Until a proper experiment is conducted by trained behavioral economists that includes real-world trade-offs and makes users aware of privacy management tools, all we can say with confidence is the following:

1. Users don't understand exactly how ads are tailored;
2. Users seem to be concerned about "tailoring" or "following" in the abstract;
3. Users are generally unwilling to pay for online content and services; and
4. Better tailoring of ads means more funding for content and services.

Only the layered approach outlined above can address all these concerns: educate users about how online advertising works and how they can implement their own privacy preferences, while constantly striving to further empower users to make privacy management easier.

Policymakers should avoid presuming they can divine the true preferences of users regarding the complex and multi-faceted trade-offs of the real world. Instead of guessing what consumers **might** choose, the FTC and other law enforcement agencies should focus on holding companies to the "expectations" they set in their official privacy policies and other statements about their any use and collection practices. In a sense, this is to approach the problem from the "supply" side rather than the "demand" side: If a browser manufacturer, for example, overstates the privacy protection offered by privacy management tools in the browser (**e.g.**, cookie settings or a private browsing mode), this might well be considered an unfair and deceptive trade practice subject to FTC enforcement. The advantage of this approach is that the FTC can, using its existing authority, play a valuable role in ensuring consistency between theory and practice in what industry actually does— without sending into the intractable morass of subjective user preferences. In other words, the FTC can help give effect to "household standards" without imposing "community standards" for everyone.

Many benefits of online ads

Berin Szoka, 2009 Progress and Freedom Foundation, Privacy Polls v. Real World Trade-Offs,
<http://www.pff.org/issues-pubs/ps/2009/ps5.10-privacy-polls-tradeoffs.html>

The Direct Benefit of Tailored Ads: Relevance

Whatever Americans tell pollsters about "tailored" ads, they also complain about irrelevant ads: A previous poll found that 72% of consumers "find online advertising intrusive and annoying when the products and services being advertised are not relevant to [their] wants and needs" and 85% say that less than 25% of the ads they see while browsing online are relevant to their wants and needs.[6] Real-world experiments confirm that users reveal a clear preference for more relevant advertising. In a 2004 experiment, click-

through rates (CTR) for behaviorally targeted ads were between 94% and 225% higher than for contextually targeted ads.[7] A 2009 study found that the difference could be between 670% and 1000% percent, depending on how well-tailored the ads were.[8] In other words, users in the real world were *two to eleven times* more likely to click on highly-tailored ads. Truly, actions speak louder than words: Users clearly "vote with their clicks" for ads they find relevant—*i.e.*, they vote for "tailoring."

Further reinforcing this conclusion is the fact that better tailoring increases not only click-through rates but also "conversion rates"—the percentage of users who actually complete the action desired by the advertiser, whether that be making a purchase or signing up for a list. A 2008 experiment found increased conversion rates of 400-900% (2008).[9] This indicates that relevant ads really do help consumers find things they like—and that they like the fruits of tailoring, however they respond when asked about "tailoring" as an abstract concept that conflates costs ("How are they following me?") and benefits ("What's in it for me?").

The Indirect Benefit of Tailored Ads: Free Content & Services

Even less apparent to poll respondents than the direct benefit of tailoring (increased relevance) are the indirect benefits: In particular, greater relevance to the user means more effective communication for the advertiser, and increased ad revenue for most online publishers per ad on their sites. Thus, there exists a clear *quid pro quo*: in effect, users "pay" for content and services by sharing information about their interests. Even more fundamentally, users "pay" for content by seeing ads. But both *quid pro quos* are implicit: Users can simply choose not to "pay" by using readily available tools in their browser to blocking ads and/or tracking. In essence, today's system allows users who don't like ads—tailored or otherwise—to opt out at little or no cost, much as if they simply decided not to pay for a product they bought at their local grocery store.

This creates a serious dilemma, given that advertising increasingly stands alone as the lifeblood of online content and services.[10] Indeed, ads have long funded the costs of generating content for radio, television, and newspapers (with subscriptions paying only for distribution).[11] The basic reason is simple economics: In competitive markets, prices tend to fall to the marginal cost of production. The Internet has simply borne this theory out in full:

1. Producing the first unit of content (*e.g.*, a news story or video) remains costly, so while the *marginal* cost of every additional unit is essentially zero, *average* cost is not.
2. The failure of micropayments online seems to confirm that, no matter how low the technological transaction costs are, the mental transaction costs involved combined with even tiny payments will exceed the perceived value of most content.
3. The world of media scarcity in which consumers could choose from only a few sources of content (*e.g.*, news, entertainment) has given way to a world of staggering media abundance and the choices of users are no longer constrained by the tyranny of physical limitations like distance and printing costs.

4. Because pure information cannot be copyrighted (and fair use allows significant referencing and quotation), very little content is so unique that users cannot find a ready substitute elsewhere if a site (or even cartel of sites) attempted to charge.

These forces have given birth to the world of "Free," where few (if any) users will pay for something they can get for nothing.[12] While there are a number of ways to fund content and services, advertising is far and away the leading business model for the new economy: Indeed, overall advertising market is expected nearly to double its share of total U.S. ad spending from 8.7% in 2008 (\$23.4 billion) to 15.2% (\$37.2 billion).[13] But with 44% of advertising revenue going to search engines (which show highly "tailored" ads simply based on search terms), hundreds of thousands of publishers—from the mightiest to the tiniest—rely on \$7.6 billion (33% of the total) in "display" ad revenue. Yet this base is tiny: Most websites earn a fraction of the revenue generated by offline ads: roughly \$0.60 to \$1.10 per thousand impressions (CPM) online versus average CPMs of \$4.54 (radio) to \$10.25 (broadcast). This unprofitability of online advertising, and the fact that certain kinds of online content (e.g., video and online services) does not provide the textual keywords necessary for basic contextual targeting is driving publishers to ad networks that offer behavioral targeting, which is expected to grow from \$525 million in 2007 to \$4.4 billion in 2012—when it will represent 25% of all display ad spending.[14]

In short, advertising is indispensable to the future of online media, but it is also currently inadequate to sustain "Free" culture. As Adam Thierer and I warned earlier this year: "The advocates of regulation pay lip service to the importance of advertising in funding online content and services but don't seem to understand that this *quid pro quo* is a fragile one: Tipping the balance, even slightly, could have major consequences for continued online creativity and innovation... *Something must give because there is no free lunch.*"[15] In 2001, long before Google mattered and before he worked for them, Kent Walker (now Google's general counsel) put it best in a seminal law review article:

Privacy is both an individual and a social good. Still, the no-free-lunch principle holds true. Legislating privacy comes at a cost: more notices and forms, higher prices, fewer free services, less convenience, and, often, less security. More broadly, if less tangibly, laws regulating privacy chill the creation of beneficial collective goods and erode social values... Such regulation would likely increase both direct and indirect costs to the individual consumer, reduce consumer choice, and inhibit the growing trend of personalization and tailoring of goods and services.[16]

Thus, as Jim Harper and Solveig Singleton concluded in their 2001 paper *With a Grain of Salt: What Privacy Surveys Don't Tell Us*:

privacy surveys in particular... suffer from the "talk is cheap" problem. It costs a consumer nothing to express a desire for federal law to protect privacy. But if such law became a reality, it will cost the economy as a whole, and consumers in particular, significant amounts that surveys do not and cannot reveal.[17]

People want targeted marketing

Daniel J. Solove, law professor, George Washington Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1895 (2013), http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Similarly, some people want targeted marketing. They want their data shared. They want catalogs to be mailed to their homes. They want to be tracked. They want to be profiled. They want companies to use their personal information to recommend products and services. These people should not be dismissed as uninformed or foolish, as it is far from clear that the costs to these people outweigh the benefits.

Big data critical to the survival of many firms

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

Aggregated information, or “big data,” is the fuel that powers much of the digital economy.¹⁹¹ Kenneth Cukier and Professor Viktor MayerSchönberger, authors of Big Data: A Revolution That Will Transform How We Live, Work, and Think, define “big data” as “the vast quantity of information now available thanks to the Internet, and which can be manipulated in ways never before possible.”¹⁹² It “is becoming a backbone of corporate performance and economic growth.”¹⁹³ For many online operators or digital media firms, information about their customers may be the firm’s only monetizable asset or intellectual property.¹⁹⁴ It allows those firms to better tailor services to existing customers while also finding new audiences or customers.¹⁹⁵ Professor Jonathan Ezor explains how data about users can be a valuable asset: Knowing the identity of current customers means that companies can offer a faster, more tailored experience, providing those goods or services the customer has previously or regularly purchased in a more prominent location, or being ready to give the customer “her usual.” Knowing who one’s potential customers are enables more effective sales pitches and solicitations; as much as consumers may be jaded when it comes to “personalized” messages in this database age, such messages are still more likely to catch their attention than those without the consumers’ names on the envelope or e-mail subject line. Companies have also long understood that their customer records may have value to other firms, and have sought to monetize that value. Whether through sharing, renting or selling customer lists, or by sending third-party solicitations to one’s own customers, businesses are able to lower costs and generate revenue well outside their ordinary operations through data mining and marketing, at times beyond the earnings potential from their core businesses.¹⁹⁶ The FTC acknowledges these realities, noting: “The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer data.”¹⁹⁷ This growth is equally true for the “apps economy,” which relies heavily on data collection and advertising.¹

Targeted ads benefit consumers and the economy

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-5B2013-George-Mason-Law-Rev%5D.pdf>

In a privacy-related BCA context, therefore, any regulatory proposal or enactment should be closely scrutinized to determine the impact on the overall health of the digital economy. Correspondingly, regulators should consider the aggregate amount of information and content that can be produced or supported by those sectors.²⁰⁴ A 2010 study by Howard Beales, former director of the Bureau of Consumer Protection at the FTC, found that “the price of [behaviorally targeted] advertising in 2009 was 2.68 times the price of run of network advertising.”²⁰⁵ That increased return on investment is important, Beales notes, because it creates “greater utility for consumers [from more relevant advertisements] and clear appeal for advertisers because of the increased conversion of ads into sales.”²⁰⁶ “Finally,” Beales continues, “a majority of network advertisers’ revenue is spent acquiring inventory, making [behavioral targeting] an important source of revenue for publishers as well as ad networks.”

General Answers

People voluntarily reveal massive amounts of information

Adam Thierer, George Mason University - Mercatus Center, Maine Law Review, 2014,
Privacy Law's Precautionary Problem,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2449308##

Compounding matters further still — especially for efforts to protect privacy — is the fact that we are our own worst enemies when it comes to information containment. Ours is a world of unprecedented individual information sharing through user-generation of content and self-revelation of data.¹² Moreover, decentralized peer-to-peer sharing and surveillance capabilities now exist that make it easier than ever for us to release information not only about ourselves but also about all those around us.

Privacy is vague and lacks a foundation

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

The inherent subjectivity of privacy as a personal and societal value is one reason why expanded regulation is not sensible. Privacy has long been a thorny philosophical and jurisprudential matter; few can agree on its contours or can cite firm constitutional grounding for the rights or restrictions they articulate.⁵

People adjust their behavior in recognition of the reality that privacy no longer exists

Jennifer Wortham, December 17, 2013, Instagram Direct and the Fracturing of Privacy,
http://bits.blogs.nytimes.com/2013/12/17/instagram-direct-and-the-evolution-of-privacy/?_r=0

There are fewer and fewer places we can really be ourselves online, a phenomenon that might not matter very much if you think that people should be spending more time with their friends in a physical space, instead of connecting with them online. But that isn't always practical — and the truth is, people spend the vast majority of their time talking to each other through a screen — and it is fun to have new and interesting ways to get in touch with them. At the same time, our notions of privacy are constantly evolving and in many cases, **being eroded altogether**. As a result, we're learning how to cope by adapting ourselves and our sharing behavior by deciding which version of ourselves to present based on the number of people who will be able to see it.

In many ways, we're fine-tuning our sharing behavior toward what attracts the most attention, posting images and videos that we think will get the biggest response and comments. Instagram Direct seems to be a response, or an acknowledgement of that shift. Which is not to say that Instagram Direct will somehow goad people into sharing their most private moments — it's still a mass-market product from Facebook, after all. But it

arrives at a time when people seem to be eager for better and less public ways to interact with their friends. That is the quiet cleverness of Instagram Direct.

Privacy remains protected in physical, property, and sanctity of the home against state actors

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

The most stable and widely accepted privacy rights in the United States have long been those that are tethered to unambiguous tangible or physical rights, such as rights in body and property, especially the sanctity of the home.²⁶ Moreover, these rights have been focused on limiting the power of state actors, not private parties.²⁷ By contrast, privacy claims premised on intangible or psychological harms have found far less support, and those claims have been particularly limited for private actors relative to the government.²⁸

Privacy undermines tailored advertising that benefits consumers

Berin Szoka / Berin is the founder and president of TechFreedom, a tech policy think tank based on pragmatic optimism about technology and skepticism about government, 2010, Privacy Trade-Offs: Comments on December 7 Privacy Workshop,
<https://techliberation.com/2009/11/11/privacy-trade-offs-pff-comments-on-december-7-ftc-privacy-workshop/>

In general, we at PFF have argued that any discussion about regulating the collection, sharing, and use of consumer information online must begin by recognizing the following:

- Privacy is “the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values.”^[1]
- As such, privacy is not a monolith but varies from user to user, from application to application and situation to situation.
- **There is no free lunch:** We cannot escape the trade-off between locking down information and the many benefits for consumers of the free flow of information.
- In particular, tailored advertising offers significant benefits to users, including potentially enormous increases in funding for the publishers of ad-supported content and services, improved information about products in general, and lower prices and increased innovation throughout the economy.
- Tailored advertising increases the effectiveness of speech of all kinds, whether the advertiser is “selling” products, services, ideas, political candidates or communities.

“Creepiness” of information sharing is not an objective harm

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

Precisely because the scope of privacy rights is so difficult to delimit, defining what constitutes “harm” in the context of information sharing and collection is similarly complicated. Some scholars have attempted to better delineate the nature and scope of privacy harms, but consensus remains elusive.³⁰ The recent FTC reports offer no clarification on the matter either.³¹ This Part focuses on the problems associated with one particular alleged privacy harm commonly associated with new information technologies and practices: “creepiness.” Practically every new information technology launched today is initially labeled “creepy” and creepiness is often the primary (or only) alleged harm that is cited as the basis of much online privacy regulation.³² Recently, for example, in various filings to the government as well as countless news stories, advocates of expanded privacy regulation have stressed the “creepiness” factor associated with targeted (or behavioral) advertising and the online data collection that makes such ads possible.³³ Concerns about “creepy” uses of wireless geolocation technologies are also increasingly commonplace, even though the public has simultaneously demonstrated an insatiable appetite for these new mobile networks and applications.³⁴ Finally, “creepiness” is a common lament heard whenever new social networking sites and services are launched. Jim Adler, Chief Privacy Officer and General Manager of Data Systems at Intelius, notes that “[w]ith increasing volume, ‘creepy’ has snuck its way in to [sic] the privacy lexicon and become a mainstay in conversations around online sharing and social networking.”³⁵ “How is it possible,” he wonders, “that we use the same word to describe Frankenstein and Facebook?”³⁶ But why should “creepiness” be the standard by which policymakers judge privacy harms at all? Although there will always be subjective squabbles over what constitutes harm as it relates to online privacy, and while many consumers will undoubtedly describe much online marketing and advertising as “creepy,”³⁷ law must be more concrete than the amorphous “creepiness” standard permits. “Creepiness” is simply too open-ended and subjective, and “creating new privacy rights cannot be justified simply because people feel vague unease.”³⁸ “[C]reepiness isn’t necessarily a sign that something is amiss” and “[a]s the history of technology shows, sometimes feelings are out of sync with reasonable responses.”³⁹ If privacy harm is reduced to “creepiness,” or even “annoyance,” such an amorphous standard for policy analysis or legal and regulatory action leaves much to the imagination and opens the door to creative theories of harm that may not actually represent true harm at all and could be exploited by those who ignore the complex tradeoffs at work when we attempt to regulate information flows online.⁴⁰ “Creepiness” is a hopelessly open-ended, eye-of-the-beholder standard that is no better than an “I-knew-it-when-I-see-it” standard for speech regulation: It would provide zero guidance to companies or courts when they are attempting to make privacy determinations. Employing a “creepiness” standard to gauge supposed privacy harm makes economic cost-benefit analysis virtually impossible, as policy considerations become purely about emotion instead of anything empirical.⁴¹ After all, one person’s “creepy” could be another’s “cool” or “killer” app. Personalized online shopping experiences, for example, might be considered too invasive by some, whereas others might greatly appreciate the benefits associated with tailored recommendations.⁴² Indeed, “more often than not, the creepy factor will go away without the need for intervention,” notes Larry Downes, because “[o]ver time, consumers either adjust to what is an essentially inert new information use, or act through the market to change the practice.

No harm to privacy violations by the private sector – they can't tax or imprison us

Adam Thierer, George Mason, 2014, January 23, Constitutional Amendment Restricting Private Sector Data Collection? <https://iapp.org/news/a/do-we-need-a-constitutional-amendment-restricting-private-sector-data-colle/>

Importantly, a private entity is just not the same as a government entity, and we should continue to distinguish between them when crafting data collection policies. Rosen says that “distinction between surveillance by the government and surveillance by Google makes little sense,” but in reality, the differences between public and private entities remains profound. Private entities cannot fine, tax or imprison us. And while we can escape the orbit of private companies and their services, the same is not true for governments.

Gmail proves people accept privacy limits in exchange for free services

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

For example, when Google launched its Gmail service in 2004, it was greeted with hostility by many privacy advocates and some policymakers.⁴⁴ Rather than charging some users for more storage or special features, Google paid for the service by showing advertisements next to each email “contextually” targeted to keywords in that email. Some privacy advocates worried that Google was going to “read users’ email,” however, and pushed for restrictions on such algorithmic contextual targeting.⁴⁵ But users enthusiastically embraced Gmail and the service grew rapidly. By the summer of 2012, Google announced that 425 million people were actively using Gmail.⁴⁶ Users adapted their privacy expectations to accommodate this new service, which offered them clear benefits (free service, generous storage, and improved search function).

Privacy norms and ethics are always changing

Adam Thierer, George Mason, 2014, January 23, Constitutional Amendment Restricting Private Sector Data Collection? <https://iapp.org/news/a/do-we-need-a-constitutional-amendment-restricting-private-sector-data-colle/>

Such paternalism is particularly problematic in this case since privacy is such a highly subjective value and one that evolves over time. As Solove notes, “the correct choices regarding privacy and data use are not always clear. For example, although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively.” Privacy norms and ethics are changing faster than ever today. One day’s “creepy” tool or service is often the next day’s “killer app.”

Privacy was eliminated before the IoT

Nick Bilton, December 15, 2013, New York Times, Disruptions: Internet's Sad Legacy: No More Secrets, http://bits.blogs.nytimes.com/2013/12/15/disruptions-internets-sad-legacy-no-more-secrets/?ref=technology&mtrref=bits.blogs.nytimes.com&_r=0

Anyone who can watch you will watch you. In technology, that is one of the big lessons of 2013. The National Security Agency and who knows who else have been tracking this or hacking that. China has been breaking into our computers. Google has been sifting through our home networks. Facebook has been tinkering with its privacy settings. No wonder outfits like Snapchat have exploded onto the scene. They seem to go against the grain, holding out the promise that all those selfies, texts and emails will simply vanish. Whisper, an “it” app for teens, supposedly lets people share secrets anonymously via smartphone. Telegram is being pitched as the adult version of Snapchat. But the fact is, many services that claim to offer that rarest of digital commodities — privacy — don’t really deliver. Read the fine print. “Just because information is unavailable to you and you don’t see it doesn’t mean that it is not being captured, stored, or even seen by someone else in transit,” said Edward W. Felten, a professor of computer science and public affairs at Princeton. Snapchat’s privacy page explains that private images are stored on someone’s phone — and on its own servers. “Forensically, even after they are deleted,” Snapchat says, those images can be retrieved. Whisper’s privacy page says the company owns the intellectual property, both images and text, that people post; Whisper reserves the right to sell that stuff to third parties. And Telegram, while seemingly less innocuous with its claims, nonetheless leaves out something you might want to know: someone can just take a screenshot or picture of that “private” conversation. Even if there are all sorts of technical barriers that the disappearing messaging services put up there, someone can just take a picture of the phone,” said Kurt Opsahl, a lawyer with the Electronic Frontier Foundation, a civil liberties organization. “If they can see it with their eyes, they can see it with a camera.” In most instances, your Internet service provider or cellphone carrier gets to watch over your shoulder with every click. Even when these messaging apps aren’t tracking your chats, the N.S.A. and other government agencies are. They’re everywhere. Even people who play fantasy video games like World of Warcraft are being watched, according to documents leaked by Edward J. Snowden.

We have laws to protect against the worst privacy violations

Adam Thierer / Adam is a senior research fellow at the Mercatus Center at George Mason University. He previously served as President of the Progress & Freedom Foundation, Director of Telecom Studies at the Cato Institute, and Fellow in Economic Policy at the Heritage Foundation, March 10, 2013, Who Really Believes in Permissionless Innovation, <https://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation/>

Of course, some alleged privacy harms involve highly sensitive forms of personal information and can do serious harm to person or property. Our legal regime has evolved to handle those harms. We have targeted legal remedies for health and financial privacy violations, for example, and state torts to fill other gaps. Meanwhile, the FTC has broad discretion under Section 5 of the Federal Trade Commission Act to pursue “unfair and deceptive practices,” including those that implicate privacy.

Claiming privacy is more important than the IoT just locks in existing technology and deprives people of innovation

PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 15, (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf, archived at <http://perma.cc/5YHWZ6EB>

Though privacy is important, this approach would be overkill, and it probably runs contrary to increasing overall social welfare. Information practices are evolving rapidly in light of the growth of the Internet and digital technologies. They should not be cabined at this early point, before we learn all the good things that can be done with information. Administrative regulation aimed at privacy would tend to lock in information practices that exist today, and deprive consumers of the benefits that future innovations would inevitably bring. “

Data collection keeps the price down

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

All these considerations and tradeoffs apply equally to IoT and wearable technologies. Health and fitness application providers already collect and sell a certain amount of user information to advertisers so they can create richer user profiles and deliver more relevant ads.²⁹⁶ Some users may find that creepy, but this process is what ensures the cost of such services remains low or even altogether free of charge. And users are always free to avoid such services completely if they fear such data collection practices.

Their privacy argument is paternalistic

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

In crafting use-based restrictions, however, policymakers must exercise caution. Overly broad restraints could end up being tantamount to a de facto ban on all uses of certain IoT or wearable technologies. Moreover, policymakers must avoid converting their preferences—or the preferences of just a small but vocal group of regulation advocates—into paternalistic policies that limit individual autonomy.²⁷³ The goal of privacy policy should not be to prevent people from making choices that others feel are unwise. [88] Privacy scholar Daniel J. Solove of the George Washington University School of Law has warned about privacy law’s “paternalism” problem.²⁷⁴ “Privacy regulation,” he notes, “risks becoming too paternalistic. Regulation that sidesteps consent denies people the freedom to make choices. The end result is that either people have choices that are not meaningful or people are denied choices altogether.”²⁷⁵ [89] Privacy is too subjective to have policymakers or academics dictating outcomes on the basis of their own preferences.²⁷⁶ As Solove notes, “the correct choices regarding privacy and data use are not always clear. For example, although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively.”²⁷⁷ Generally speaking, barring a clear showing of actual—not prospective or hypothetical—harm,²⁷⁸ U.S. culture has rejected the paternalistic idea that law must “save us from ourselves” (i.e., from citizens’ own irrationality or mistakes).²⁷⁹ Importantly, the term harm in this context has usually been narrowly defined as action that poses a direct threat to human well-being, personal property, or the home.

Privacy loss is worth the benefits

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

[90] That approach generally makes sense in light of both how subjective privacy can be and the high value Americans place on privacy in balancing it against other values, such as freedom of speech and journalistic freedoms (which will be discussed in the next section), as well as economic innovation and consumer choice. “We have fallen in love with this always-on world,” note Hal Abelson, Ken Ledeen, and Harry Lewis, authors of Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion.²⁸³ “We accept our loss of privacy in exchange for efficiency, convenience, and small price discounts.”²⁸⁴ Although many privacy advocates are loath to hear it, the reality is that “[w]e give away information about ourselves—voluntarily leave visible footprints of our daily lives—because we judge, perhaps without thinking about it very much, that the benefits outweigh the costs. To be sure, the benefits are many,” argue Abelson, Ledeen, and Lewis.²⁸⁵

Turn – Information collected protected by the First Amendment

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

But more than just journalistic freedoms are at stake here. The First Amendment protects the right of all citizens to observe and freely gather information about the world around them and to use various technologies to help them do so. As the Seventh Circuit explained in its 2012 decision in *ACLU v. Alvarez*, The act of making an audio or audiovisual recording is necessarily included within the First Amendment’s guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording. The right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of making the recording is wholly unprotected, as the State’s Attorney insists. By way of a simple analogy, banning photography or note-taking at a public event would raise serious First Amendment concerns; a law of that sort would obviously affect the right to publish the resulting photograph or disseminate a report derived from the notes. The same is true of a ban on audio and audiovisual recording.³⁰⁰

There are values other than privacy – innovation, entrepreneurialism, economic growth

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

Some of the privacy and security concerns about IoT and wearable technologies are legitimate and deserve responses. But those responses should not be top down or command and control in nature. Privacy and security are important values worthy of attention, but so too are innovation, entrepreneurialism, economic growth, price competition, and consumer choice. Regulation—especially regulation of fast-moving, rapidly evolving technologies—is likely to be premature and overly rigid and is unlikely to allow the many beneficial uses of these technologies.⁵ Such constraints would be highly unfortunate because these technologies “will have profound implications for addressing important social and economic issues.”⁶

IoT improves the quality of life, which is what their terminal impact is

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

The promise of IoT, as described by New York Times reporter Steve Lohr, is that “[b]illions of digital devices, from smartphones to sensors in homes, cars, and machines of all kinds, will communicate with each other to automate tasks and make life better.”⁴⁵ “Consumers and public officials can use the connected world to improve energy conservation, efficiency, productivity, public safety, health, education, and more,” predicts CEA.⁴⁶ “The connected devices and applications that consumers choose to adopt will make their lives easier, safer, healthier, less expensive, and more productive.”⁴⁷ In addition to giving consumers more control over their lives, these technologies can also help them free up time by automating routine tasks and chores.

At least half of society prefers free to privacy

Daniel Newman [CEO of Broadsuite Media Group], “There is No Privacy on the Internet of Things,” Forbes, 08/20/14, <http://www.forbes.com/sites/danielnewman/2014/08/20/there-is-noprivacy-on-the-internet-of-things/2/#75d558fc1333>

This feeling of connectedness undoubtedly gives many a sense of community and happiness as it is through the sharing of our everyday lives that we are able to garner the feedback we seek and the validity that we need. However, if we are fooled, for even a moment as to what all of this is really about; the desire to have us tethered without wires and connected without cost, then we are delusional. I for one can say that I have almost never read the privacy policy of an application I downloaded. As a millennial I suppose this puts me in the group of about [half of us that are okay with trading our privacy](#) for a potentially better experience online. Now whether having more targeted ads and content during our everyday browsing is really a better experience; that is yet to be seen. As a society, it really came down to our insatiable desire for free. Free content, free social media, free productivity tools and free games. We want to be connected and we want to play with the latest games, toys and widgets, but we by in large don’t want to trade our cash for them. So instead we trade something else; our data and our privacy. Just as long as you know what you are giving up and you make that choice then you are fine. But know, whatever you know “They” know and that is the way it will be.

You can shape how the data is used and control any privacy loss

Patrick Tusker, 2014, The Naked Future, Kindle edition, page number at end of card, Patrick Tucker is a science journalist and editor. Tucker's writing on emerging technology has appeared in The Atlantic, Defense One, Quartz, National Journal, Slate, Salon, The Sun, MIT Technology Review, Wilson Quarterly, The Futurist, BBC News Magazine, and Utne Reader, among other publications. Tucker, Patrick. The Naked Future: What Happens in a World That Anticipates Your Every Move? . Penguin Publishing Group. Kindle Edition.

Today, we've convinced ourselves that we can't have improved public safety without giving up liberty. But perhaps in the future, children will see this trade-off as unnecessary, a failure of imagination. We've discounted the possibility that we can use public data and personal data in ways that empower individuals without making them feel uncomfortably exposed or more dangerous to one another. Get involved in how your local department uses or plans to use advanced analytics. Start a Facebook page that discusses how more involvement in how local police treat data is the trade-off we have to make for greater safety. You may get the brush-off, or you may be surprised to discover a bunch of smart public servants who are eager for more citizen participation. When police chiefs confront the reality of how income, employment, housing density, schooling, taxation, and even urban planning affect robbery, assault, and murder, they often start sounding less like cops and a lot more like sociologists. Tucker, Patrick. The Naked Future: What Happens in a World That Anticipates Your Every Move? (pp. 221-222). Penguin Publishing Group. Kindle Edition.

Your data is owned by you and you can use it to improve your own life

Patrick Tusker, 2014, The Naked Future, Kindle edition, page number at end of card, Patrick Tucker is a science journalist and editor. Tucker's writing on emerging technology has appeared in The Atlantic, Defense One, Quartz, National Journal, Slate, Salon, The Sun, MIT Technology Review, Wilson Quarterly, The Futurist, BBC News Magazine, and Utne Reader, among other publications. Tucker, Patrick. The Naked Future: What Happens in a World That Anticipates Your Every Move? . Penguin Publishing Group. Kindle Edition.

The threat of creeping techno-totalitarianism is real. But the realization of our worst fears is not the inevitable result of growing computational capability. Just as the costs of using big data have decreased for institutions, those costs will continue to trend downward as systems improve and as consumer services spring up in a field that is currently dominated by business-to-business players. The balance of power will shift—somewhat—in favor of individuals. Your phone may be from Apple; your carrier may be AT&T; your browser may be Google; but your data is yours first because you created it through your actions. Think of it not as a liability but as an asset you can take ownership of and use. In the naked future, your data will help you live much more healthily, realize more of your own goals in less time, avoid inconvenience and danger, and, as detailed in this book, learn about yourself and your own future in a way that no generation in human history ever thought possible. In fact, your data is your best defense against coercive, Target-like marketing and perhaps even against intrusive government practices. Your data is nothing less than a superpower waiting to be harnessed. T

We still have choices to make. I'll discuss some of the forms those choices will take. But the worst possible move we as a society can make right now is demand that technological progress reverse itself. This is futile and shortsighted. We may be uncomfortable with the way companies, the NSA, and other groups use and abuse our information but that doesn't mean we will be producing less data anytime soon. As I mentioned earlier, according to the research group IDC there will be forty-four times as much digital information in 2020 as there was in 2009.⁴ You have a clear choice: use your data or someone else will. This is not a book about a change that is going to happen so much as a change that has already occurred but has yet to be acknowledged or fully felt. This is not a declaration of independence from corporate America, the government, or anything else. It's the record of our journey to this new place: the naked future. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (p. xviii). Penguin Publishing Group. Kindle Edition.

IoT outweighs privacy because it can stop a deadly flu outbreak, including the deadly bird flu

Patrick Tusker, 2014, *The Naked Future*, Kindle edition, page number at end of card, Patrick Tucker is a science journalist and editor. Tucker's writing on emerging technology has appeared in The Atlantic, Defense One, Quartz, National Journal, Slate, Salon, The Sun, MIT Technology Review, Wilson Quarterly, The Futurist, BBC News Magazine, and Utne Reader, among other publications. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* . Penguin Publishing Group. Kindle Edition.

PERHAPS you aren't yet convinced that the naked future offers any improvement to compensate for the sacrifice of privacy that it demands. Certainly, this new era will distribute rewards and punishments unfairly and unequally (sort of like the Old Testament depiction of God). But consider that every year millions of people in the United States truck themselves down to clinics for flu shots and wind up getting the flu anyway. According to epidemiologists, flu shots are 70 percent effective in the general population at most. The reason? Every shot contains an (inactive) mixture of only the three virus strains that epidemiologists believe are going to be prevalent in the coming season.² In the last several years, that has included strains of H3N2 (the base of the swine flu virus and several other influenza strains common in mammals), H1N1 (the famous bird flu), and a variety of influenza B strains, which are considered less dangerous and more likely to strike later in the flu season. But this is a small percentage of the types of flu known to be in existence. The Centers for Disease Control and Prevention (CDC) almost apologetically states on its Web site, "It's not possible to predict with certainty which flu viruses will predominate during a given season. Flu viruses are constantly changing (called 'antigenic drift')— they can change from one season to the next or they can even change within the course of one flu season. Experts must pick which viruses to include in the vaccine many months in advance in order for vaccine to be produced and delivered on time."³ Perhaps it's a sign of how far medicine has advanced that we, like naive children, simply assume the shots we get will actually work.³ In the last several years, the emergence of superlarge, publicly accessible databases of virus sequences such as the Global Initiative on Sharing All Influenza Data (GISaid)⁴ and the National

Institutes of Health's GenBank⁵ have greatly reduced bureaucratic barriers to finding and sharing the most current information about new influenza observations. Wider use of sequencing technology could lead to earlier detection of new types of flu, which would help pharmaceutical companies create better vaccines. Today, devices like Life Science's Ion Proton can sequence all 3 billion base pairs of the human genome in less than a day for a price of \$ 1,000, according to the machine's makers. With just eight ribonucleic acid (RNA) segments, influenza is an exponentially simpler organism to sequence than the human genome. But sequencing influenza is very rarely done at a nurse's office— what epidemiologists call "the point of surveillance." Instead, when flu samples are collected they're usually sent to a county or state public health lab, by which point a great deal of time has been lost. Collecting samples from birds and animals that are showing flu symptoms is, arguably, a more important step in curbing the spread of new deadly flu types. But that sort of sampling doesn't happen very often. As the editors of Nature pointed out in a recent Op-Ed: "Just 7 of the 39 countries with more than 100 million poultry in 2010 collected more than 1,000 avian flu samples between 2003 and 2011. Eight countries—Brazil, Morocco, the Philippines, Colombia, Ecuador, Algeria, Venezuela and the Dominican Republic— collected none at all . . ." 7, 8 The current state of flu detection leaves much to be desired. Yet the Josh Grant scenario outlined above could become reality within a decade. You can see its initial outlines today. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (p. 55). Penguin Publishing Group. Kindle Edition.

People can scramble their own data

Patrick Tusker, 2014, *The Naked Future*, Kindle edition, page number at end of card, Patrick Tucker is a science journalist and editor. Tucker's writing on emerging technology has appeared in The Atlantic, Defense One, Quartz, National Journal, Slate, Salon, The Sun, MIT Technology Review, Wilson Quarterly, The Futurist, BBC News Magazine, and Utne Reader, among other publications. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* . Penguin Publishing Group. Kindle Edition.

What can we do to protect our privacy in a world where its value is falling faster than that of last year's cell phone? One creative if tongue-in-cheek proposal comes from British artist Mark Shepard whose Sentient City Survival Kit includes such items as a CCD-Me-Not umbrella studded with 256 infrared light-emitting diodes (LEDs) to scramble the night vision of closed-circuit camera systems. My favorite item in the kit is the Under(a) ware, a set of undergarments that can detect RFID tags and vibrate to alert the wearer. "In the near future sentient shopping center, item level tagging and discrete data sniffing will become both pervasive corporate culture and a common common criminal pastime," states a computerized voice on the demo video. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (p. 217). Penguin Publishing Group. Kindle Edition.

Transparency reduces police abuse

Patrick Tusker, 2014, *The Naked Future*, Kindle edition, page number at end of card, Patrick Tucker is a science journalist and editor. Tucker's writing on emerging technology has appeared

in The Atlantic, Defense One, Quartz, National Journal, Slate, Salon, The Sun, MIT Technology Review, Wilson Quarterly, The Futurist, BBC News Magazine, and Utne Reader, among other publications. Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* . Penguin Publishing Group. Kindle Edition.

Unless our legal system becomes more transparent, accountable, and accessible we'll never feel certain that the people looking out for us won't abuse their power to persecute people who may technically be criminals but pose no real threat, such as pot smokers, prostitutes, and those who commit an act of trespass as part of a protest. How will we respond to this? Yes, we could put RFID tag readers in our underpants. Alternatively, we could decide to use surveillance and data to actually make the world safer and not abuse it. When you adopt the assumption that that's possible, opportunities open up. If the bad news is the cops are going to have a better window into your career as a lawbreaker, the good news is that in the naked future you're more than just a suspect on her way to her next crime; you're a set of probabilities, potential costs, and potential benefits. The challenge for all of us now is to make the price of overzealous or discriminatory policing both high and conspicuous. The benefits of good policing must be more readily obvious as well. The social and public costs of pestering and prosecuting people for petty crimes should be visible to citizens, lawmakers, and police all at once. Before that happens we may have to settle for those costs becoming more transparent to law enforcement, where at least some departments or agencies will use them as part of their decision making. The same sort of technology that took away your privacy is beginning to provide that opportunity.

Privacy can't be restored – technological and corporate invasions happen all the time.

Lewis 2014

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies. Previously, US Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service.

"Underestimating Risk in the Surveillance Debate" - Center For Strategic & International Studies - Strategic Technologies Program – December - <http://csis.org/publication/underestimating-risk-surveillance-debate>

On average, there are 16 tracking programs on every website.⁴ This means that when you visit a website, it collects and reports back to 16 companies on what you've looked at and what you have done. These programs are invisible to the user. They collect IP address, operating system and browser data, the name of the visiting computer, what you looked at, and how long you stayed. This data can be made even more valuable when it is matched with other data collections. Everything a consumer does online is tracked and collected. There is a thriving and largely invisible market in aggregating data on individuals and then selling it for commercial purposes. Data brokers collect utility bills, addresses, education, arrest records (arrests, not just convictions). All of this data is recorded, stored, and made available for sale. Social networking sites sell user data in some anonymized form so that every tweet or social media entry can be used to calculate market trends and refine advertising strategies. What can be predicted from this social media data is amazing—unemployment trends, disease outbreaks, consumption patterns for different groups, consumer preferences, and political trends. It is often more accurate than polling because it reflects peoples' actual behavior rather than the answer they think an interviewer wants to hear. Ironically, while the ability of U.S. agencies to use this commercial data is greatly restricted by law and policy, the same restrictions do not apply to foreign governments. The development of the Internet would have been very different and less dynamic if these business models had not been developed. They provide incentives and financial returns to develop or improve Internet services.

There is an implicit bargain where you give up privacy in exchange for services, but in bargains between service providers and consumers, one side holds most of the cards and there is little transparency. But the data-driven models of the Internet mean that it is an illusion to think that there is privacy online or that NSA is the only entity harvesting personal data.

Privacy is an unobtainable right – it always trades off with itself leading to circumvention of the plan's efforts

David Pozen 15, Associate Professor of Law at Columbia University, 6/28/15, 83

U. CHI. L. REV. __ (2015), “Privacy-Privacy Tradeoff,”

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2624281

Privacy clashes with important social values. We are told as much all the time.¹ Commentators struggle to reconcile privacy and security,² privacy and efficiency,³ privacy and technological innovation,⁴ and privacy and free speech, among other (real or imagined) antinomies. Privacy is constantly being juxtaposed with competing goods and interests, balanced against alternative needs and demands. Legal and policy debates about privacy revolve around these tradeoffs.

But privacy also clashes with itself. That is to say, in myriad social and regulatory contexts, enhancing or preserving privacy along a certain dimension may entail compromising privacy along another dimension. If they wish to be more analytically rigorous, theorists and decisionmakers must take such privacy-privacy tradeoffs into account. If they wish to advance the cause of privacy, civil libertarians must do the same.

Privacy-privacy tradeoffs come in a variety of flavors. Sometimes they are unexpected and unwanted. When EU citizens began exercising their right to be forgotten last year and flooded Google with “delete me” requests, the deleted links quickly reappeared—in more concentrated form—on a website devoted to documenting Internet censorship.⁷ Other times, privacy-privacy tradeoffs are consciously cultivated and promoted. The Transportation Security Administration’s PreCheck program invites travelers to “volunteer personal information in advance” if they wish “to leave on their shoes, belts and light outerwear and keep their laptops in their bags.” Enhanced governmental access to your data can be traded for reduced access to your body and belongings.

In many cases, privacy-privacy tradeoffs simply follow from scarce resources and opportunity costs. A tenant on a fixed budget who spends money soundproofing her walls will have less to spend on mending her window curtains or protecting her online identity. Alternatively, these tradeoffs may be caused by behavioral responses and dynamic feedback effects. Increasing airline-passenger privacy levels from X at Time 1 to a multiple of X at Time 2 may increase the odds of a terrorist attack, with the consequence that passengers’ privacy levels will be reduced to a fraction of X at Time 3. In still other cases, risk is redistributed across different aspects or bearers of privacy. By establishing a forensic DNA database, law enforcement officials may impair the privacy of everyone whose DNA is included but protect the privacy of a smaller group who will not be needlessly investigated for the crimes of others. By stripping its analysts of “any privacy or anonymity when they look at [collected] data,”⁹ an intelligence agency may deter them from exceeding their investigative mandates and thereby secure a measure of privacy for the rest of society—or at least for the analysts’ love interests.¹⁰

Privacy too vague to be legitimate

Chris DL Hunt 11, PhD Candidate in law and WM Tapp Scholar, Gonville & Caius College, University of Cambridge, “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort”, <http://queensu.ca/lawjournal/issues/pastissues/Volume37a/5-Hunt.pdf>)

The “right to be let alone” occupies a hallowed place in privacy discourse. Although the phrase was coined by Judge Cooley⁴²—who used it not to justify a right to privacy, but rather to explain why tort law regards trespass to the person as wrongful—it is now generally attributed to Warren and Brandeis, who invoked it throughout their seminal 1890 article.⁴³ The latter authors analyzed numerous cases of trespass, defamation, confidence, and especially common law copyright, and identified a latent principle of privacy—operating unarticulated—which they argued should thenceforth be protected independently, as a distinct tort.⁴⁴ This principle of privacy, expressed as a “right to be let alone”, is anchored in the more fundamental interest of an “inviolate personality”.⁴⁵ The Warren and Brandeis formulation has come under much academic criticism. The first problem is its vagueness.⁴⁶ Because neither the “right to be let alone” nor the concept of “inviolate personality” is adequately defined,⁴⁷ the article gives no practical or conceptual guidance on the scope of the right.⁴⁸ A related criticism is that the phrase “right to be let alone” itself appears to be less a definition of privacy than simply a description of one example of it.

Extensions – No Harm to Private Use of Data

No harm from commercial use of private data

Thomas M. Lenard & Paul H. Rubin, The Big Data Revolution: Privacy Considerations 24 (Dec. 2013), <https://techpolicyinstitute.org/wp-content/uploads/2013/12/the-big-data-revolution-privac-2007594.pdf>

Two additional themes running through some of the recent privacy literature suggest that the use of data and algorithms may produce “harms” quite different from what we normally think of as privacy and security harms (i.e., harms which involve the exposure of individuals’ data to people who shouldn’t see them). Some writers argue that big data will facilitate manipulating consumers to purchase things they don’t “really” want. Others are concerned that consumers will get too much of what they want—that they will live in a “filter bubble” determined by big data. The literature on misuse of algorithms does not present any evidence that is inconsistent with our conclusion that there is little demonstrable harm from the legal use of commercial information.⁵⁴

For example, Calo’s examples of “objective privacy harms” include: use of blood test data for drunk driving; data used for a no-fly list; police use of information from a psychologist.⁵⁵ None of these involve commercial information. The only example he uses of a commercial use is from Google gmail ads. But in this case, the consumer voluntarily uses the service in full knowledge that he will receive targeted ads. Moreover, the “harm” identified is speculative and quite indirect—consumers using the service are not typically aware of any harm. More generally, it is difficult to draw a boundary between what is called “manipulation” and the provision of information that helps a consumer in making purchases. For example, in a separate paper, Calo discusses profitable opportunities for firms to capitalize on irrational behavior.⁵⁶ As an example, he suggests that a harmful use of information would be to send an obese consumer a text message from a donut shop when the consumer is trying to avoid snacking. But of course the consumer might want a donut, even though Calo thinks he should not have one. Moreover, given the rate of evolution of apps, there will soon be one (if there is not now) that a diet conscious consumer with weak willpower could program to ignore all messages with certain keywords, including “donut”, or to remind him of the caloric content of the donut and his current weight-loss goal.

As Calo acknowledges, profiting from irrational behavior would be difficult (perhaps impossible) since it would be extremely difficult to determine what is rational for a given consumer.⁵⁷ Moreover, he does not explain why firms would want to do this. Using large data sets, firms might simply determine when they can sell products, and most of the time that would be to consumers who want the product, and that would generally be to rational consumers. Moreover, while some firms might try to sell products that the consumer does not “really” want, others would be trying to sell products that the consumer does want, and those firms can be expected to win out. The fundamental problem with this line of analysis is that many of the privacy advocates and writers on the subject do not trust the consumers for whom they purport to advocate. This is also apparent in writers who express concern about consumers living in a “filter bubble.” For example, Pariser laments that “[t]he statistical models that make up the filter bubble write off the outliers. But in human life it’s the outliers who make things interesting and give us inspiration.”⁵⁸ Dwork and Mulligan are concerned that “filter bubbles” will take away “the tumult of traditional public forums—sidewalks, public parks, and street corners—where a measure of randomness and unpredictability yields a mix of discoveries and encounters that contribute to a more informed populace.”⁵⁹

If consumers want variety, big data and algorithms, particularly as they get more sophisticated, should be helpful in providing that to them. However, the notion that algorithms will give consumers “too much” of what they want at the expense of what is good for them is a more

radical idea with unclear policy implications. Does it mean we should limit the collection and use of data to purposely produce less accurate algorithms? That doesn't seem to make much sense.

Extensions – People Voluntarily Share Info

People voluntarily share massive amounts of information

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

Finally, modern digital systems make it increasingly easy for anyone to be a one-person publishing house or self-broadcaster. As such, restrictions on information sharing, aggregation, and reuse will become increasingly difficult to devise and enforce.⁸⁰ This phenomenon is particularly relevant to any discussion of privacy regulation, as individuals are currently placing massive volumes of personal information online—both about themselves and others. “We live in what one might call the Peeping Tom society,” argues Professor Lawrence M. Friedman, in that “[n]ew technology puts powerful tools for invading privacy into the hands of ordinary people.”⁸¹ The rapid rise of data self-revelation leads many scholars to puzzle about the existence of a so-called “privacy paradox,” which refers to the fact that “[p]eople value their privacy, but then go out of their way to give it up.”⁸² Regardless, slowing such information flows through public policy will be remarkably challenging because many people continue to voluntarily release and widely distribute their personal information. Moreover, because of the highly connected nature of social networks and the sheer volume of information sharing that takes place across them, absolute privacy control becomes an impossible task. For example, in 2011, Facebook reported that its users submitted around 650,000 comments on the 100 million pieces of content served up every minute on its site.⁸³ And Hilbert and López found that humankind shared 65 exabytes of information in 2007,⁸⁴ the equivalent of every person in the world sending out the contents of six newspapers every day, they estimate.⁸⁵ Not all of that shared information was personal information, of course, but much of it probably was. This problem will be exacerbated by the increasing ubiquity of mobile computing and communications devices that capture and reproduce information instantaneously.⁸⁶ For example, most adults and many teenagers today carry a powerful digital sensor or surveillance technology with them at all times: their mobile phones.⁸⁷ Individuals use these technologies to record audio and video of themselves and the world around them and instantaneously share that data with many others.

Extensions – Isn’t/Can’t Define

Privacy is subjective and poorly defined

PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 15, (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf, archived at <http://perma.cc/5YHWZ6EB>

We can understand them better by considering them as such. Indeed, “privacy” itself needs to be recognized as a particular state of affairs having to do with information, rather than a confused jumble of different problems. For too long, privacy has been a catchword for any number of concerns that face us as we enter the digital age. People commonly use the words “privacy” and “security” interchangeably, despite important differences. They refer to the serious crime problem of identity fraud as a “privacy” problem. And they object to spam — millions of e-mails sent in the absence of knowledge about the recipient — as an invasion of “privacy.” These significant information policy problems each relate to privacy in different ways, but they are not at the heart of privacy itself. In the absence of a useful definition, the term “privacy” has done more to frustrate than to help the people who want to solve these important policy problems.

Privacilla.org has proposed a definition of privacy that is intended to assist people working seriously to solve privacy-related public policy problems: Privacy is a subjective condition that exists when two factors are in place. First, one must have legal power to control information about one’s self. Second, one must have exercised that power consistent with his or her interests and values. Importantly, privacy is a subjective condition. This means that individuals determine its contours for themselves based on their own highly personal wants and needs. Through experience, upbringing, and culture, each person develops a sense of privacy that is his or her own. One person can not tell another what his or her sense of privacy should be. Nor can legislators or regulators determine for an entire society what information practices deliver privacy to the people in it.

Privacy is subjective and constantly changing

PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 15, (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf, archived at <http://perma.cc/5YHWZ6EB>

Privacy is also emphatically not an area where preventing risk requires a high degree of technical expertise. Privacy is a social construct, not a technical matter. People’s definitions of privacy are subjective; in each individual, privacy competes with other interests. Privacy is also constantly changing for individuals and for society as a whole. Attempts to treat privacy as a technical matter are foolishness.

Measuring privacy emotional, intangible, impracticable

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

The fundamental problem with applying BCA to digital privacy proposals is that—as with online safety policy—it is riddled with emotional appeals⁷² and highly subjective assertions of harm.⁷³ This makes it challenging to satisfy the first prerequisite of BCA: to provide “a clear explanation of the need for the regulatory action, including a description of the problem that the agency seeks to address.”⁷⁴ Further complicating matters is the fact that, as Professor Alessandro Acquisti has noted, “[t]here may be privacy considerations that affect individuals’ well-being and are not merely intangible, but in fact immeasurable.”⁷⁵ Again, the same is true for online safety. What constitutes optimal “safety” and “privacy” online is both hopelessly subjective⁷⁶ and difficult to quantify.⁷⁷

Can't define privacy

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

Professor Daniel J. Solove has noted that privacy has long been a “conceptual jungle” and a “concept in disarray.”¹⁸ “[T]he attempt to locate the ‘essential’ or ‘core’ characteristics of privacy has led to failure,” he says.¹⁹ “Privacy has really ceased to be helpful as a term to guide policy in the United States,” argues Professor Woodrow Hartzog, “because privacy means so many different things to so many different people.”²⁰

Vagueness means it isn't a formal right

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

Of course, privacy has always been a highly subjective philosophical concept.²² It is also a constantly morphing notion that evolves as societal attitudes adjust to new cultural and technological realities.²³ For these reasons, America may never be able to achieve a coherent fixed definition of the term or determine when it constitutes a formal right outside of some narrow contexts.

Extensions – No Impact

Privacy harms can't be demonstrated under widely accepted tests

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

These factors might explain why the Obama administration and other public officials have failed to fully grapple with the question of privacy harms in their recent privacy reports and statements. Under traditional harms-based analysis, agencies consider whether concrete harms exist and then weigh the benefits of regulation against its costs.⁹⁴ The FTC formalized this process in its 1984 Policy Statement on Unfairness.⁹⁵ This statement clarified for members of Congress how the FTC interpreted and enforced its statutorily granted authority under Section 5 of the Federal Trade Commission Act.⁹⁶ Section 5 prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁹⁷ In its unfairness policy statement, the agency noted that, “To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.”⁹⁸ As two former FTC officials have noted, this “is essentially a cost-benefit test.”⁹⁹ Of particular relevance to BCA for privacy enactments is the agency’s requirement in the policy statement that “the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. . . . Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair.”¹⁰⁰

Privacy happiness are values we can pursue, but they are not rights

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

In one sense, the FTC’s abandonment of strict harms-based analysis is understandable. Elsewhere I have argued that efforts to delineate the scope of privacy rights and associated harms may prove a quixotic quest, similar to a hypothetical effort to define a “right to happiness” and “happiness harms.”¹⁰³ This is not to say that privacy, safety, or even happiness are unimportant values. To the contrary, everyone would agree that these values are important and that we have the right to pursue them.¹⁰⁴ But efforts to define them as “rights” and to delineate associated “harms” will always be extraordinarily challenging.

Everyone does not value privacy

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

Public policy discussions about digital privacy often treat privacy as a value that is shared equally by all. This is an error. “In the real world, preferences are rarely so uniform,” notes practitioner Meredith Kapushion.¹⁶¹ “Consumers have wildly divergent preferences based on their individual needs and tempered by the costs they are willing to bear.”

Extensions—Benefits of the Services Outweigh People won’t pay for the services

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-5B2013-George-Mason-Law-Rev%5D.pdf>

Despite the lack of empirical data, some analysts suggest that paying for online services would help consumers achieve greater privacy protections. “Truly, the only way to get around the privacy problems inherent in advertising-supported social networks is to pay for services that we value,” argues Alexis Madrigal of The Atlantic.¹⁶⁶ “It’s amazing what power we gain in becoming paying customers instead of the product being sold.”¹⁶⁷ It remains unclear, however, whether web users would be willing to pay for what we might think of as a “privacy premium” for online sites and services that would presumably collect less personal information or serve up no targeted advertising. As noted, even if more online operators offered pay-for-service options, it is unclear whether they would differentiate themselves from rivals by focusing on privacy or safety enhancements. Paid offerings are just as likely—perhaps far more likely—to be tailored to other user desires. In other words, it remains uncertain how much of a market there is for privacy, and this further complicates the question of whether any sort of market failure exists in this context.

Sure, people like privacy, but prefer free convenient services

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-5B2013-George-Mason-Law-Rev%5D.pdf>

In a sense, there is no more a “privacy paradox” than there is a “milk paradox”: people will say they want milk, and they will gladly accept it if it is being offered for free.¹⁷⁹ The fact that they want less of it when they have to pay for it is, therefore, not a paradox. By extension, “if privacy were free, we would all want more.”¹⁸⁰ Yet, when faced with real-world trade-offs—higher prices, less service, lower quality products, etc.—many people reveal that they are willing to trade privacy for other benefits. Importantly, lab experiments,¹⁸¹ surveys, and public opinion polls¹⁸² represent a poor substitute for real-world WTP analysis. All too often, privacy advocates and policymakers make assertions about online safety and digital privacy based largely upon such polling or survey data.¹⁸³ Yet, polls typically fail to offer useful insights regarding how much people actually value safety and privacy relative to the benefits they receive. “Empirical research on [privacy] is still in its infancy,”¹⁸⁴ notes New York Times reporter Somini Sengupta. “Most studies ask for personal opinion, rather than measure the digital choices people make, and even there, the results usually find a gap between what people say and what they do about their privacy online.”¹⁸⁵ Often, this discrepancy is because polls ask simplistic questions about whether consumers care about their privacy without requiring the respondents to even bother with the mental calculus of evaluating the trade-offs associated with regulations aimed at enhancing online privacy.¹⁸⁶ Even then, some polls suggest privacy isn’t as big a concern as some regulatory advocates suggest.¹⁸⁷ Of course, how polling questions are framed likely has a profound bearing on how much people say they value privacy.¹⁸⁸ Regardless, simply because people say they are concerned about privacy

does not mean they will pay a premium for it.¹⁸⁹ Further analysis, and more careful WTP/WTA analysis, is necessary when conducting BCA for privacy proposals.¹⁹⁰

Privacy Bad – Social Cohesion

Privacy undermines social cohesion

Kelsey Finch, Westin Research Fellow, International Association of Privacy Professionals, 2015, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town,” FORDHAM URBAN LAW JOURNAL v. 41, <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2549&context=ulj>,

Now, they can blend into the masses, leading an individual life and proactively managing their engagement—and data sharing—with relatives, friends, and colleagues.⁶⁶ Moreover, in the city “[t]here can be something enjoyable, even revelatory about that feeling of selfprotection.”⁶⁷ Virginia Woolf, among other modern authors, was fascinated by this aspect of city life, and highlighted in Mrs. Dalloway “the feeling of solitude-on-display that the sidewalk encourages, and by the way that ‘street haunting,’ as she called it, allows you to lose and then find yourself in the rhythm of urban novelty and familiarity.”⁶⁸ At the same time, this urban anonymity also imposes steep costs—including the loss of social cohesion and a sense of community; the unresponsiveness of local government to citizen concerns; and the inevitable loneliness of an anonymous life.

Privacy Bad – Gender

Privacy used to protect men's dominance over women in that sphere

Steven G. Gey, John W. and Ashley E. Frost Professor of Law, Florida State University College of Law, "The Case Against Postmodern Censorship," UNIVERSITY OF PENNSYLVANIA LAW REVIEW, "v. 145 n. 2, 12—96, pp. 193-297

Criticism of the notion that the government should respect a realm of "private" expression has long been a fixture in both critical race and feminist literature. Feminists, in particular, have produced a large body of work analyzing the concept of privacy, including private expression. In many ways, criticism of the concept of privacy is the linchpin of Catharine MacKinnon's version of feminism. She views the legal protection of privacy as a key way in which government has historically shunted the concerns of women into a no-woman's-land, and excluded women from the sorts of protective social intervention that have traditionally protected men.

Privacy constructs a sphere where men can oppress women

Steven G. Gey, John W. and Ashley E. Frost Professor of Law, Florida State University College of Law, "The Case Against Postmodern Censorship," UNIVERSITY OF PENNSYLVANIA LAW REVIEW, "v. 145 n. 2, 12—96, pp. 193-297

The feminist critique of privacy is a subset of the theory's broader critique of the concept of human freedom. At its most extreme, this critique denies the very existence of freedom-especially freedom cast in the form of free will. MacKinnon's statement that, "[t]he liberal ideal ... holds that, so long as the public does not interfere, autonomous individuals interact freely and equally,"⁶ correctly points out that the concept of privacy is closely tied to notions of human freedom, and that both freedom and privacy are essential elements of liberal democratic theory. According to MacKinnon, these presumptions of freedom are inapplicable to women: [Privacy] is personal, intimate, autonomous, particular, individual, the original source and final outpost of the self, gender neutral. It is, in short, defined by everything that feminism reveals women have never been allowed to be or to have, and everything that women have been equated with and defined in terms of men's ability to have.⁷ The liberal notion of privacy is, according to MacKinnon, "a right of men 'to be let alone' to oppress women one at a time. It embodies and reflects the private sphere's existing definition of womanhood.... It keeps some men out of the bedrooms of other men."⁸

In MacKinnon's view, protection of privacy amounts to protection of systematic domination. In this way, MacKinnon views privacy as an automatic ally of the status quo. Specifically, she asserts that "[t]he existing distribution of power and resources within the private sphere will be precisely what the law of privacy exists to protect."⁹ MacKinnon would abandon the protection of privacy, as well as every other major premise of current First Amendment doctrine, including the "most basic assumption" that any speech is truly free. She would, quite literally, turn First Amendment doctrine on its head and impose a new definition of "freedom" in the form of government control in the service of particular social goals. This new definition is necessary because "[f]or women, the urgent issue of freedom of speech is not primarily the avoidance of state intervention as such, but finding an affirmative means to get access to speech for those to whom it has been denied."¹⁰ This means not just expanding the universe of speakers by using

government resources to give women and other subjugated people access to the means of communication; it means using the coercive apparatus of government to suppress pornography and other "expressive means of practicing inequality," " even if they occur in private.

Note – Gey thinks privacy is good but references these arguments to identify a kritik of it. You can find the original kritik here –

CATHARINE A. MACKINNON, Privacy v. Equality: Beyond Roe v. Wade, in FEMINISM UNMODIFIED,

CATHARINE A. MACKINNON, TOWARD A FEMINIST THEORY OF THE STATE 204 (1989).

Answers –

An excellent starting point is: Ruth Gavison, Feminism and the Public/Private Distinction, 45 STAN. L. REV. 1, 2 (1992) ("When the external elements of [the feminist challenge to the public/private distinction] become too sweeping.... they become misleading and counterproductive and may actually facilitate the devaluation of important aspects of human life that are currently identified as 'private' and .personal."").

Discrimination Answers

Laws solve discrimination

Adam Thierer, Senior Research Fellow, Mercatus Center at George Mason University, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>

For example, if policymakers attempt to craft a use-based restriction that prohibits the use of wearable data on grounds that it could be used to discriminate against users, lawmakers should narrowly tailor that rule to address truly invidious forms of racial, sexual, or religious discrimination.²⁸⁹ Of course, many antidiscrimination laws that might make such practices illegal anyway already exist.²⁹⁰ But the term discrimination should not be construed to include any form of service differentiation, such as tailored product offerings that help expand the range of consumer services.²⁹¹ In the future, some IoT developers might craft creative data sharing policies that provide consumers with a wide variety of unanticipated benefits. Serendipitous discoveries and datadriven innovation can materialize only in a policy environment that embraces trial-and-error experimentation.²⁹² That is why flexible data collection and use proposals and evolving best practices will ultimately serve consumers better than one-size-fits all, top-down regulatory edicts.

Free Speech Turn

Limits the exchange of information threatens the First Amendment

Adam Thierer, George Mason University, 2013, Harvard Law Review, The Pursuit of Privacy Where Information Control is Failing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680

Taken to the extreme, however, giving such a notion the force of law would put privacy rights on a direct collision course with the First Amendment, and press rights in particular.⁵⁵ For instance, Professor Eugene Volokh has argued that Answers to: The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me. We already have a code of “fair information practices,” and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is “fair” or not.⁵⁶

Data mining and sales are protected by the First Amendment

Adam Thierer, George Mason, Mercatus Center, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 GEO. MASON L. REV. 1055, 1066–69 (2013),
<https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-%5B2013-George-Mason-Law-Rev%5D.pdf>

In the wake of the Supreme Court’s 2011 decision in Sorrell v. IMS Health Inc.,²²⁶ these First Amendment concerns are even more relevant.²²⁷ Sorrell dealt with a state law prohibiting data aggregators from selling personal information to pharmaceutical companies, which in turn use the data to customize their marketing pitches to doctors.²²⁸ The Court held that restrictions on the sale, disclosure, and use of personally-identifying information were subject to heightened judicial scrutiny.²²⁹ Agreeing with the lower court, the Supreme Court found that the regulation violated the First Amendment because it restricts the speech rights of data miners without directly advancing legitimate state interests.²³⁰ In line with its ruling in Thompson v. Western States Medical Center,²³¹ the Court noted that “‘the fear that people would make bad decisions if given truthful information’ cannot justify content-based burdens on speech.”²³²

First Amendment/free speech outweighs privacy

Neil Richards, law professor, Washington University, 2015, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Kindle edition, page number at end of card

Despite the complexity of privacy, speech, and the Internet, my argument boils down to two simple ideas. First, I suggest that when free speech and traditional notions of privacy conflict, free speech should almost always win. Warren and Brandeis thought of privacy as a tort action against newspaper gossip causing emotional harm. Their idea that privacy and speech are in conflict has framed how we think about privacy in the legal system and in the wider world. But as I will show, the Warren and Brandeis argument for tort privacy was flawed even on its own terms in

1890. Over a century later, their argument is inconsistent with a society committed to free speech and robust public debate. Our commitment to free speech means we must reject their argument in almost all cases. Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (p. 4). Oxford University Press. Kindle Edition.

Answer to Affirmative Arguments

AT Surveillance State

The surveillance state is too pervasive. All branches and agencies, plus corporations, exercise biopower over the people; NSA only reform will fail.

Whitehead, 5-16-15 [John, constitutional and human rights attorney, and founder of the Rutherford Institute, "The NSA's Technotyranny: One Nation Under Surveillance," WashingtonsBlog, 5-16-15, <http://www.washingtonsblog.com/2015/05/the-nsas-technotyranny-one-nation-under-surveillance.html>]

The National Security Agency (NSA) has been a perfect red herring, distracting us from the government's broader, technology-driven campaign to render us helpless in the face of its prying eyes. In fact, long before the NSA became the agency we loved to hate, the Justice Department, the FBI, and the Drug Enforcement Administration were carrying out their own secret mass surveillance on an unsuspecting populace. Just about every branch of the government—from the Postal Service to the Treasury Department and every agency in between—now has its own surveillance sector, authorized to spy on the American people. Then there are the fusion and counterterrorism centers that gather all of the data from the smaller government spies—the police, public health officials, transportation, etc.—and make it accessible for all those in power. And of course that doesn't even begin to touch on the complicity of the corporate sector, which buys and sells us from cradle to grave, until we have no more data left to mine. The raging debate over the fate of the NSA's blatantly unconstitutional, illegal and ongoing domestic surveillance programs is just so much noise, what Shakespeare referred to as "sound and fury, signifying nothing." It means nothing: the legislation, the revelations, the task forces, and the filibusters. The government is not giving up, nor is it giving in. It has long since ceased to take orders from "we the people."

NSA surveillance isn't analogous to Foucault's Panopticon. At best, reactions to rather than applications of surveillance are comparable.

McGraw, '13 [Bryan, Associate Professor of Politics at Wheaton College, "How NSA Surveillance is NOT Like Foucault (but our reactions are)," Civitas Peregrina, June 11, 2013, <https://civitasperegrina.wordpress.com/2013/06/11/how-nsa-surveillance-is-not-like-foucault-but-our-reactions-are/>]

It's easy to see why we might then jump from the NSA's Prism program to Foucault. But here's what makes Foucault's argument interesting and not just some obtuse forerunner of the "X Files" (or any other conspiracy minded move/tv show). One of the panopticon's key features was that the tower where the guards resided was mirrored so that the prisoners could not tell if they were actually under observation at any particular moment. In fact, they need not be under observation at all for the tower to do its job. Foucault's view was that our liberal society was indeed one of deep disciplining, but it was not the case that there was a "them" that was doing the disciplining. Rather, we all are caught up and participate in our mutual disciplining. We are, to Foucault's mind, our own oppressors in that we impose a kind of "normalization" on one another. What the NSA=Foucault folks suppose is that Foucault had in mind a social order in which some small elite, armed with technologies and power, would herd the rest of us into docile compliance. Foucault's argument was actually much more worrisome: that all of us, armed with the ordinary technologies of communication and observation, would herd ourselves into docile submission. So the NSA program (whatever its merits and demerits) isn't Foucauldian. Rather, I would argue, it is our reactions – where commentators assume their expected positions, offer ritualized expressions of support or outrage, and punish (via dialogue) those who range outside the bounds of "proper" discourse – that reminds me of Foucault.

Alternative Causality: the modern Imperial Presidency is the root cause of Foucauldian biopower.

Smith, '13 [Reid, Freedom Works' staff writer and editor, "The Surveillance State in Your Head," The American Conservative, July 19, 2013,
<http://www.theamericanconservative.com/articles/the-surveillance-state-in-your-head/>]

With the fall of the Soviet Union, there was hope that the imperial presidency would be scaled back by Congress, but such optimism proved hollow. In The Cult of the Presidency, Gene Healy notes that while partisan rhetoric today is as acerbic as it has been in decades, Republicans and Democrats alike accept the bottomless depth of executive responsibility and the president's unique grasp on power. We've normalized dependence on his guidance and our subordination. The modern president has greatly exceeded, in size and scope, the few enumerated powers initially bestowed upon him and in the process has become a great deal more powerful—and potentially more dangerous. His powers of surveillance and social compulsion are virtually unmatched in human history. From a Foucauldian perspective, one might argue our president (Bush or Obama, it hardly matters) has staked his claim as our watchman. We become increasingly aware that all we do takes place under surveillance, and our dull surprise at this revelation suggests our submission to the system—the inevitable outcome of our assent to political power.

Foucauldian critique of NSA surveillance is impossible under modern capitalism. Current power structures are self-reinforcing.

Bruno, '14 [Zachary, BA, Critical Theory, Occidental College, "The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden," March 24, 2014,
<http://www.zachcbruno.com/academic/dd-preview/images/pdf/PrismProgramPanopticon.pdf>]

With this, Foucault would propose that critiquing the NSA's illicit surveillance program would first require deconstructing the structures of power and discursive claims making which surround it. In this regard, Reeves (2003) argues that a self-reinforcing dynamics exists, as it pertains to the discourses and power structures sustaining such governmental tools. In this regard, the difficulty of critiquing them, in the sense which Foucault (1995) intends, is related to the manner in which this power is self-reinforcing. Indeed, to garner a better understanding of the difficulties of critique in such a context, one need only examine Foucault's work on sexuality, repression, and biopolitics-based social control to understand the operation of these mechanisms. With the above in mind, what becomes most apparent, from considering Foucault's portrayal of the diffusion of normalizing power in contemporary society, is that it is impossible to resist the potency of this power from within modern society itself. Given that the latter is permeated with multiple structures of repression, often invisible to the human eye, or already internalized to such a degree that we are no longer capable of even recognizing their existence; it becomes clear that we live in a social context in which resistance through critique, within society, is at least temporarily impossible. If a social revolution were to ever undo the structures of normalizing power which currently permeate our social interactions, it might become possible to rebuild a society without the concentrations of capital, and thus power, which prevail today. In the interim, however, resisting and informally critiquing within the confines of organized modern capitalist society is a futile endeavor because of the all-too-deep entrenchment of those entities which regulate us, and force us to adopt certain behaviors in spite of our desires. Thus, because the entirety of our society has been permeated by these powerful exogenous forces, there is no true potential for resistance within society. Instead, because we cannot necessarily understand or confront all of the elements of our oppression, it is clear that resistance to the forces identified by Foucault must take place outside of mainstream society. On this basis, critique of the everyday colloquial variety is impossible simply because it necessitates that we accept and take for granted the imposed structures of meaning which emerge from society's most significant power bases.

The American populace cannot engage in Foucauldian critique of NSA surveillance because of disciplinary structures like the War on Terror.

Bruno, '14 [Zachary, BA, Critical Theory, Occidental College, "The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden," March 24, 2014, <http://www.zachcbruno.com/academic/dd-preview/images/pdf/PrismProgramPanopticon.pdf>]

Applied to the context of the NSA's surveillance Panopticon, the ultimate reality of the impossibility of critique is one wherein it is impossible for the American mass to understand the multiple structures of oppression inherent to the PRISM Program. Indeed, the apathy discussed by Zurchner (2014) is likely an embodiment of a context wherein the American population is blinded by the other disciplinary structures, like the purported threats of the War on Terror, which serve to maintain high levels of fear in American society. In this regard, the work of Lokaneeta (2010) suggests that these, associated with the notion of American governmentality, have preponderated in the post-9/11 context because of the visceral power of the discourse of threat which the Bush and Obama Administrations have spread.

AT Overload

Alt Causes

Alt causes – data reduction isn't enough to solve Zoldan, 13

Ari Zoldan is an entrepreneur in the technology industry and business analyst based primarily in New York City and Washington, D.C. “More Data, More Problems: is Big Data Always Right?” Wired, May 2013, <http://www.wired.com/2013/05/more-data-more-problems-is-big-data-always-right/> // IS

How do we fight the problems of big data? First, we need to approach every data set with skepticism. You have to assume that the data has inherent flaws, and that just because something seems statistically right, doesn't mean it is. Second, you need to realize that data is a tool, not a course of action. Would you ask your hammer how to build a house? Of course not! You can't let the data do the thinking for you, and can never sacrifice common sense. And third, having a lot of data is good, but what we need are the means to analyze and interpret it for use.

Inev

Overload is inevitable and quick-fix solutions fail

Bawden & Robinson, Department of Information Science City University

London, '08 (David Bawden; Lyn Robinson, Department of Information Science, City

University London, “The dark side of information: overload, anxiety and other paradoxes and pathologies” 9/19/2008 http://www.bollettinoadapt.it/old/files/document/21976david_b-2008.pdf) //GY

While it is true to say that overload has been recognised most clearly in the business and commercial sectors, and in specialist areas such as science and healthcare, it has been a matter of concern to information specialists in all environments, including academic and public libraries. It may be argued that information overload is the natural and inevitable condition of the human species. There has been a consistent viewpoint suggesting that the issue is exaggerated, or even imagined: see, for example, Savolainen [23]. Our senses, particularly the visual sense, are able to handle a huge amount of input, and to identify significant patterns within it. The modern information environment, however, presents us with information in forms with which our senses, and prior experiences, are ill-equipped to deal. The causes of overload, in this sense, are multiple and complex; hence the difficulty in providing any single “quick fix” solution. It is tempting, and usual, to assume that a major contributing factor, if not the only significant factor, in information overload is the TMI effect: “too much information”. This is readily supported by statistics of the sort often quoted [17]: a weekly edition of the New York Times contains more information than the average person was likely to come across in a lifetime in seventeenth-century England; the English language of the late 20th century contains about 50,000 words, five times more than in Shakespeare’s lifetime; the collections of the large US research libraries doubled between 1876 and 1990; over one thousand books were published each day across the world during 1990; more information has been created in the past 30 years than in the previous 5,000 years; the number of records in publicly available online databases increased from 52 million in 1975 to 6.3 thousand million in 1994; the number of documents on the Internet doubled from 400 million to 800 million from 1998 to 2000; it would take over 200,000 years to ‘read all the Internet’, allowing 30 minutes per document. Increasing diversity of information can also lead to overload, partly by virtue of a consequent increase in the volume of information on a given topic, which may come from varying perspectives, but also because of an intellectual difficulty in fitting it within a cognitive framework appropriate for the use and the user.

Diversity may occur both in the nature of the information itself, and in the format in which it appears, with a typical business user having to deal with paper, e-mail, voicemail, traditional websites, and so on, to which the newer blogs, wikis and the like must be added. New information and communication technologies, aimed at providing rapid and convenient access to information, are themselves responsible for a high proportion of the overload effect: see, for example, Allen and Shoard [24]. Certain kinds of technology are generally highlighted in this respect, particularly “push” systems, which actively deliver information to the user without any request for it. While the volume of information available for search and retrieve at the user’s discretion—“pull”—may be so large as to be daunting, there is not the same sense of information constantly arriving without being under the user’s control as with the active delivery systems. E-mail is usually regarded as the worst offender, particularly with overuse of “blanket” e-mail or needless “cc-ing” of messages.

More data good

Bitcoin avoids PRISM compliance—the plan prevents federal data collection on it through domestic companies

Neagle, 13

(Colin, 6-12-13, Network World, “Bitcoin isn't PRISM-proof”,
<http://www.networkworld.com/article/2167213/software/bitcoin-isn-t-prism-proof.html>, amp)

In the aftermath of the revelation of PRISM, the NSA spying program that collects user data from nine major U.S. tech companies, many have highlighted alternate options from organizations that are not known to be cooperating with government surveillance efforts.

Among those alternatives, Bitcoin has been pegged as a more private payment option. At Prism-Break.org, which lists alternatives to all the services that fall under the PRISM umbrella, Bitcoin is the only listed alternative to online payment services, such as PayPal and Google Wallet.

Bitcoin ATM is 'horrible for money laundering', says co-creator

But users should know that Bitcoin is not as anonymous as it seems, and while there is no evidence that Bitcoin services are collaborating with federal agencies, information on Bitcoin transactions is readily available to them on the Internet.

A 2011 study conducted by University College Dublin researchers Fergal Reid and Martin Harrigan concluded that although anonymity has been one of Bitcoin's main selling points, “Bitcoin is not inherently anonymous.”

“We have performed a passive analysis of anonymity in the Bitcoin system using publicly available data and tools from network analysis,” the researchers wrote in a blog post. “The results show that the actions of many users are far from anonymous. We note that several centralized services, e.g. exchanges, mixers and wallet services, have access to even more information should they wish to piece together users' activity. We also point out that an active analysis, using say marked Bitcoins and collaborating users, could reveal even more details.”

In 2012, the publicly available data on Bitcoin transactions was used by researchers Adi Shamir and Dorit Ron to identify the first ever transaction on the network, which is believed to be from an account held by Bitcoin's mysterious creator, known only as Satoshi Nakamoto. While these transactions were covered up quite well, Ron and Shamir concluded that they are not entirely untraceable.

“Finally, we noted that the subgraph which contains these large transactions along with their neighborhood has many strange looking structures which could be an attempt to conceal the existence and relationship between these transactions, but such an attempt can be foiled by following the money trail in a sufficiently persistent way,” the report explains.

This may not come as a surprise to the most passionate members of the Bitcoin community, who look at Bitcoin as a movement to revolutionize online payments, rather than a tool to remain anonymous on the Internet. Zach Harvey, co-founder of Lamassu and co-creator of the Bitcoin ATM, says Bitcoin is actually “horrible for money laundering” because the veil of anonymity can be lifted.

Indeed, late last month the online currency exchange service Liberty Network, which is similar to Bitcoin, was infiltrated by international law enforcement agencies that allege it laundered more than \$6 billion in money for criminal organizations. The investigation was brought down after an undercover agent created an account on Liberty Network and listed the purpose as “cocaine.”

Basically, if independent researchers can trace Bitcoin transactions back to the people responsible, and the U.S. government can investigate digital currencies hosted overseas (Liberty Network was based in Costa Rica), then the NSA, CIA, FBI or any other federal agency can likely peek into Bitcoin activity as well.

Extra-PRISM authorities are key to investigate the Dark Web Green, 15

(Shemmyla, 4-19-15, Cyberbear Tracks, “Exploring the Deep Web”,
<http://cyberbeartracks.com/?p=545>, amp)

Darknet is a subsection of Deep Web that is accessed by Tor. Tor is a web browser, like Chrome or Safari, and free software that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. It sends Internet data through a series of ‘relays’, adding extra encryption, making web traffic practically impossible to trace. This is the place where much of the anonymous dark, perverted, creepy and illegal activity is, but is it truly anonymous? If the FBI truly seized the Silk Road’s servers illegally and based off what has been discovered about NSA and Prism, the answer is no.

“There is no such thing as really being anonymous on the Internet. If [hackers and government agencies] want you, they will get you. At the moment the Tor network’s security has never been broken, but there are flaws around it that can be exploited,” Andy Malone, of Microsoft Enterprise Security and founder of the Cyber Crime Security Forum, said at the Microsoft TechEd North America 2014.

Now let’s discuss PRISM and the NSA. PRISM is a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major Internet services like Gmail, Facebook, Outlook, and others. It’s the latest evolution of the US government’s post-9/11 electronic surveillance efforts, which began under President Bush with the Patriot Act, and expanded to include the Foreign Intelligence Surveillance Act (FISA) amended in 2006 and 2007. NSA programs collect two kinds of data: metadata and content. Metadata is the sensitive byproduct of communications, such as phone records that reveal the participants, times, and durations of calls; the communications collected by PRISM include the contents of emails, chats, VoIP calls, cloud-stored files, and more. This method of catching criminals appears very intrusive to the average law abiding citizen and is a violation of our 4th Amendment rights. In order to obtain search warrant law enforcement officers must:

1. Have probable cause to believe a search is justified.
2. Support this showing with sworn statements (affidavits), and
3. Describe in particularity the place they will search and the items they will seize.

Not the polar opposite method.

Bitcoin and the dark web cause lone wolf terrorism

Terence **Check 13**, J.D. Candidate, Cleveland-Marshall College of Law, 5/5/13, “Shadow currency: how Bitcoin can finance terrorism,” <http://theworldoutline.com/2013/05/shadow-currency-how-bitcoin-can-finance-terrorism/>

This “crypto-currency” has already been the inspiration for several online robberies where cyber-thieves hack into a computer to steal the vital electronic information at the heart of Bitcoins. Beyond cyber-larceny, the secrecy of **Bitcoin poses unique**, and even frightening **security challenges** for a world that has yet to fully understand the problems posed by the internet age.

For example, consider the various national and international anti-money laundering statutes. These laws seek to prevent the illegal flow of currency between criminals, terrorists and other unsavory characters. But these laws require that there are actual shipments of cash between countries and criminal networks (or at the very least funds transfers between banks).

The **Bitcoin** protocol **promises to remove the fundamental risk in money laundering**, **the risk of interception and detection**. By using a monetary exchange like Mt.Gox, criminals can buy Bitcoins at the market rate and then they can sell to a confederate across the world at a higher price, effectuating the exchange of money. Even if Bitcoin performs poorly, it nevertheless provides an opportunity to exchange money via the anonymous P2P network.

The Silk Road can make Bitcoin even more insidious. While the Silk Road, as site policy, **forbids the sale of destructive items** (stolen credit cards, explosives, etc.), **it could be a matter of time before a similar website arises**. Then, the **firearms laws of the Western world will become virtually useless**. Guns can be disassembled, and their parts shipped piecemeal through the postal service. Even **substances like Tannerite could be bought and shipped across the globe, providing new opportunities for destructive capacity**. If this alone is not enough to compel attention to the **growing black market on cyberspace**, consider the following.

Bitcoin can make security and law enforcement measures less effective by simply **removing the possibility of detection**. **Terrorist cells or lone wolf operators** can get supplies and currency by using the anonymous underbelly of the internet. Government agents are able to **detect terrorists through logistical networks** (Usama bin Laden was found through his courier). **Counter-terrorism**, for better or worse, **succeeds when it has human networks to exploit**. **Terrorists need accomplices**, handlers, recruits, and suppliers. Sooner or later, one of the individuals in this vast network becomes frightened or disillusioned with the cause and becomes a government informant. **Remove the extended logistical network that exposes terrorists to investigation** at a critical juncture (where their plans are neither theoretical nor well-supplied enough to implement) **and there may be grievous results**.

So what legal paths can be utilized to make sure such a development does not occur? **The easiest and most effective way to deal with this threat is to make sure that it never comes into fruition**. The Silk Road is difficult to take down given its place within the “Deep Internet”, but an arms-trading counterpart may be more susceptible to infiltration and dismemberment.

The second option spells doom for electronic currencies. Much like domestic laws that flag large banking transactions, **governments** and the private sector **can collude to run Bitcoin out of the currency market**. Simply put, **laws could** be passed that **force banks to reject bitcoin transactions**. Thus, **even if Bitcoins continue to be traded, there is no way to turn them back into real currency**. The final approach would require nations to expand the police power of domestic and foreign intelligence agencies on the web. While there is a visceral aversion to government personnel infiltrating internet communications, the ultimate security benefits may outweigh the cost to certain freedoms.

Metadata is the crux of counterterrorism—key to hindsight and prediction Hines, 13

(Pierre, defense council member of the Truman National Security Project, 6-19-13, Quartz, “Here’s how metadata on billions of phone calls predicts terrorist attacks”, <http://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/>, amp)

Yesterday, when NSA Director General Keith Alexander testified before the House Committee on Intelligence, he declared that the NSA’s surveillance programs have provided “critical leads to help prevent over 50 potential terrorist events.” FBI Deputy Director Sean Boyce elaborated by describing four instances when the NSA’s surveillance programs have had an impact: (1) when an intercepted email from a terrorist in Pakistan led to foiling a plan to bomb of the New York subway system; (2) when NSA’s programs helped prevent a plot to bomb the New York Stock Exchange; (3) when intelligence led to the arrest of a U.S. citizen who planned to bomb the Danish Newspaper office that published cartoon depictions of the Prophet Muhammad; and (4) when the NSA’s programs triggered reopening the 9/11 investigation.

So what are the practical applications of internet and phone records gathered from two NSA programs? And how can “metadata” actually prevent terrorist attacks?

Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted. Section 215 of the Patriot Act provides the legal authority to obtain “business records” from phone companies. Meanwhile, the NSA uses Section 702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According to the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases.

One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists’ planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat.

Even more useful than hindsight is a crystal ball that gives the intelligence community a look into the future. Simply knowing how many individuals are in a chat room, how many individuals have contacted a particular phone user, or how many individuals are on an email chain could serve as an indicator of how many terrorists are involved in a plot. Furthermore, knowing when a suspect

communicates can help identify his patterns of behavior. For instance, metadata can help establish whether a suspect communicates sporadically or on a set pattern (e.g., making a call every Saturday at 2 p.m.). Any deviation from that pattern could indicate that the plan changed at a certain point; any phone number or email address used consistently and then not at all could indicate that a suspect has stopped communicating with an associate. Additionally, a rapid increase in communication could indicate that an attack is about to happen.

Metadata can provide all of this information without ever exposing the content of a phone call or email. If the metadata reveals the suspect is engaged in terrorist activities, then obtaining a warrant would allow intelligence officials to actually monitor the content of the suspect's communication.

In Gen. Alexander's words, "These programs have protected our country and allies . . . [t]hese programs have been approved by the administration, Congress, and the courts." Now, Americans will have to decide whether they agree.

Mass collections solves terror – all data is important

Schulberg, Huffington Post, 5/10 (Jessica Schulberg, correspondent Huffington Post, MA international politics "Richard Burr Says 9/11 Could Have Been Preventable With Mass Surveillance" 05/10/2015 http://www.huffingtonpost.com/2015/05/10/burr-patriot-act-911_n_7251814.html) //GY

Sen. Richard Burr (R-N.C.) said on Sunday that the Sept. 11, 2001, attacks may have been preventable if the bulk phone collection program that exists today under the Patriot Act was in effect back then. Speaking on ABC's "This Week," Burr, who chairs the Senate Intelligence Committee, rejected the idea of returning to a narrower surveillance program that would only collect data on people suspected of being terrorists. "That turns us back to pre-9/11," said Burr. "It was very time consuming, it was cumbersome." Explaining the decision to pass the Patriot Act, Burr said, "What we looked at was the impact of 9/11 and the fact that we might have been able to stop 9/11, had we had bulk collection." Three sections of the Patriot Act, the law passed immediately after the attacks, are set to expire June 1 (but May 22 is the last day Congress has to act before going into recess). One key provision that is set to expire is Section 215, which has served as the legal justification for the government's phone records collection program. ¶ "I do think it should continue for the simple reason that it's very effective at keeping America safe," Burr said Sunday. "And in addition to that, we've had absolutely no incident of anybody's privacy being intruded on." ¶ The already contentious debate about whether to reauthorize the program has been further complicated by Thursday's federal appeals court ruling, which found that Congress did not authorize the phone collections program in its current form when it passed the Patriot Act. ¶ Sen. Ron Johnson (R-Wis.), chairman of the Senate Homeland Security Committee, was quick to note that the court's ruling did not definitively rule out the legality of such a program. ¶ "It's important to note that the Second Circuit Court of Appeals did not rule it unconstitutional," he said Sunday on CNN's "State of the Union." "They just said it was not being applied properly based on the law that was written. So we need to take a very careful look at the way we write these, quite honestly, very complex laws." ¶ Johnson criticized Edward Snowden's revelations about the program as "demagoguery" that has "done great harm to our ability to gather information." He added, "Our best line of defense, trying to keep this nation safe and secure, is an effective intelligence-gathering capability, with robust congressional oversight." ¶ Sen. Ron

Wyden (D-Ore.) promised on Sunday to filibuster a reauthorization of the Patriot Act unless it includes significant reforms.¶

Squo solves – Big Data

No NSA overload – Big Data solves

Rosenbach et al. 13 (Marcel Rosenbach, German journalist, Holger Stark, Professor at the University of Göttingen, and Jonathan Stock, German Journalist, 6/10, "Prism Exposed: Data Surveillance with Global Implications", <http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761-2.html//Tang>)

It is now clear that what experts suspected for years is in fact true -- that the NSA monitors every form of electronic communication around the globe. This fact raises an important question: How can an intelligence agency, even one as large and well-staffed as the NSA with its 40,000 employees, work meaningfully with such a flood of information? The answer to this question is part of a phenomenon that is currently a major topic for the business community as well and goes by the name "Big Data." Thanks to new database technologies, it is now possible to connect entirely disparate forms of data and analyze them automatically. A rare glimpse into what intelligence services can do by applying this "big data" approach came last year from David Petraeus. This new form of data analysis is concerned with discovering "non-obvious relationships," the then freshly minted CIA director explained at a conference. This includes, for example "finding connections between a purchase here, a phone call there, a grainy video, customs and immigration information." The goal, according to Petraeus, is for big data to "lead to automated discovery, rather than depending on the right analyst asking the right question." Algorithms pick out connections automatically from the unstructured sea of data they trawl. "The CIA and our intelligence community partners must be able to swim in the ocean of 'Big Data.' Indeed, we must be world class swimmers -- the best, in fact," the CIA director continued. The Surveillance State The value of big data analysis for US intelligence agencies can be seen in the amount the NSA and CIA are investing in it. Not only does this include multimillion-dollar contracts with providers specializing in data mining services, but the CIA also invests directly, through its subsidiary company In-Q-Tel, in several big data start-ups. It's about rendering people and their behavior predictable. The NSA's research projects aim to forecast, on the basis of telephone data and Twitter and Facebook posts, when uprisings, social protests and other events will occur. The agency is also researching new methods of analysis for surveillance videos with the hopes of recognizing conspicuous behavior before an attack is committed. Gus Hunt, the CIA's chief technology officer, made a forthright admission in March: "We fundamentally try to collect everything and hang onto it forever." What he meant by "everything," Hunt also made clear: "It is really very nearly within our grasp to be able to compute on all human-generated information," he said. That statement is difficult to reconcile with the Fourth Amendment to the US Constitution, which guarantees the right to privacy. This is probably why Hunt added, almost apologetically: "Technology in this world is moving faster than government or law can keep up."

Squo solves overload – big data

Segal, 14

Mark E. Segal, Chief of the Computer and Information Sciences Research Group at the NSA, "Guest Editor's Column," The Next Wave, 11/28/14,
<https://www.nsa.gov/research/tnw/tnw204/article1.shtml // IS>

As Big Data analytics become more ubiquitous, concerns naturally arise about how data is collected, analyzed, and used. In particular, people whose data is stored in vast data repositories, regardless of who owns the repositories, are worried about potential privacy rights violations. Although privacy issues are not discussed in detail in this issue of TNW, an excellent overview of the relevant issues may be found in a report titled "Big Data and privacy: A technological perspective" authored by the President's Council of Advisors on Science and Technology and delivered to President Obama in May 2014 [1]. Another useful resource on this topic and other topics related to Big Data is the article "Big Data and its technical challenges" by H. V. Jagadish et al. published in the July 2014 issue of Communications of the ACM [2].

According to a 2012 study by the International Data Corporation, there will be approximately 1022 bytes of data stored in all of the computers on Earth by 2015 [3]. To put that number in perspective, that's more than the estimated 7.5×10^{18} grains of sand on all of the beaches of the Earth [4], and almost as much as the estimated 1022 to 1024 stars in the Universe [5, 6]. Let's harness the tools and algorithms currently being used to process Big Data to solve some of our planet's most critical problems. We hope you find this issue of TNW interesting, informative, and thought-provoking.

Squo solves - CC

Squo solves overload – cloud computing

Burkhardt, 14

Paul Burkhardt, computer science researcher in the Research Directorate at NSA. He received his PhD from the University of Illinois at Urbana-Champaign. “An overview of Big Data,” The Next Wave, 11/28/14, <https://www.nsa.gov/research/tnw/tnw204/article2.shtml> // IS

The volume and velocity of Big Data is exceeding our rate of physical storage and computing capacity, creating scalability demands that far outpace hardware innovations. Just as multicore chips were designed in response to the limits of clock speeds imposed by Moore’s Law, cloud technologies have surfaced to address the impending tidal wave of information. The new cloud architectures pioneered by Google and Amazon extended distributed computing from its roots in high-performance computing and grid computing, where hardware was expensive and purpose-built, to large clusters made from low-cost commodity computers, ushering the paradigm of “warehouse” computing. These new cloud data centers containing thousands of computer cabinets are patrolled by administrators on motorized carts to pull and replace failed components.

Squo Solves – gov checks

Squo solves overload – government checks

Gross 13

Grant Gross, citing a former civil liberties watchdog in the Obama White House, “Critics question whether NSA data collection is effective,” PC World, 6/25/13,
http://www.pcworld.idg.com.au/article/465878/critics_question_whether_nsa_data_collection_effective/ // IS

But Timothy Edgar, a former civil liberties watchdog in the Obama White House and at the Office of Director of National Intelligence, partly defended the NSA collection programs, noting that U.S. intelligence officials attribute the surveillance programs with preventing more than 50 terrorist actions. Some critics have disputed those assertions.

Edgar criticized President Barack Obama's administration for keeping the NSA programs secret. He also said it was "ridiculous" for Obama to suggest that U.S. residents shouldn't be concerned about privacy because the NSA is collecting phone metadata and not the content of phone calls. Information about who people call and when they call is sensitive, he said.

But Edgar, now a visiting fellow at the Watson Institute for International Studies at Brown University, also said that Congress, the Foreign Intelligence Surveillance Court and internal auditors provide some oversight of the data collection programs, with more checks on data collection in place in the U.S. than in many other countries. Analysts can query the phone records database only if they see a connection to terrorism, he said.

Squo solves - investment

Squo solves overload – investment

Burkhardt, 14

Paul Burkhardt, computer science researcher in the Research Directorate at NSA. He received his PhD from the University of Illinois at Urbana-Champaign. “An overview of Big Data,” The Next Wave, 11/28/14, <https://www.nsa.gov/research/tnw/tnw204/article2.shtml> // IS

In March 2012, the White House announced the National Big Data Research and Development Initiative [14] to help address challenges facing the government, in response to the President’s Council of Advisors on Science and Technology, which concluded the “Federal Government is under-investing in technologies related to Big Data.” With a budget of over \$200 million and support of six federal departments and agencies, this initiative was created to:

Advance state-of-the-art core technologies needed to collect, store, preserve, manage, analyze, and share huge quantities of data;

Harness these technologies to accelerate the pace of discovery in science and engineering, strengthen our national security, and transform teaching and learning; and

Expand the workforce needed to develop and use Big Data technologies.

As part of the Big Data Initiative, the National Science Foundation (NSF) and the National Institutes of Health are funding a joint Big Data solicitation to “advance the core scientific and technological means of managing, analyzing, visualizing, and extracting useful information from large and diverse data sets.” In addition, the NSF is funding the \$10 million Expeditions in Computing project led by University of California at Berkeley, to turn data into knowledge and insight, and funding a \$2 million award for a research training group to support training for students in techniques for analyzing and visualizing complex data.

The Department of Defense (DoD) is also investing \$250 million annually to “harness and utilize massive data in new ways” and another \$60 million for new research proposals. DARPA, the research arm of the DoD, will invest \$25 million annually under its XDATA program for techniques and tools to analyze large volumes of data, including

Developing scalable algorithms for processing imperfect data in distributed data stores, and

Creating effective human-computer interaction tools for facilitating rapidly customizable visual reasoning for diverse missions.

The Department of Energy is similarly providing \$25 million in funding to establish the Scalable Data Management, Analysis and Visualization Institute to develop new tools for managing and visualizing data.

Squo Solves - research

Squo solves overload – Research Direcorate NSA, 11

NSA, on a website describing its internal structure for its “premier unclassified event,” “Government Host Descriptions,” 2011, http://www.ncsi.com/nsabiam11/host_descriptions.html // IS

In the NSA/CSS Research Directorate, opportunities abound. We are committed to providing the tools, the technology, and the techniques to ensure the success of the Agency’s Signals Intelligence and Information Assurance missions now and in the future. Our vital research program focuses on four critical goals: We develop the means to dominate the global computing and communications network. We cope with the overload of information in our environment and turn that overload to our strategic advantage. We provide the means for ubiquitous, secure collaboration both within our government and through its interactions with various partners. We create the means for penetrating into the “hard” targets that threaten our nation wherever, whenever, or whomever they many be.

Squo solves - tech

New technology means no overload

Rosenbach et al, '13 (By Marcel Rosenbach, Holger Stark and Jonathan Stock – acclaimed German political scientists and journalists “Prism Exposed: Data Surveillance with Global Implications” Spiegel Online International, June 10, 2013
<http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761-2.html>) //GY

It is now clear that what experts suspected for years is in fact true -- that the NSA monitors every form of electronic communication around the globe. This fact raises an important question: How can an intelligence agency, even one as large and well-staffed as the NSA with its 40,000 employees, work meaningfully with such a flood of information?¶ The answer to this question is part of a phenomenon that is currently a major topic for the business community as well and goes by the name "Big Data." Thanks to new database technologies, it is now possible to connect entirely disparate forms of data and analyze them automatically.¶ A rare glimpse into what intelligence services can do by applying this "big data" approach came last year from David Petraeus. This new form of data analysis is concerned with discovering "non-obvious relationships," the then freshly minted CIA director explained at a conference. This includes, for example "finding connections between a purchase here, a phone call there, a grainy video, customs and immigration information."¶ The goal, according to Petraeus, is for big data to "lead to automated discovery, rather than depending on the right analyst asking the right question." Algorithms pick out connections automatically from the unstructured sea of data they trawl. "The CIA and our intelligence community partners must be able to swim in the ocean of 'Big Data.' Indeed, we must be world class swimmers -- the best, in fact," the CIA director continued.¶ The Surveillance State. The value of big data analysis for US intelligence agencies can be seen in the amount the NSA and CIA are investing in it. Not only does this include multimillion-dollar contracts with providers specializing in data mining services, but the CIA also invests directly, through its subsidiary company In-Q-Tel, in several big data start-ups.¶ It's about rendering people and their behavior predictable. The NSA's research projects aim to forecast, on the basis of telephone data and Twitter and Facebook posts, when uprisings, social protests and other events will occur. The agency is also researching new methods of analysis for surveillance videos with the hopes of recognizing conspicuous behavior before an attack is committed.¶ Gus Hunt, the CIA's chief technology officer, made a forthright admission in March: "We fundamentally try to collect everything and hang onto it forever." What he meant by "everything," Hunt also made clear: "It is really very nearly within our grasp to be able to compute on all human-generated information," he said.¶ That statement is difficult to reconcile with the Fourth Amendment to the US Constitution, which guarantees the right to privacy. This is probably why Hunt added, almost apologetically: "Technology in this world is moving faster than government or law can keep up."

Squo solves overload – new tools

Kirby, 13

Bob Kirby, vice president of sales for CDW·G, a leading technology provider to government and education. “Big Data Can Help the Federal Government Move Mountains. Here's How.” FedTech Magazine, 08/01/13, <http://www.fedtechmagazine.com/article/2013/08/big-data-can-help-federal-government-move-mountains-heres-how> // IS

The White House took a step toward helping agencies find these technologies when it established the National Big Data Research and Development Initiative in 2012. The initiative included more than \$200 million to make the most of the explosion of Big Data and the tools needed to analyze it.

The challenges that Big Data poses are nearly as daunting as its promise is encouraging. Storing data efficiently is one of these challenges. As always, budgets are tight, so agencies must minimize the per-megabyte price of storage and keep the data within easy access so that users can get it when they want it and how they need it. Backing up massive quantities of data heightens the challenge.

Analyzing the data effectively is another major challenge. Many agencies employ commercial tools that enable them to sift through the mountains of data, spotting trends that can help them operate more efficiently. (A recent study by MeriTALK found that federal IT executives think Big Data could help agencies save more than \$500 billion while also fulfilling mission objectives.)

Custom-developed Big Data tools also are allowing agencies to address the need to analyze their data. For example, the Oak Ridge National Laboratory's Computational Data Analytics Group has made its Piranha data analytics system available to other agencies. The system has helped medical researchers find a link that can alert doctors to aortic aneurysms before they strike. It's also used for more mundane tasks, such as sifting through résumés to connect job candidates with hiring managers.

AT Chinese Cyberwar

No US-China cyber escalation – litany of checks

Lindsay, 15

Jon Lindsay, Assistant Professor of Digital Media and Global Affairs at the University of Toronto, research scientist with the University of California Institute on Global Conflict and Cooperation, assistant adjunct professor at the UC San Diego School of International Relations and Pacific Studies, and an Oxford Martin Associate with the Oxford Global Cyber Security Capacity Centre, “Exaggerating the Chinese Cyber Threat,” Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2015,
http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html // IS

Policymakers in the United States often portray China as posing a serious cybersecurity threat. In 2013 U.S. National Security Adviser Tom Donilon stated that Chinese cyber intrusions not only endanger national security but also threaten U.S. firms with the loss of competitive advantage. One U.S. member of Congress has asserted that China has "laced the U.S. infrastructure with logic bombs." Chinese critics, meanwhile, denounce Western allegations of Chinese espionage and decry National Security Agency (NSA) activities revealed by Edward Snowden. The People's Daily newspaper has described the United States as "a thief crying 'stop thief.'" Chinese commentators increasingly call for the exclusion of U.S. internet firms from the Chinese market, citing concerns about collusion with the NSA, and argue that the institutions of internet governance give the United States an unfair advantage.

The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution. Fears about the paralysis of the United States' digital infrastructure or the hemorrhage of its competitive advantage are exaggerated. Chinese cyber operators face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property. More important, both the United States and China have strong incentives to moderate the intensity of their cyber exploitation to preserve profitable interconnections and avoid costly punishment. The policy backlash against U.S. firms and liberal internet governance by China and others is ultimately more worrisome for U.S. competitiveness than espionage; ironically, it is also counterproductive for Chinese growth.

No US-China cyber escalation – no incentives and interdependence

Lindsay, 15

Jon Lindsay, Assistant Professor of Digital Media and Global Affairs at the University of Toronto, research scientist with the University of California Institute on Global Conflict and Cooperation, assistant adjunct professor at the UC San Diego School of International Relations and Pacific Studies, and an Oxford Martin Associate with the Oxford Global Cyber Security Capacity Centre, “Exaggerating the Chinese Cyber Threat,” Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2015,
http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html // IS

Many Western observers fear that cyber reform based on the principle of internet sovereignty might legitimize authoritarian control and undermine the cosmopolitan promise of the multistakeholder system. China, however, benefits too much from the current system to pose a credible alternative. Tussles around internet governance are more likely to result in minor change at the margins of the existing system, not a major reorganization that shifts technical protocols and operational regulation to the United Nations. Yet this is not a foregone conclusion, as China moves to exclude U.S. firms such as IBM, Oracle, EMC, and Microsoft from its domestic markets and attempts to persuade other states to support governance reforms at odds with U.S. values and interests.

CONCLUSION

Information technology has generated tremendous wealth and innovation for millions, underwriting the United States' preponderance as well as China's meteoric rise. The costs of cyber espionage and harassment pale beside the mutual benefits of an interdependent, globalized economy. The inevitable frictions of cyberspace are not a harbinger of catastrophe to come, but rather a sign that the states inflicting them lack incentives to cause any real harm. Exaggerated fears of cyberwarfare or an erosion of the United States' competitive advantage must not be allowed to undermine the institutions and architectures that make the digital commons so productive.

AT Border Overload

No overload – there are still gaps AP, 14

Associated Press, "Drones patrol half of Mexico border," The Daily Mail, 11/13/14,
<http://www.dailymail.co.uk/wires/ap/article-2832607/Drones-patrol-half-Mexico-border.html> //
IS

The government has operated about 10,000 drone flights under the strategy, known internally as "change detection," since it began in March 2013. The flights currently cover about 900 miles, much of it in Texas, and are expected to expand to the Canadian border by the end of 2015.

The purpose is to assign agents where illegal activity is highest, said R. Gil Kerlikowske, commissioner of Customs and Border Protection, the Border Patrol's parent agency, which operates nine unmanned aircraft across the country.

"You have finite resources," he said in an interview. "If you can look at some very rugged terrain (and) you can see there's not traffic, whether it's tire tracks or clothing being abandoned or anything else, you want to deploy your resources to where you have a greater risk, a greater threat."

If the video shows the terrain unchanged, Border Patrol Chief Michael Fisher calls it "proving the negative" — showing there isn't anything illegal happening there and therefore no need for agents and fences.

The strategy was launched without fanfare and expanded at a time when President Barack Obama prepares to issue an executive order by the end of this year to reduce deportations and enhance border security.

Rep. Michael McCaul, a Texas Republican who chairs the House Homeland Security Committee, applauded the approach while saying that surveillance gaps still remain. "We can no longer focus only on static defenses such as fences and fixed (camera) towers," he said.

AT NSA good – cyberterror

Alt causes – the aff isn't enough Goldsmith, 13

Jack Goldsmith, Henry L. Shattuck Professor at Harvard Law School, “We Need an Invasive NSA,” New Republic, 10/10/13, <http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks // IS>

To keep these computers and networks secure, the government needs powerful intelligence capabilities abroad so that it can learn about planned cyber-intrusions. It also needs to raise defenses at home. An important first step is to correct the market failures that plague cybersecurity. Through law or regulation, the government must improve incentives for individuals to use security software, for private firms to harden their defenses and share information with one another, and for Internet service providers to crack down on the botnets—networks of compromised zombie computers—that underlie many cyber-attacks. More, too, must be done to prevent insider threats like Edward Snowden's, and to control the stealth introduction of vulnerabilities during the manufacture of computer components—vulnerabilities that can later be used as windows for cyber-attacks. And yet that's still not enough. The U.S. government can fully monitor air, space, and sea for potential attacks from abroad. But it has limited access to the channels of cyber-attack and cyber-theft, because they are owned by private telecommunication firms, and because Congress strictly limits government access to private communications. “I can't defend the country until I'm into all the networks,” General Alexander reportedly told senior government officials a few months ago. For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation. It will also allow it to discern patterns of malicious activity in the swarm of communications, even when it doesn't possess the malware's signature. And it will better enable the government to trace back an attack's trajectory so that it can discover the identity and geographical origin of the threat.

AT legal solutions solve

Politics and legal solutions can't change the surveillance state

North, PhD, '13 (Gary North, PhD UC Riverside “Surveillance state will collapse; data overload increasingly blinds it” July 29, 2013 <http://nooganomics.com/2013/07/surveillance-state-will-collapse-data-overload-increasingly-blinds-it/>) //GY

On the next day, July 24, the House of Representatives voted down an amendment to cut the NSA's budget — the official one, not the real one, which is secret. It was Nancy Pelosi who made the difference. She carried the NSA's water. The failure of Congress to make a token cut in the National Security Agency's official budget on July 24 was a green light for the NSA to spy on all Americans, forever. ¶ Congress knows that the voters do not care enough to mobilize against the Patriot Act, which is the heart of the surveillance state. They also know that most House members are immune from the voters. Gerrymandering works. They also know that they, personally, are not immune from the NSA's monitoring of their telephone calls, emails, and other communications. They can count the votes. They know who is on top. The surveillance state is on top. ¶ **The surveillance state is now unstoppable politically.** Legally, there is no possibility that it will be rolled back. It is now the non-law of the land. Wyden thinks the voters may roll it back. They won't. It is unstoppable politically.

AT Panopticism

The Foucaldian Panopticon is inherent to a myriad of government agencies. Restricting NSA based surveillance is too narrowly based to succeed.

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

The Panopticon is real. It siphons billions of dollars each year from a federal budget in crisis. And it **is watching you** and your children. **Lost in the debate about NSA spying**, however — **and** even most public **resistance to it** — **have been** the various **other federal agencies** also **complicit in Fourth Amendment abuses**. Even **critics of domestic surveillance have** largely **failed to recognize how many government agencies spy on Americans**. A presidential review panel recently recommended substantial changes to FBI powers, including ending the authority to issue National Security Letters. NSLs are secret data requests used to circumvent both First and Fourth Amendment protections, demanding information about third parties and gagging the recipients. **The FBI’s pattern of abusing undercover infiltration** to disrupt First Amendment protected organizations, however, stretches back decades, threatens democracy even more deeply than NSLs, and **continues unabated**. **Beyond the NSA and FBI, many other agencies are** also involved in **domestic surveillance**. **And** all of them **continue to evade** public and congressional **scrutiny**.

Federal agencies other than NSA are complicit in maintaining the Panopticon.

A. Department of Homeland Security:

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

The Department of Homeland Security (**DHS**) is a sprawling behemoth, with nearly a quarter million employees scattered across nearly two dozen component agencies. **While purporting to protect the “homeland”** (a term with loaded connotations worth noting, but setting aside for now) from various threats, **DHS spies on Americans** in several disturbing ways. Some of **the most dystopian** piggyback on **programs** presented to the public as supporting immigration enforcement. Border security agencies, like Customs & Border Protection (CBP) and Immigration & Customs Enforcement (ICE), have **facilitated a record number of deportations** under the Obama administration, creating a domestic humanitarian crisis. Critics of the administration’s immigration crackdown have vocally challenged its failures. According to the New York Times, “**the department’s** continually shifting **strategies** against illegal immigration had two things in common. They **were** **ineffective and cruel.**”

B. Postal Service:

Buttar, '13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,”

Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

Nor are law enforcement agencies the only ones joining the intelligence agencies to spy on Americans. Even the US Postal Service is getting in on the surveillance racket. In July, the New York Times reported on the Mail Isolation Control and Tracking program, “in which Postal Service computers photograph the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces last year....” It concluded that “postal mail is subject to the same kind of scrutiny that the National Security Agency has given to telephone calls and e-mail.” Like the NSA’s ubiquitous electronic wiretapping, postal surveillance carries disturbing implications, particularly in terms of enabling the suppression of political dissent. Most astounding in the context of the controversy over NSA spying, however, is the sheer ignorance about the postal service’s monitoring practices.

C. State and local law enforcement:

Buttar, ’13 [Shahid, former executive director of the Bill of Rights Defense Committee, is a constitutional lawyer and grassroots organizer. Shahid directed a national program to combat racial and religious profiling, after serving for three years as associate director of the American Constitution Society for Law & Policy, “Beyond the Panopticon: The NSA Isn’t Alone,” Defending Dissent Foundation, 12-26-13, <http://www.bordc.org/blog/beyond-panopticon-nsa-isn%E2%80%99t-alone>]

DHS also erodes constitutional rights through its collaborations with local police. State and local law enforcement agencies around the country collaborate with a series of over 70 regional DHS-funded fusion centers pursuing ambiguous missions at unknown costs. DHS leaders have praised fusion centers, but critics — extending from the libertarian CATO Institute and immigrant rights groups to FBI veterans — have described them as wasteful, duplicative, constitutionally offensive, and ineffective from a public safety standpoint. Targeted surveillance, of the sort abused by the FBI, is also a problem across state & local departments. For years, peace activists, Ron Paul supporters, environmentalists, and Muslims have been targeted for government spying in dozens of states--not only by the FBI, but also by state and local police. Until being shut down by the Governor in 2010, Pennsylvania state officials not only spied on environmental activists, but also shared its intelligence reports with their corporate targets, including mining companies. DHS also facilitates the paramilitarization of local and state police agencies, which around the country have sought DHS grants to buy everything from sophisticated listening devices to surveillance cameras, automated drivers license plate scanners developed originally for military uses, aerial surveillance drones, and even armored tanks.

AT Authoritarianism

The claims about authoritarianism are hyperbolic and paranoid. All law enforcement practice might be used improperly, but accountability checks the worst practices.

Simon, 2014,

William H. Simon, Arthur Levitt Professor of Law at Columbia University, 10-20-2014, "Rethinking Privacy," Boston Review, <http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance>

The third trope of the paranoid style is the slippery slope argument. The idea is that an innocuous step in a feared direction will inexorably lead to further steps that end in catastrophe. As The Music Man (1962) puts it in explaining why a pool table will lead to moral collapse in River City, Iowa, "medicinal wine from a teaspoon, then beer from a bottle." In this spirit, Daniel Solove in Nothing to Hide (2011) explains why broad surveillance is a threat even when limited to detection of unlawful activity. First, surveillance will sometimes lead to mistaken conclusions that will harm innocent people. Second, since "everyone violates the law sometimes" (think of moderate speeding on the highway), surveillance will lead to over-enforcement of low-stakes laws (presumably by lowering the costs of enforcement), or perhaps the use of threats of enforcement of minor misconduct to force people to give up rights (as for example, where police threaten to bring unrelated charges in order to induce a witness or co-conspirator to cooperate in the prosecution of another). And finally, even if we authorize broad surveillance for legitimate purposes, officials will use the authorization as an excuse to extend their activities in illegitimate ways. Yet, slippery slope arguments can be made against virtually any kind of law enforcement. Most law enforcement infringes privacy. ("Murder is the most private act a man can commit," William Faulkner wrote.) And most law enforcement powers have the potential for abuse. What we can reasonably ask is, first, that the practices are calibrated effectively to identify wrongdoers; second, that the burden they put on law-abiding people is fairly distributed; and third, that officials are accountable for the lawfulness of their conduct both in designing and in implementing the practices.

Surveillance doesn't harm freedom or autonomy, because they aren't reliant on digital communication.

Sagar, 2015

Rahul, associate professor of political science at Yale-NUS College and the Lee Kuan Yew School of Public Policy at the National University of Singapore. He was previously assistant professor in the Department of Politics at Princeton University., "Against Moral Absolutism: Surveillance and Disclosure After Snowden," Ethics & International Affairs / Volume 29 / Issue 02 / 2015, pp 145-159.

The second harm Greenwald sees surveillance posing is personal in nature. Surveillance is said to undermine the very essence of human freedom because the "range of choices people consider when they believe that others are watching is . . . far more limited than what they might do when acting in a private realm."¹⁶ Internet-based surveillance is viewed as especially damaging in this respect because this is "where virtually everything is done" in our day, making it the place "where we develop and express our very personality and sense of self." Hence, "to permit surveillance to take root on the Internet would mean subjecting virtually all forms of human interaction, planning, and even thought itself to comprehensive state examination."¹⁷ This claim too seems overstated in two respects. First, it exaggerates the extent to which our self-development hinges upon electronic communication channels and other related activities that leave electronic traces. The arrival of the Internet certainly opens new vistas, but it does not entirely close earlier ones. A person who fears what her browsing habits might communicate to the authorities can

obtain texts offline. Similarly, an individual who fears transmitting materials electronically can do so in person, as Snowden did when communicating with Greenwald. There are costs to communicating in such “old-fashioned” ways, but these costs are neither new nor prohibitive. Second, a substantial part of our self-development takes place in public. We become who we are through personal, social, and intellectual engagements, but these engagements do not always have to be premised on anonymity. Not everyone wants to hide all the time, which is why public engagement—through social media or blogs, for instance—is such a central aspect of the contemporary Internet.

AT Tyranny

The argument that NSA surveillance enables tyranny is wrong. The data exists inevitably and if you are concerned about the risk of a tyrant taking over, there are much bigger issues than privacy to be concerned about.

Etzioni, Professor of International Relations at the George Washington University, 2014

Amitai Etzioni , Intelligence and National Security (2014): NSA: National Security vs. Individual Rights, Intelligence and National Security, DOI: 10.1080/02684527.2013.867221

Part VI: The Coming Tyrant? A common claim among civil libertarians is that, even if little harm is presently being inflicted by government surveillance programs, the infrastructure is in place for a less-benevolent leader to violate the people's rights and set us on the path to tyranny. For example, it has been argued that PRISM 'will amount to a "turnkey" system that, in the wrong hands, could transform the country into a totalitarian state virtually overnight. Every person who values personal freedom, human rights and the rule of law must recoil against such a possibility, regardless of their political preference'.¹⁷⁷ And Senator Rand Paul (R-KY) has been 'careful to point out that he is concerned about the possible abuses of some future, Hitler-like president'.¹⁷⁸ A few things might be said in response. First, all of the data that the government is collecting is already being archived (at least for short periods – as discussed above) by private corporations and other entities. It is not the case that PRISM or other such programs entail the collection of new data that was not previously available. Second, if one is truly concerned that a tyrant might take over the United States, one obviously faces a much greater and all-encompassing threat than a diminution of privacy. And the response has to be similarly expansive. One can join civic bodies that seek to shore up democracies, or work with various reform movements and public education drives, or ally with groups that prepare to retreat to the mountains, store ammunition and essential foods, and plan to fight the tyrannical forces. But it makes no sense to oppose limited measures to enhance security on these grounds.

AT State Abuses are morally objectionable

No Ethical abuse – ethical benefits to surveillance outweigh AND inherent safeguards check

Taylor 05

[In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance James Stacey Taylor Public Affairs Quarterly Vol. 19, No. 3 (Jul., 2005), pp. 227-246 Published by: University of Illinois Press on behalf of North American Philosophical Publications Stable URL: <http://www.jstor.org/stable/40441413> //duff

It must be admitted that, in practice, a system of constant State surveillance is likely to be abused to some extent.²⁰ However, if one adopts a rights-based understanding of claim (ii) above (i.e., if one holds that such a system of State surveillance is permissible as long as it does not in itself violate persons' moral rights), this objection can be readily rebutted. On such an understanding of claim (ii) one could first note that this abuse-based objection gets its force from the view that such abuse would violate persons' moral rights. The proponent of a rights-based understanding of claim (ii) would certainly agree with this underlying view, and would join with its advocates in condemning such abuse. However, the rights theorist who was in favor of such a system of State surveillance would also note that the condemnation of the abuse of State surveillance is not to condemn State surveillance itself. To condemn the use of x for the purposes of v, where y violates persons' rights (e.g., to privacy or autonomy) is not also to condemn the use of x for the purposes of z, where z does not violate persons' rights. Thus, a rights theorist who was a proponent of State surveillance could argue, to offer the possibility of abuse as an objection to constant State surveillance is to confuse the moral status of different possible uses of such surveillance. For such proponents of State surveillance, then, this first objection can be readily dismissed. If one adopts a consequentialist understanding of claim (ii), however, defending the use of constant State surveillance against this objection is more difficult. This is because the likelihood of such abuse together with the likelihood of such abuse causing harm must be weighed against the benefits (as outlined above) that such a system is likely to provide. And, given that such a system has not yet been implemented, such a weighing and balancing of its relative costs and benefits will be difficult to assess with certainty. Despite this, however, there is good reason to believe that little harm will accrue from the abuse of such a system of surveillance. Thus, given the likelihood that such a system of State surveillance will bring important benefits to the citizens of the State in which it is installed, the possibility of its abuse should not deter consequentialists from endorsing the above pro-surveillance argument. To show why there is good reason to believe that little harm would accrue from such a system of State surveillance its consequentialist proponents should first distinguish between major abuses of such a system and minor abuses of it. A major abuse of such a system would be one in which the State used its power together with its improved surveillance capabilities to persecute or oppress its citizens, either individually or as a whole. A minor abuse of the system would be one in which some of the agents of the State secured access to the information gathered by its surveillance devices for their own nefarious purposes, such as voyeurism or the mockery of the persons whose recorded actions they are viewing. The consequentialist proponent of constant and universal State surveillance need not be unduly concerned about the possibility of major abuses of the State surveillance system. If the State were prone to abuse its citizens in this way prior to the installation of such a system, this would provide good consequentialist grounds for resisting its introduction. The consequentialist proponent of constant State surveillance is thus only concerned with defending the introduction of such a surveillance system in those cases where the State was not prone to abusing its citizens in this way. This is not to say, however, that a State (or the agents of a State) that was not prone to persecuting or oppressing its citizens might not occasionally persecute individual citizens. In response to this the consequentialist proponent of constant State surveillance should note that given its power were the State (or its agents) to decide to persecute some of its citizens in this way it would not need a system of surveillance to do this effectively. Thus, although such a surveillance system might make it easier for the State (or its agents) to engage in the persecution that it had decided upon, this would not make things any worse for the person or persons thus persecuted. As such, then, the possibility of the major abuse of a system of constant and universal State surveillance by a State that was not prone to persecuting its citizens would not, for a consequentialist, be a significant objection to the introduction of such a system. What, then, of the concern that such a system of constant State surveillance would be subject to minor abuses? The most obvious response to this concern is to argue that if such a system of surveillance is introduced then it must be accompanied by a series of safeguards that would reduce the possibility that the information that

it gathers would be abused in this way. It might, for example, be that such a system should be accompanied by the requirement that only a very few persons have access to the information that it gathers, that such persons be screened carefully and supervised closely, and that they are subject to draconian penalties for any abuses that they might perpetrate. If they were severe enough such safeguards would be likely to reduce the possibility of the minor abuse of such a system of surveillance to a level whereby the harm that its abusers might cause would be outweighed by the advantages that it would provide to the State's citizens as a whole. However, the consequentialist proponent of State surveillance also has a second - and more philosophically interesting - response to the concern that such surveillance would be subject to minor abuse: that such abuse would not be harmful, and so would not detract from the advantages outlined above. This response is based on observing that given the penalties for abuse by which such a system would be accompanied (as outlined above) any such abuse would be perpetrated covertly. As such, its victims (e.g., persons subjected to the voyeuristic gaze of some of the agents of the State) would not know that they were victims. Yet even though this is so, the proponents of this second response to the above abuse-based objection do not use this observation to argue that, since such persons did not know that they were being watched, this watching did not harm them.²¹ This is because, as Joel Feinberg has persuasively argued, the mere fact that a person is ignorant of the frustration of her interests (e.g., her interest not to be the unwilling subject of voyeurism) does not mean that she has not thereby been harmed.²² Rather, this second consequentialist response to the above abuse-based objection conjoins this observation with the claim that for a person to be harmed her life must have been adversely affected in some way, whether she knew of this or not. To support this latter claim it will be useful to examine more closely Feinberg's argument against the view that a person can be harmed only if she knows that she has been harmed. This examination will serve two purposes. First, it will show why the consequentialist proponent of constant State surveillance should not claim that the unwitting victim of (e.g.) State voyeurism failed to be harmed by it owing to her ignorance of it. Second, it will support the claim that a person's life must be adversely affected for her to be considered harmed - the claim on which this second response rests.

AT Abuse of Surveillance

The NSA is well-regulated and constrained by judicial oversight.

Cohen, 2015

Michael A. Cohen, 15, fellow at The Century Foundation. Previously, Michael served in the U.S. Department of State as chief speechwriter for U.S. Representative to the United Nations Bill Richardson and Undersecretary of State Stuart Eizenstat. , 6-3-2015, "NSA Surveillance Debate Drowned Out on Both Sides by Fear Tactics," World Politics Review, <http://www.worldpoliticsreview.com/articles/15905/nsa-surveillance-debate-drowned-out-on-both-sides-by-fear-tacticsa>

The arguments of NSA opponents have, for two years, relied on hypothetical, trumped-up fears of the government ransacking our private information. These concerns have been raised even though, from all appearances, the NSA's domestic surveillance activities are reasonably well-regulated and constrained by judicial oversight. NSA opponents like to point out that a recent court decision determined that the bulk records collection program was illegal, which ignores the many other court decisions that accepted its legality. More important, it ignores the decisions of the secret FISA Court, which ordered the NSA not to scrap collection programs that were determined to be operating unconstitutionally, but rather to make changes to them to get them in line with constitutional constraints.

There's no evidence of abuse of surveillance powers.

Simon, 2013,

David Simon, producer of HBO's The Wire, 7/3/13, "We are shocked, shocked..."
<http://davidsimon.com/we-are-shocked-shocked/>

I know it's big and scary that the government wants a data base of all phone calls. And it's scary that they're paying attention to the internet. And it's scary that your cell phones have GPS installed. And it's scary, too, that the little box that lets you go through the short toll lane on I-95 lets someone, somewhere know that you are on the move. Privacy is in decline around the world, largely because technology and big data have matured to the point where it is easy to create a net that monitors many daily interactions. Sometimes the data is valuable for commerce — witness those facebook ads for Italian shoes that my wife must endure — and sometimes for law enforcement and national security. But be honest, most of us are grudging participants in this dynamic. We want the cell phones. We like the internet. We don't want to sit in the slow lane at the Harbor Tunnel toll plaza. The question is not should the resulting data exist. It does. And it forever will, to a greater and greater extent. And therefore, the present-day question can't seriously be this: Should law enforcement in the legitimate pursuit of criminal activity pretend that such data does not exist. The question is more fundamental: Is government accessing the data for the legitimate public safety needs of the society, or are they accessing it in ways that abuse individual liberties and violate personal privacy — and in a manner that is unsupervised. And to that, the Guardian and those who are wailing jeremiads about this pretend-discovery of U.S. big data collection are noticeably silent. We don't know of any actual abuse. No known illegal wiretaps, no indications of FISA-court approved intercepts of innocent Americans that occurred because weak probable cause was acceptable. Mark you, that stuff may be happening. As happens the case with all law enforcement capability, it will certainly happen at some point, if it hasn't already. Any data asset that can be properly and legally invoked, can also be misused — particularly without careful oversight. But that of course has always been the case with electronic surveillance of any kind.

AT Right to Privacy

Anti-terror measures won't lead to authoritarianism and security is a precondition for freedom

Paul Rosenzweig, Heritage Senior Legal Research Fellow, 2004

["Preventive Detention and Actionable Intelligence," 9/16, w/ James Jay Carafano, <http://www.heritage.org/Research/HomelandDefense/lm13.cfm>]

The response to this criticism is threefold: First, the criticism blinks reality. We already have incomplete and irregular forms of preventive detention because it is a necessity. We advance liberty when we regularize the practice, cabin it to narrow circumstances, and use it sparingly. Second, as detailed above, other countries (such as the United Kingdom) have managed to adopt very limited forms of preventive detention without becoming noticeably “unfree” or “authoritarian.” Adoption of similar legal forms in the United States will not render us an authoritarian regime either. Finally, and most important, to reject preventive detention in those rare circumstances in which it is necessary is to exalt liberty at the expense of security. The founding of the American Republic was for the purpose of constructing a political system of ordered liberty. It simply cannot be right to unilaterally prefer liberty. Liberty is not an absolute value; it depends upon security (both personal and national) for its exercise. As Thomas Powers has written: “In a liberal republic, liberty presupposes security; the point of security is liberty.” The growth in danger from the consequences of the failure to stop terrorism necessitates altering our tolerance for governmental order. More fundamentally, our goal should be to maximize both order and liberty.

The foundation of rights is the promotion of the public good

John Hasnas, professor of Business Ethics, Georgetown, NORTHWESTERN UNIVERSITY LAW REVIEW, 1995, p. 916

Rights are conferred (and their correlating duties imposed) with the direct or immediate purpose of promoting the general good; (as, for example, tie rights of judges and other political subordinates): and rights are conferred indirectly to the same extensive purpose, although their proximate end be the advantage of the parties entitled, or of other determinate parties for whom they are conferred in trust.

Constitutional Rights are not trump cards; policy goals can outweigh the interests of rights & no rights are absolute under the Constitution

Harvey, J.D., Yale Law School, '02 (Philip Harvey, "Human Rights and Economic Policy Discourse: Taking Economic And Social Rights Seriously", Spring, 2002, 33 Colum. Human Rights L. Rev. pp. 370-1)

A view frequently expressed by human rights advocates is that valid rights should "trump" other policy goals, but I argue that this prescription, if taken at face value, is inadequate. A genuine trump outweighs even the highest valued card in another suit, but rights-based claims are rarely treated that way. They are given added weight, but not a genuinely trumping value. For example, in American constitutional jurisprudence, even fundamental rights may be infringed; however, a "compelling state interest" is required to justify such actions. What I argue is needed, therefore, is not a social choice methodology that treats rights as absolute trumps, but one that treats them with appropriate deference. The level of deference owed a particular right may vary with the importance of the ultimate interests it protects and with the nature of the countervailing interests that oppose it. Whether the balance between human rights protection and other policy goals is struck appropriately in particular instances may not be easy to determine. It certainly will not be demonstrable with the mathematical precision to which welfare economics aspires. The most we can expect is persuasive argument.

Turn -- Absolutism hurts rights – we get lost in moral constraints rather than being moved by real concern

Waldron, Jeremy, 1993 (Liberal Rights, Collected Papers: Cambridge Univ. Press)

I have some sympathy with this, but, as I also argue in Chapter 9, the insistence on absolutism does not make the conflicts go away; it doesn't make the situations that appear to call for trade-offs disappear. Those situations are not something that consequentialists and their fellow travelers have perversely *invented* in order to embarrass moral absolutists. It is not the theorist's fault that there are sometimes several drowning people and only one lifeguard. As I said earlier, the world turns out not to be the sort of place to which absolute moral requirements are an apt response. If we insist on the absoluteness of rights, there is a danger that we may end up with no rights at all, or, at least, no rights embodying the idea of real concern for the individuals whose rights they are. At best, we will end up with a set of moral constraints whose absoluteness is secured only by the contortions of agent-relativity, that is, by their being understood not as concerns focused on those who may be affected by our actions but as concerns focused on ourselves and integrity.

Turn -- One must divert to utilitarianism when the alternative is to let everyone die

Kateb, Professor of Politics, 1992 (George, Prof of Politics, Princeton Univ., The Inner Ocean: Individualism and Democratic Culture; Cornell University Press, p. 12)

The main point, however, is that utilitarianism has a necessary place in any democratic country's normal political deliberations. But its advocates must know its place, which ordinarily is only to

help to decide what the theory of rights leaves alone. *When may rights be overridden by government?* I have two sorts of cases in mind: overriding a particular right of some persons for the sake of preserving the same right of others, and overriding the same right of everyone for the sake of what I will clumsily call "civilization values." An advocate of rights could countenance, perhaps must countenance, the state's overriding of rights for these two reasons. The subject is painful and liable to dispute every step of the way. For the state to override is, sacrifice—a right of some so that others may keep it. the situation must be desperate. I have in mind, say, circumstances in which the choice is between sacrificing a right of some and letting a right of all be lost. The state (or some other agent) may kill some (or allow them to be killed), if the only alternative is letting every-one die. It is the right to life which most prominently figures in thinking about desperate situations. I cannot see any resolution but to heed the precept that "numbers count." Just as one may prefer saving one's own life to saving that of another when both cannot be saved, so a third party—let us say, the state—can (perhaps must) choose to save the greater number of lives and at the cost of the lesser number, when there is otherwise no hope for either group. That choice does not mean that those to be sacrificed are immoral if they resist being sacrificed. It follows, of course, that if a third party is right to risk or sacrifice the lives of the lesser for the lives of the greater number when the lesser would otherwise live, the lesser are also not wrong if they resist being sacrificed.

You are responsible for outcomes that are caused by others when you cause the others to do the outcome

Uniacke (University of Wollongong, NSW, Australia) '99

(Suzanne, Jun99, International Journal of Philosophical Studies, "Absolutely Clean Hands? Responsibility for What's Allowed in Refraining from What's Not Allowed," Vol. 7 Issue 2, p189, 21p)

We bear responsibility for the outcome of another's actions, for instance, when we provoke these actions (Iago); or when we supply the means (Kevorkian), identification (Judas), or incentive (Eve); or where we encourage another to act as he [or she] does (Lady Macbeth). Despite his disclaimer, Pilate cannot acquit himself entirely of the outcome of what others decide simply by ceding the judgment to them. In these examples agents are indirectly, partly responsible for the outcomes of what others do in virtue of something they themselves have done. But indirect, partial responsibility for what another person does can also arise through an agent's non-intervention and be grounded in intention or fault; for example, when Arthur does not prevent Brian killing Catherine, because Arthur wants Catherine dead, or because Arthur simply cannot be bothered to warn her or call the police. Of course attributions of indirect, partial responsibility can be difficult. And as far as absolutism is concerned, the relevant sense of 'brings about', outlined earlier, will sometimes be quite stretched where an agent is attributed with responsibility for what someone else does. All the same, by our non-intervention we can help bring about some things that are directly and voluntarily caused by others.

Turn -- Consequentialism affirms the unconditional value of rational beings as equals – its is the best framework; Kantian ethics faces the same dilemma of kill to save

Cummiskey, Associate Professor of Philosophy, Bates College, '96 (David, Kantian Consequentialism, New York: Oxford University Press, p. 150-1)

On the other hand, in practice, consequentialists do not defend the sacrifice of the innocent as a principle of public policy. In practice, of course, a Kantian consequentialist can and should appeal to good consequentialist reasons for limiting the use of coercion and maintaining a sphere of personal liberty. There are good consequentialist reasons for secondary principles that constrain a direct appeal to the more basic consequentialist principle. Just as honesty is typically the best policy, protecting individual rights really does advance the common good. In addition, the demands of duty are such that, as Kant would say, finite rational beings cannot be expected to fully satisfy them. We must distinguish what one should do if one can from what we should expect or demand of ourselves and others. Although consequentialists reject moral complacency and self-satisfaction, they also provide a justification for a distinction between extraordinary and ordinary compliance with duty. Thus, the Kantian consequentialist should follow the tradition, going back at least to Aquinas," that recognizes that "human law" should externally legislate only the more harmful vices and should set its demands at a level a normally virtuous person can satisfy. Full virtue is indeed best left to the internal legislation of finite rational beings. Consequentialism thus provides an indirect justification for our intuitive conviction that we should not demand that the innocent sacrifice themselves, and also that we should not sacrifice the innocent. Kant's moral theory, however, simply does not provide a more direct and indefeasible justification for deontological constraints. In principle, a conscientious Kantian moral agent may be required to kill one in order to save two. Nonetheless, if someone is unable to do so, this may well not be grounds for reproach. Similarly, if I cannot amputate a leg to save a life-either my own or that of another-I may not be blameworthy for my failure, although it is true that I should have done the nasty deed. Still, in such a situation I must try to force my attention on the good I am doing and thereby enable myself to act. Similarly, in the highly unusual case where it would truly be best to kill some to save others, a good person should also try to focus on the lives to be saved rather than becoming fixated exclusively on those who will be killed. Nonetheless, even though sacrificing some to save others is sometimes the right thing to do, one should still feel regret and mourn the people who are lost. After all, the goal is to save each and every person; thus, one should indeed feel the loss of even one. According to Kant, the objective end of moral action is the existence of rational beings. Respect for rational beings requires that in deciding what to do, one must give appropriate practical consideration to the unconditional value of rational beings and to the conditional value of happiness. Since agent-centered constraints require a non-value-based rationale, the most natural interpretation of the demand that one give equal respect to all rational beings leads to a consequentialist normative theory. We have seen that there is no sound Kantian reason for abandoning this natural consequentialist interpretation. In particular, a consequentialist interpretation does not require sacrifices that a Kantian ought to consider unreasonable, and it does not involve doing evil so that good may come of it. It simply requires an uncompromising commitment to the equal value and equal claims of all rational beings and a recognition that in the moral consideration of conduct, one's own subjective concerns do not have overriding importance.

Security is a fundamental economic and social right

HARVARD CIVIL RIGHTS CIVIL LIBERTIES LAW REVIEW, Summer 1995, p. 589-90

The *Pratt* decision and continuing litigation typifies the way in which strict adherence to classical liberalism's understanding of freedom creates an incomplete balance between fundamental rights and the basic needs imperative to realize those rights. The court's formalistic adherence to a classical liberal view of civil and political rights obscured the public housing residents' underlying social and economic rights. By privileging the civil and political rights of residents, *Pratt* ignores their basic need for security. The legal parameters in which the *Pratt* case was decided forced public housing residents to pay for one of their most fundamental constitutional rights, the right to be free from governmental intrusion, with their basic need for security.

The risk of extinction via nuclear war outweighs all - ethics demands you evaluate consequences

Robert A. Seeley, Central Committee for Conscientious Objectors, **1986**, The Handbook of Non-Violence, p. 269-70

In moral reasoning prediction of consequences is nearly always impossible. One balances the risks of an action against its benefits; one also considers what known damage the action would do. Thus a surgeon in deciding whether to perform an operation weighs the known effects (the loss of some nerve function, for example) and risks (death) against the benefits, and weighs also the risks and benefits of not performing surgery. Morally, however, human extinction is unlike any other risk. No conceivable human good could be worth the extinction of the race, for in order to be a human good it must be experienced by human beings. Thus extinction is one result we dare not-may not-risk. Though not conclusively established, the risk of extinction is real enough to make nuclear war utterly impermissible under any sane moral code.

AT “Petro – Freedom is Absolute”

freedoms can't be absolute because freedoms contradict

Roberto Unger, CRITICAL LEGAL STUDIES, Ed. Hutchinson, 1984, p. 26

The theory of formal freedom suffers from the same dilemma as the morality of reason, of which it is the political equivalent. Take Kant's universal principle of right, “Every action is right that in itself or in its maxim is such that the freedom of the will of each can coexist together with the freedom of the will of everyone according to a universal law.” When this proposition is left in its abstract form, it seems impossible to derive from it definitive conclusions about what precisely the laws should command, prohibit, or permit...But, as soon as we try to reach the level of concrete regulation of conduct, we are forced to prefer some values to others. This, however, is just what the formal theory of freedom was meant to avoid. Like the morality of reason, the formal doctrine of freedom has to choose between being unworkable and being incoherent.

Freedom can't be absolute because it is grounded in the social

Roberto Unger, THE CRITICAL LEGAL STUDIES MOVEMENT, 1986, p. 104

The other available answer to the question- what lies on the other side of arbitrary constraint – might be called existentialist. This is the answer that modernists themselves often give and that, lacking any other alternative to the Aristotelian view, they must give. It sees nothing on the other side but the pure and purely negative experience of freedom itself. The aim becomes to assert the self as freedom and to live freedom as rebellion against whatever is partial and facilitious in the established social or mental structures. The existentialist position seems unsatisfactory for reasons of its own It fails to acknowledge that enduring social and mental orders may differ from one another in the extent to which they display the truth about human freedom. Consequently, it is also powerless to deal adequately with a basic objection: freedom, to be real, must exist in lasting social practices and institutions; it cannot effectively exhaust itself in temporary acts of context smashing.

AT Government Surveillance with IoT Bad

Government started using surveillance well before the IoT

G. Alex Sinha, Aryeh Neier Fellow, Human Rights Watch and the American Civil Liberties Union, NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW Winter 2013, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2327806

Since shortly after 9/11, if not earlier, the National Security Agency (NSA) has been collecting massive amounts of data about American citizens and permanent residents, ostensibly with the aim of preempting future terrorist attacks.

Several meaningful reports about the scope of the program followed the passage of the FAA. In April of 2009, the New York Times revealed that the NSA had “intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress [in the FAA] . . .”¹⁵⁷ The Times suggested that the problem became apparent during the FAA certification process described above, which requires the Attorney General and Director of National Intelligence to submit surveillance protocols for approval by the FISC.¹⁵⁸ The Times also suggested that the over-collection of data may have been unintentional, at least in part the result of difficulties in distinguishing “between communications inside the United States and those overseas as [the NSA] uses its access to American telecommunication companies’ fiber-optic lines and its own spy satellites to intercept millions of calls and e-mail messages.”¹⁵⁹ A

Many existing NSA surveillance programs

G. Alex Sinha, Aryeh Neier Fellow, Human Rights Watch and the American Civil Liberties Union, NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW Winter 2013, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2327806

Within a matter of days, Edward Snowden came forward as the source of the documents underlying The Guardian’s reporting.¹⁹⁷ A twenty-nine-year-old former contractor who had spent the preceding four years working with the NSA, Snowden claimed to have been disturbed by the breadth of NSA surveillance and motivated by a desire to reveal more information about the program for the benefit of the public.¹⁹⁸ A number of subsequent reports appeared, many focused on Snowden himself,¹⁹⁹ as well as his efforts to seek asylum.²⁰⁰ As of September 2013, Russia had granted Snowden temporary asylum.²⁰¹ The media also published a number of subsequent stories about the NSA’s surveillance activities, many of them based on documents leaked by Snowden. First, The Guardian reported on an NSA sub-program called “PRISM.”²⁰² Citing secret, authenticated documents from within the NSA, The Guardian reported that PRISM ostensibly allows the NSA to gain direct access to ““emails, chat conversations, voice calls, documents and more . . . from the servers of . . . Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, [and] Apple.””²⁰³ All of the companies implicated in the program denied any knowledge that the government had direct access to their servers and insisted that they only turn over information to the government in the face of legitimate, specific requests to do so.²⁰⁴ The Guardian subsequently reported that the NSA has paid millions of dollars to the companies involved in PRISM to cover the costs of compliance with the program.²⁰⁵ The authority for the PRISM program appears to derive from the FAA, under a provision for the deliberate targeting of communications from “foreign nationals believed to be not on U.S. soil.”²⁰⁶ According to The Guardian, “Snowden’s revelations have shown that US emails and calls are collected in large quantities . . . either deliberately because the individual has been in contact with a

foreign intelligence target or inadvertently because the NSA is unable to separate out purely domestic communications.”²⁰⁷ The Guardian also revealed the existence of a sub-program called “Boundless Informant,”²⁰⁸ which allows the NSA to quantify the data it collects from U.S. computer systems.²⁰⁹ Boundless Informant appears to focus on transactional data,²¹⁰ and the ability of the NSA to discern “how much data [is] gathered from US computers” would seem to contradict some of its public statements.²¹¹ Further, The Guardian reported on the government’s interpretation of one of the provisions of the FAA described above—§ 702, which allowed the FISC to issue broad, yearlong warrants for the deliberate gathering of communications where the target of the surveillance is overseas.²¹² According to the Washington Post, “[t]he law prohibits officials from intentionally targeting data collection efforts at U.S. citizens or anyone in the United States” and “[t]he standards for intentional targeting require that an analyst have a ‘reasonable belief,’ at least 51 percent confidence, that the target is a foreign national.”²¹³ Yet much turns on the definition of the term “target,” and The Guardian validated the concerns of FAA critics who thought that incidental collection of American communications would be acceptable under at least one possible interpretation of the relevant statutory provision.²¹⁴

AT Privacy Key to Dignity

Any dignity harms is not quantifiable, permanent, or long-term

Heidi Reamer Anderson, Assistant Professor, Florida Coastal School of Law, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public," I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY v. 7 n. 3, 2012,
https://kb.osu.edu/dspace/bitstream/handle/1811/72997/ISJLP_V7N3_543.pdf?sequence=1

a. Refuting Assumptions that the Dignity Harm is Permanent, Irrefutable, and Quantifiable The first harm most often associated with the Obscurity Problem is a loss of dignity or other emotional harm felt by the person exposed and by persons who fear such exposure.¹⁷⁶ I do not question that some people subjected to the Obscurity Problem suffer some emotional harm that causes them sincere pain.¹⁷⁷ However, I do question whether this harm, as some scholars appear to have assumed or argued, is permanent, irrefutable, and quantifiable. The first assumption that potentially exaggerates the dignity harm is the assumption that such harm is permanent.⁷⁸ As noted above, some scholars claim that the Obscurity Problem makes one a "prisoner of his recorded past," suggesting that once one is exposed, one permanently drags around the exposed information like a tattoo or like a ball and chain around one's neck.⁷⁹ However, a cursory "where are they now"-style Internet search for the most oft-cited victims of the Obscurity Problem,¹⁸⁰ reveals that many were not damaged as much as one initially would think. Others that initially were harmed have returned to or risen to positions objectively better than before the exposure. For example, "Star Wars Kid," now a young adult, serves as President of a conservation society while studying for his law degree at McGill.¹⁸¹ Jonas Blank, the law firm associate whose profanely critical email traveled around the world, was hired full-time by the same top law firm he criticized.¹⁸² Countless others had their fifteen minutes of undignified fame fade even before or shortly after rising to the pitied status of an "example used in privacy scholar's work."⁸³ Further, the average shelf-life of any documented dignity harm likely will fade even more rapidly as more people are exposed, i.e., as the democratization of exposure expands.¹⁸⁴ This is because the increased amount of information available about individuals, and the ever-decreasing window of time during which a single piece of information remains in the public's collective interest, makes any one exposure less and less noticeable.⁸⁵ In sum, as more information about more people is made available in a shorter and shorter news cycle, the staying power of any one exposure is limited and the supposed permanence of the dignity harm grows ever more questionable.

Impact of the harm is overclaimed

Heidi Reamer Anderson, Assistant Professor, Florida Coastal School of Law, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public," I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY v. 7 n. 3, 2012,
https://kb.osu.edu/dspace/bitstream/handle/1811/72997/ISJLP_V7N3_543.pdf?sequence=1

The dignity harm also may be overstated because it appears based, at least in part, on the assumption that the victim of the harm cannot reduce the harm by responding in her defense. After an exposure, some serious emotional damage may have been done; however, that does not mean that it cannot be mitigated. Every alleged victim of an exposure has the opportunity to post a reply and many are quite effective.¹⁸⁷ Even Dog Poop Girl posted an online apology.¹⁸⁸ Additionally, exposure on the Internet unleashes a mob of eager factcheckers, raring to go and expose the initial citizen journalist as a fraud. For example, when Department of Agriculture official Shirley Sherrod was falsely "exposed" for saying, on tape, that she purposefully refused to help a farmer of a different race than her own, but further, near-immediate exposure, through the posting of and commentary regarding the entire tape, revealed that she in fact did help the farmer and that she learned a great lesson regarding race and class in society.⁸⁹ In this respect,

exposing the information to a large mass of people simultaneously helped improve the accuracy of the information. This automatic "right to reply" has not always been available (simply put, not everyone owned a newspaper) but now, the very technology some vilify is the same technology that empowers a reply.¹⁹⁰ And, most importantly, every reply reduces the harm associated with the exposure and loss of obscurity.¹⁹¹

Impossible to quantify

Heidi Reamer Anderson, Assistant Professor, Florida Coastal School of Law, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public," I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY v. 7 n. 3, 2012,
https://kb.osu.edu/dspace/bitstream/handle/1811/72997/ISJLP_V7N3_543.pdf?sequence=1

Finally, the dignity harm often is overstated because it cannot be quantified. Emotional harm is inherently subjective.¹⁹² The only one who accurately can quantify the harm is the person affected, and there is no direct way for the rest of us to get inside her head and feel the harm in the same way she feels it. This difficulty has led, at least in part, to the law's skepticism of emotional harm, especially when the alleged harm was caused by the sharing of truthful information. For example, a privacy tort plaintiff must be able to point to a specific harm, such as a reputational loss, versus mere "hurt feelings," in order to obtain damages.¹⁹³ The Supreme Court, too, has expressed a reluctance to limit speech based on its potential to hurt feelings.¹⁹⁴ Although it remains possible to assess the harm on an objective basis, assuming a rational, reasonable audience,¹⁹⁵ the currently unquantifiable nature of emotional harm makes the dignity harm a weak leg on which to support a right to obscurity.¹⁹⁶ Further, to the extent it can be quantified, the dignity harm likely is offset by the emotional benefits of exposure, as discussed in Part B below.

AT Need a Thinking Space

Assumptions of the thinking space argument are flawed

Heidi Reamer Anderson, Assistant Professor, Florida Coastal School of Law, "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public," I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY v. 7 n. 3, 2012,
https://kb.osu.edu/dspace/bitstream/handle/1811/72997/ISJLP_V7N3_543.pdf?sequence=1

The next harm—previously described as the destruction of perceived "thinking space"—is also overstated due to its apparent reliance on a questionable assumption. Namely, this harm assumes that a public, yet somewhat secure space absolutely free from later reporting by anyone of what has transpired there is necessary for, and helpful to thought development and free association, especially political thought and association. More pointedly, some seem to fear that if we let regular people report what they see and hear to millions of others at the click of a button, no one will say the important things that need to be said.¹⁹⁷ Although some people rightfully may feel that potential exposure discourages them from engaging in thoughtful debate,¹⁹⁸ others may feel that potential exposure to a huge and immediate audience encourages sharing and debate. In fact, the inherent appeal of reaching such a broad audience likely is partly responsible for the meteoric rise in the use of social networking sites like Twitter and Facebook. On these sites and elsewhere, many individuals and groups seek out exposure and publicity for their ideas, rather than hide from them. Their reasons for doing so presumably range from egotism or vanity to more utilitarian reasons, such as the fact that speaking with someone else about your thoughts often improves them or the fact that making one's ideas known helps them to spread and gain favor. Regardless of the precise reason that people share ideas with others, it simply cannot be said with convincing authority that people generally need a public-yet-private incubator for their secret camaraderie and thoughts.¹⁹⁹ Further, encouraging some people to pause before they share a thought may result in beneficial self-censorship.²⁰⁰ Thus, the "thinking space" harm likely has been overstated and obscurity is not a necessary prerequisite for thought generation and association. Various legal sources support the idea that the lack of public-yetprivate thinking space is an acceptable lack of obscurity rather than a serious harm. Perhaps the most recent and direct challenge to the idea that lack of thinking space in public is a serious harm comes from the Supreme Court in its recent decision, *Doe v. Reed*.²⁰¹ In *Doe*, the Supreme Court held that state disclosure of the names and addresses of those who sign petitions in support of ballot referenda does not categorically violate the petition signers' First Amendment speech rights.²⁰² In challenging the state statute requiring such disclosure, the signers of an anti-gay rights petition had argued that disclosing their names and addresses would chill speech, expose them to harassment and deprive them of privacy for their thoughts.²⁰³ This argument tracks that of privacy scholars who suggest that little to no obscurity will chill expression and thought development.²⁰⁴ The *Doe v. Reed* Court rejected this argument in an eight to one decision.²⁰⁵ Specifically, the Court found that the state law was a constitutional disclosure requirement that "may burden the ability to speak, but [does] not prevent anyone from speaking."²⁰⁶ In so finding, the court rejected a call for more privacy to facilitate activities deemed "intellectual,"²⁰⁷ at least when they have a lawmaking effect.²⁰⁸ Thus, in at least one context, the Supreme Court has considered and rejected the "lack of thinking space" privacy harm as a reason to restrict the exposure of truthful information. Another legal reality that undermines the perceived lack of thinking space harm is the fact that there already are adequate methods to obtain legal protection for one's ideas and thoughts when necessary—namely, confidentiality or nondisclosure agreements.²⁰⁹ If secrecy of publicized thought truly is valuable enough to someone, it can be obtained via an express agreement prior to or after it is shared.²⁰ Admittedly, obtaining such agreements involves various transaction costs that may deter their use by some speakers. However, the ubiquitous availability of these legal options at least questions whether one absolutely needs a right to obscurity in order to develop thought. Accordingly, the "thinking space" harm likely has been

overstated. Sunshine laws and the benefits they have produced also call into question the need for privacy in public in order to facilitate thought development.²¹¹ One subset of sunshine laws generally requires governmental policy-related meetings to be open to the public and, in many cases, recorded, and even posted on a website.¹² Similarly, many federal and state agencies require that people meeting with agency officials file a written notice describing what was discussed.²¹³ Further, our nation has a history of open town meetings.²⁴ If those most directly responsible for making public policy decisions do not need privacy in public, then it is at least questionable whether those with a more remote role need such absolute privacy either. Finally, much of the most justifiable fear regarding deprivation of thinking space is triggered only when the state is the one collecting the information or when the information collection is a constant, pervasive threat.²¹⁵ The Obscurity Problem involves neither statebased nor constant surveillance. State surveillance is not directly involved because it is "Little Stranger," and not "Big Brother," that is collecting the information.²¹⁶ When it is one's fellow citizens versus one's government officials doing the exposing, freedom of association and related issues are less of a concern.²¹⁷ Second, arguments regarding surveillance's potential to chill expression are most persuasive when the surveillance is constant, versus intermittent.²¹⁸ With the Obscurity Problem, surveillance is only occasional-and thus less of a threat to "thinking space."²¹⁹

AT Privacy an Absolute Right/Moral Obligation

The right to privacy can't be absolute

Robert Gerstein, Professor of Political Science, UCLA, PHILOSOPHICAL DIMENSIONS OF PRIVACY, Ferdinand Schoeman, ed., 1984, p.247-8.

If privacy is a constitutional right it is immediately apparent that it cannot be an absolute right. Governments have always compelled people to disclose some sorts of information about themselves, and it is hard to see how they could get along effectively without the ability to do so. If the argument for privacy is made so broadly as to sweep away tax returns, accident reports, and the capacity to compel testimony on personal matters in civil cases, for example, it must surely be rejected. The right of privacy cannot be understood as embodying the rule that "privacy may never be violated.

Privacy is not an absolute right – government must violate it to function

Robert **Gerstein, Professor of Political Science**, UCLA, PHILOSOPHICAL DIMENSIONS OF PRIVACY, Ferdinand Schoeman, ed., **1984**, p.247-8.

If privacy is a constitutional right it is immediately apparent that it cannot be an absolute right. Governments have always compelled people to disclose some sorts of information about themselves, and it is hard to see how they could get along effectively without the ability to do so. If the argument for privacy is made so broadly as to sweep away tax returns, accident reports, and the capacity to compel testimony on personal matters in civil cases, for example, it must surely be rejected. The right of privacy cannot be understood as embodying the rule that "privacy may never be violated."

The Fourth Amendment does not protect an absolute privacy right

Silas Wasterstrom, law professor, GEORGETOWN LAW JOURNAL, October 1998, pp. 61-2

Unfortunately, however, a rights-based approach does not mesh very well with the structure of the fourth amendment. The amendment, as commonly understood, does not provide an absolute shield against even the most extreme invasions of privacy and liberty. It does not establish a right to privacy that trumps competing policy concerns. Instead, the fourth amendment prohibits searches only when the likelihood that the invasion will be productive fails to justify the cost. In its most general form, this translates into an insistence that the search be reasonable. When the Court attempts to give the requirement a somewhat more determinate content, it insists that the search be supported by "probable cause" or "reasonable suspicion." In either case, however, the amendment requires no more than that the invasion be cost-justified in some sense.

Fourth Amendment rights and privacy claims are not absolute

Silas Wasterstrom, law professor, GEORGETOWN LAW JOURNAL, October 1998, p. 62

In this respect, the fourth amendment is crucially different from other constitutional guarantees, such as the freedom of speech, press, and religion, which may be more compatible with rights-based Kantian approaches. Of course, the rights protected by these provisions, as commonly understood, also may on occasion give way to especially compelling countervailing interests. But first amendment analysis does begin from the premise that there is a right to free speech, press, and religious worship, with a strong burden of proof on the party wishing to overcome the right. There is no comparable premise concerning a right to personal privacy built into the fourth amendment and no presumption against the validity of reasonable privacy invasions.

AT Privacy is an Inalienable Right”

Everyone does not value privacy, some are willing to trade it away for convenience, and their advocacy smacks of a paternalism that will result in social control

Adam Thierer / Adam is a senior research fellow at the Mercatus Center at George Mason University. He previously served as President of the Progress & Freedom Foundation, Director of Telecom Studies at the Cato Institute, and Fellow in Economic Policy at the Heritage Foundation, January 27, 2014, Is Privacy an Unalienable Right? The Problem with Privacy paternalism, <https://techliberation.com/2014/01/27/is-privacy-an-unalienable-right-the-problem-with-privacy-paternalism/>

Jeff Rosen now appears to be adopting the sort of approach Solove identifies by claiming that privacy is an “unalienable right” such that it cannot be traded away for other things. By making that choice for us, Rosen’s proposed amendment would, therefore, suffer from that same sort of privacy paternalism Solove identifies. In a forthcoming law review article that will appear in the *Maine Law Review*, I identify some of the problems associated with privacy paternalism. Most obviously, these scholars should keep in mind that not everyone shares the same privacy values as they do and that many of us will voluntarily trade some of our data for the innovative information services and devices that we desire. If imposed in the form of legal sanctions, privacy paternalism would open the door to almost boundless controls on the activities of both producers and consumers of digital services, potentially limiting future innovations in this space.

For example, when we were on *NPR* together, Rosen mentioned wireless geolocation technology as a potential source of serious privacy harm, although he did not make it clear whether he wanted it stopped entirely or what. If used improperly, wireless geolocation technology certainly can raise serious privacy concerns. But wireless geolocation technology is also what powers the mapping and traffic services that most of us now take for granted. Many of us expect — no, we *demand* — that our digital devices be able to give us real-time mapping and traffic notification capabilities. And most of us are willing to make the minor privacy trade-off associated with sharing our location constantly in exchange for the right to receive these services, which are also provided to us free of charge.

Rights do not exist to protect us from ourselves – it is within our rights to trade convenience for a loss of privacy

Adam Thierer / Adam is a senior research fellow at the Mercatus Center at George Mason University. He previously served as President of the Progress & Freedom Foundation, Director of Telecom Studies at the Cato Institute, and Fellow in Economic Policy at the Heritage Foundation, January 27, 2014, Is Privacy an Unalienable Right? The Problem with Privacy paternalism, <https://techliberation.com/2014/01/27/is-privacy-an-unalienable-right-the-problem-with-privacy-paternalism/>

As I will discuss in my forthcoming *Maine Law Review* article and I also discussed in my recent *George Mason University Law Review* article, at least here in the United States, consumer protection standards have traditionally depended on a clear showing of *actual*, not prospective or hypothetical, harm. In some cases, when the potential harm associated with a particular practice or technology is extreme in character and poses a direct threat to physical well-being, law has preempted the general presumption that ongoing experimentation and innovation should be allowed by default. But these are extremely rare scenarios, at least as it pertains to privacy concerns under American law, and they mostly involved health and safety measures aimed at preemptively avoiding catastrophic harm to individual or environmental well-being. In the vast majority of other cases, our culture has not

accepted that paternalistic idea that law must “save us from ourselves” (i.e., our own irrationality or mistakes). As Solove notes in his recent essay, “People make decisions all the time that are not in their best interests. People relinquish rights and take bad risks, and the law often does not stop them.”

AT “Privacy is a Right”

Privacy is not a right

Jim Harper is the editor of Prvacilla.org and director of information policy studies at the Cato Institute, 2004, Understanding Privacy – and the Real Threats to It,
<http://object.cato.org/sites/cato.org/files/pubs/pdf/pa520.pdf>

Though generations of advocates have called information privacy a “right,” the better view is that it is not. Privacy is a condition people maintain by exercising personal initiative and responsibility. Other legal rights allow them to do this. An example can illustrate how something as vitally important as privacy is not a right: Most people agree that individuals should be allowed to develop and follow their own sense of morality, as long as they do not harm others. People may decide for themselves, for example, whether a higher power exists; whether bad acts have consequences in a future life; and whether to sing, pray, or remain silent. These, one could argue, reflect a “right” to morality. As important as morality is, though, there is no “right” to it. Instead, morality is a quality that individuals develop and practice in the shelter given by individual rights like the right to free speech, the right to free exercise of religion, the right to associate with others, and the right to own property. These rights protect individuals from government interference and shelter essential human institutions like morality. People who seek morality as an entitlement from government are censors, at best. Privacy is the same kind of “good.” It is developed and maintained in the shelter of legal rights that give individuals autonomy. Maintaining privacy requires that we know how information moves and that we refrain from sharing what we wish to keep private. Privacy is not a gift from politicians or an entitlement that can be demanded from government. Privacy is a product of personal responsibility. Like moral living, privacy is the product of careful consideration and concerted effort by individuals. To be sure, protecting privacy can be hard. It involves knowledge, vigilance, and constant trade-offs. But if protecting privacy in private-sector interactions is hard, protecting privacy from government is impossible. Governments have the power to take personal information from citizens by force of law. After they collect it, they can change the rules under which they keep and use personal information. And they often stand in the way of steps people might otherwise take to protect privacy. That makes governments the most formidable threat to privacy. Though nearly always animated by good intentions, nearly every government program undermines privacy in some way. It is fair to say that lost privacy is a cost of government. Those interested in

allowing individuals to protect their own conceptions of privacy will address this most significant threat to privacy first.

AT Privacy Key to Democracy

Information seclusion undermines democracy

Paul M. Schwartz, law professor, 1999, Brooklyn, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613, <http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf>

Privacy-control as permitting information seclusion is swept aside because of two collective demands that weigh heavily against this right. First, as shown in this Article's discussion of democratic deliberation, public accountability often requires outside access to personal information.³³¹ Second, as indicated in this Article's analysis of managerial data processing, bureaucratic rationality often demands outside access to personal information.³³² The idea of data seclusion is a deceptive paradigm because it applies to such a narrow exception. Information seclusion is rarely achievable. As a result, scholars and courts, in their evaluation of interests, frequently reject entirely personal claims framed in terms of privacy-control in favor of requests for personal data made by outside entities, whether the state or private organizations.³³³

Elderly are willing to accept privacy limits for the benefits of home monitoring

- . Jillisa Bronfman, Director, Privacy and Technology Project, Institute for Innovation Law, University of California-Hastings, Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population, DUKE LAW & TECHNOLOGY REVIEW v. 14, February 2016,
<http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1289&context=dltr>
- . to consumers. Home monitoring technologies upgrade the consumer and the consumer's home to a higher standard of living at a low cost. In the case of monitoring elderly and disabled consumers, the cost of a home health care aide may be excessive or prohibitive,⁵ relative to purchasing a small device, even with monthly fees. Thus, because just the necessary devices may be purchased, the home monitoring system may be more cost-effective as well as more structurally flexible to scale up and down based on individual needs for assistance. Further, empirical studies have shown that older individuals value home monitoring devices because such devices allow them to age in place, among other reasons.⁶ Next, we should question the amount of private information traded for the use of these new technologies. There is some room for individual variance, but there is also a threshold level of information required for basic participation. Each user must consider how much

individual or family information she is willing to upload into the thermostat or medical alert device in order for the device to function optimally. In many cases, the elderly, and particularly the frail or disabled elderly, are willing to downgrade the general expectation of privacy in order to receive the benefits of safety and monitoring technology in the home.⁷