Premier Debate

January 2021

Expert PF Brief

PremierDebate.com

Like Us on Facebook

Introduction

Friends of Premier Debate,

Welcome to the new year! The January topic is "**Resolved: The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents."** We are excited to help you prepare on this topic!

This topic is broad and offers a wide variety of contentions, spanning from rights-based contentions about privacy to technical details about national security. Success on this topic will require ingenuity and strong evidence.

This expert brief provides **over 100 additional cards**. These include additional framing evidence, new aff contentions (internet freedom, whistleblowing, cybersecurity, efficiency), new neg contentions (circumvention, disease, presidential powers), and additional link/impact arguments. These arguments should give you a competitive edge for this topic.

Best practice for brief use is to use it as a guide for further research. Find the articles and citations and cut them for your own personal knowledge. You'll find even better cards that way. If you want to use the evidence in here in a pinch, you should at least re-tag and highlight the evidence yourself so you know exactly what it says and how you're going to use it. Remember, briefs can be a tremendous resource but you need to familiarize yourself with the underlying material first.

We're always looking for ways to make the briefs better, so please, let us know what you think! And, if you use these briefs please help us direct other debaters to premierdebate.com/briefs where we will continue uploading .doc versions of the briefs.

If you like what we're doing and these cards have been helpful to you, consider signing up for online coaching through Premier Debate. Our coaches were elite competitors in their own right and have now coached students to elimination rounds, earning TOC bids, and qualifying to state and national championships. See premierdebate.com/coaching for more details on how to apply!

Finally, we'd like to thank Amy Santos and Peter Zhang for their help in assembling this brief. These are some of the best, round-ready cards you'll see on the topic, and we couldn't have done it without them.

Good luck everyone. See you 'round!

Bob Overing & John Scoggin

Directors | Premier Debate

Table of Contents

Background

NSA

Cooperation

The NSA cooperates with the CSS and 16 other agencies.

Rouse 18 Margaret Rouse writes for and manages WhatIs.com, TechTarget's IT encyclopedia and learning center. "National Security Agency." Tech Target. March 2018. https://searchsecurity.techtarget.com/definition/National-Security-Agency. [Premier]

The National Security Agency is the official U.S. cryptologic organization of the United States Intelligence Community under the Department of Defense.

Responsible for the coordination of communications intelligence activities throughout the government, the top secret NSA was covertly formed in November 1952 under a directive from President Harry S. Truman and the National Security Council.

Secrecy around the agency's activities has suffered, however, as security breaches have exposed global surveillance programs and cyberweapons -- malware agents -- developed to target computers and networks of U.S. adversaries.

Responsibilities of the NSA

The agency exists to protect national communications systems integrity and to collect and process information about foreign adversaries' secret communications to support national security and foreign policy. The classified information is disseminated to 16 separate government agencies that make up the U.S. Intelligence Community.

In October 2017, Attorney General Loretta Lynch signed new guidelines to enable the NSA to provide intercepted communications and raw signals intelligence -- before applying domestic and foreign privacy protections -- to **16 government agencies**, including the FBI and CIA.

The National Security Agency works in close conjunction with the Central Security Service, which was established by presidential executive order in 1972 to promote full partnership between the NSA and the cryptologic elements of the armed forces. The director of the NSA/CSS, in accordance with a Department of Defense directive, must be a high-ranking -- at least three stars -- commissioned officer of the military services.

Although the organization's number of employees -- as well as its budget -- falls into the category of classified information, the NSA lists among its workforce analysts, engineers, physicists, linguists, computer scientists, researchers, customer relations specialists, security officers, data flow experts, managers, and administrative and clerical assistants.

It also claims to be the largest employer of mathematicians in the U.S., and possibly worldwide. NSA/CSS mathematicians perform the agency's two critical functions: they design cryptographic systems to protect U.S. communications, and they search for weaknesses in the counterpart systems of U.S. adversaries.

The NSA denies reports claiming that it has an unlimited black budget -- undisclosed even to other government agencies. Nevertheless, the agency admits that, if it were judged as a corporation, it would rank in the top 10% of Fortune 500 companies.

Technique

The NSA uses private partnerships and intercept centers to collect information.

EFF EFF. "How It Works." Electronic Frontier Foundation. No Date. https://www.eff.org/nsa-spying/how-it-works. [Premier]

The NSA's domestic spying program, known in official government documents as the "President's Surveillance Program," ("The Program") was implemented by President George W. Bush shortly after the attacks on September 11, 2001. The US Government still considers the Program officially classified, but a tremendous amount of information has been exposed by various whistleblowers, admitted to by government officials during Congressional hearings and with public statements, and reported on in investigations by major newspaper across the country.

Our NSA Domestic Spying Timeline has a full list of important dates, events, and reports, but we also want to explain—to the extent we understand it—the full scope of the Program and how the government has implemented it.

In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades. When the NSA's spying program was first exposed by the New York Times in 2005, President Bush admitted to a small aspect of the program—what the administration labeled the "Terrorist Surveillance Program"—in which the NSA monitored, without warrants, the communications of between 500-1000 people inside the US with suspected connections to Al Qaeda.

But other aspects of the Program were aimed not just at targeted individuals, but perhaps millions of innocent Americans never suspected of a crime.

Details of Every American's Call History

First, the government convinced the major telecommunications companies in the US, including AT&T, MCI, and Sprint, to hand over the "**call-detail records**" of their customers. According to an investigation by USA Today, this included "customers' names, street addresses, and other personal information." In addition, the government received "detailed records of calls they made—across town or across the country—to family members, co-workers, business contacts and others."

A person familiar with the matter told USA Today that the agency's goal was "to create a database of every call ever made" within the nation's borders. All of this was done without a warrant or any judicial oversight.

Real Time Access to Phone and Internet Traffic

Second, the same telecommunications companies also allowed the NSA to install sophisticated communications surveillance equipment in secret rooms at key telecommunications facilities around the country. This equipment gave the NSA unfettered access to large streams of domestic and international communications in real time—what amounted to at least 1.7 billion emails a day, according to the Washington Post. The NSA could then data mine and analyze this traffic for suspicious key words,

patterns and connections. Again, all of this was done without a warrant in violation of federal law and the Constitution.

The Technology That Made It Possible

But how did the government accomplish this task and how do we know? In addition to investigative reports by the New York Times and others, AT&T technician turned whistleblower Mark Klein provided EFF with eyewitness testimony and documents describing one such secret room located at AT&T's Folsom Street facility in San Francisco, California.

It works like this: when you send an email or otherwise use the internet, the data travels from your computer, through telecommunication companies' wires and fiber optics networks, to your intended recipient. To intercept these communications, the government installed devices known as "fiber-optic splitters" in many of the main telecommunication junction points in the United States (like the AT&T facility in San Francisco). These splitters make exact copies of the data passing through them: then, one stream is directed to the government, while the other stream is directed to the intended recipients.

The Klein documents reveal the specific equipment installed at the AT&T facility and the processing power of the equipment within the secret rooms. One type of machine installed is a Narus Semantic Traffic Analyzer, a powerful tool for deep packet inspection. Narus has continually refined their capabilities and—as of the mid-2000s—each Narus machine was capable of analyzing 10 gigabits of IP packets, and 2.5 gigabits of web traffic or email, per second. It is likely even more powerful today. The Narus machine can then reconstruct the information transmitted through the network and forward the communications to a central location for storage and analysis.

In a declaration in our lawsuit, thirty-year NSA veteran William Binney estimates that "NSA installed no few than ten and possibly in excess of twenty intercept centers within the United States." Binney also estimates NSA has collected "between 15 and 20 trillion" transactions over the past 11 years.

In April 2012, long-time national security author James Bamford reported NSA is spending $2 billion to construct a data center in a remote part of Utah to house the information it has been collecting for the past decade. "Flowing through its servers and routers and stored in near-bottomless databases," Bamford wrote, "will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'"

Phone Surveillance

While the NSA may give up authorities under the Freedom Act, it still has powers under FISA.

Shackford 19 Scott Shackford is an associate editor at Reason. "The NSA Defended the Domestic Surveillance That Snowden Exposed. Now the Agency Wants to End It." Reason. 25 May 2019. https://reason.com/2019/04/25/the-nsa-defended-the-domestic-surveillance-that-snowden-exposed-now-the-agency-want-to-end-it/. [Premier]

But the NSA reportedly stopped trying to access these phone records earlier in the year, and now The Wall Street Journal reports that the agency says it doesn't want the program any more. That's a big deal, as the powers granted by the USA Freedom Act are up for renewal this year.

There are a few likely reasons why this is happening. First: Though officials kept insisting that the authority to collect these records was vital to tracking down terrorism, it has yet to be credited for catching any terrorists or stopping any terrorist acts. Second: The NSA has found itself collecting massive amounts of private data that it acknowledges it's not allowed to have, forcing it to purge its records. Third: In the time since the NSA first launched this surveillance—back in 2001, when the PATRIOT Act was passed—smartphone users have shifted away from communicating through voice conversations and are more likely to use apps (particularly encrypted ones) to communicate via texting.

If the USA Freedom Act goes away, that doesn't mean that the federal government will lose all its authority to snoop on Americans. Just last year, Congress and President Donald Trump renewed and expanded the feds' powers under the Foreign Intelligence Surveillance Act to secretly surveil Americans for wholly domestic criminal matters.

Domestic

Programs

The two main domestic surveillance programs are executive order 12333 and Section 702 of FISA.

St. Vincent 19 Sarah St.Vincent is a researcher on U.S. national security and surveillance at Human Rights Watch. "National Security Agency's Domestic Spying Program Needs to End Permanently." The Progressive. 18 March 2019. https://progressive.org/op-eds/nsa-domestic-spying-must-end-st.vincent-190318/. [Premier]

The reforms Congress imposed in the USA Freedom Act were a good start, but insufficient to end the human rights violations this domestic spying entailed. If this program is indeed dormant, the government should let it stay that way until the law underpinning it expires.

Congress should also look hard at other surveillance activities that may **trample rights domestically** and abroad. These include snooping under the highly secretive **Executive Order 12333**, a 1981 authority that could let the NSA spy on people in the United States, and Section 702 of the **Foreign Intelligence Surveillance Act**, which allows widespread NSA and FBI use of warrantless surveillance.

As the experience with the domestic call-records program shows, government claims that spying activities are justified should not be taken at face value – and the intrusion on rights should be taken seriously.

The three domestic surveillance programs are section 702, EO 12333, and the Patriot Act.

BC 18 "Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page." Brennan Center. 25 October 2018. https://www.brennancenter.org/our-work/research-reports/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333. [Premier]

The term "foreign intelligence" conjures images of spies collecting information about our adversaries in other countries. But Americans can get caught up in foreign intelligence investigations, too – whether they are targets themselves, communicating with targets, or simply sending e-mails that get stored or routed overseas.

Since the 1970s, there have been laws in place to safeguard the rights of Americans in foreign intelligence investigations. But some of these laws have been significantly weakened since 9/11, while others were too weak to begin with. The inadequacy of civil liberties protections in the law creates enormous potential for abuse without any corresponding security benefit.

This collection of resources focuses on **three legal authorit**ies that provide insufficient protection for the privacy rights of Americans and law-abiding citizens of other countries.

Section 702 of the Foreign Intelligence Surveillance Act (FISA): This law was passed in 2008 to legalize President George W. Bush's warrantless wiretapping program. It removed the requirement, in place

since 1978, that the government obtain a warrant from the FISA Court when seeking to wiretap communications between a foreign target and an American from inside the U.S. It also greatly broadened the scope of permissible foreign targets to include private citizens not suspected of any wrongdoing. The FISA Court must approve the general procedures for Section 702 surveillance but does not approve individual targets.

Although the target must be a foreigner overseas, Section 702 surveillance is believed to result in the "incidental" collection of millions of Americans' communications. Agencies make broad use of these communications, notwithstanding the fact that Section 702 requires them to "minimize" the retention and sharing of Americans' information. For instance, the FBI may comb through Section 702 data for information to use against Americans in ordinary criminal cases.

Executive Order 12333: This order, issued by President Reagan in 1981, governs electronic surveillance that the NSA conducts overseas. Unlike NSA surveillance conducted domestically (which is regulated under Section 702), overseas surveillance is not subject to any judicial oversight, and congressional oversight is limited.

While Executive Order 12333 prohibits the targeting of individual Americans, it allows "bulk collection," resulting in the acquisition of massive amounts of Americans' communications and other data. Under one program, for instance, the NSA collects and stores for 30 days all of the phone calls coming into and out of certain countries, including the Bahamas.

Section 215 of the Patriot Act: Passed in the immediate aftermath of 9/11, Section 215 allowed the NSA to acquire "any tangible thing" from third parties (such as telephone companies) if it could persuade the FISA Court that the item was "relevant" to a foreign intelligence investigation. In 2013, Edward Snowden revealed that the NSA was using this authority to collect Americans' telephone records in bulk. The FISA Court approved the collection, interpreting Section 215 to permit the collection of vast quantities of irrelevant records so long as there were relevant records buried within them.

In 2015, Congress enacted the USA Freedom Act to end the NSA's bulk collection program. In its place, Congress created a new program under which the NSA can obtain the telephone records of suspected terrorists and anyone in contact with them.

XO 12333 = Topical

XO12333 includes foreign and domestic – we only limit collection on Americans

Schneier 15 Bruce Schneier, 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. "Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World." 2015. https://books.google.com/books/about/Data_and_Goliath.html?id=_grPBgAAQBAJ. [Premier]

Executive Order 12333, the 1981 presidential document authorizing most of NSA's surveillance, is incredibly permissive. It is supposed to primarily allow the NSA to conduct surveillance outside the US, but it gives the agency **broad authority to collect data on Americans**. It provides minimal protections for Americans' data collected outside the US, and even less for the hundreds of millions of innocent non-Americans whose data is incidentally collected. Because this is a presidential directive and not a law, courts have no jurisdiction, and congressional oversight is minimal. Additionally, at least in 2007, the president believed he could modify or ignore it at will and in secret. As a result, we know very little about how Executive Order 12333 is being interpreted inside the NSA.

Bulk records collection means the NSA inevitably captures domestic communications – it's incapable of excluding it

Sommer 14 Jacob. "FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition" Litigation, Spring 2014, Vol. 40 No. 3 http://www.americanbar.org/publications/litigation_journal/2013-14/spring/fisa_authority_and_blanket_surveillance_gatekeeper_without_opposition.html. [Premier]

The NSA discontinued SHAMROCK in 1975, but it still incidentally collected Americans' communications—much like it does (to a lesser extent) today. The Church Committee described the NSA's "initial interception of a stream of communications" as "analogous to a vacuum cleaner." "NSA picks up all communications carried over a specific link that it is monitoring. The combination of this technology and the use of words to select communications of interest results in NSA analysts reviewing the international messages of American citizens, groups, and organizations for foreign intelligence." Id. at 741. This is eerily similar to the FISC's description of bulk records collection as recently as October 2011, in which it stated "that NSA has acquired, is acquiring, and . . . will continue to acquire tens of thousands of **wholly domestic** communications," Redacted, slip op. at 33 (FISA Ct. Oct. 3, 2011), because it intercepts **all communications** over certain Internet links it is monitoring and is "**unable to exclude certain Internet transactions**." Id. at 30.

Servers are located in different geographical locations

Arnbak and Goldberg 14 Axel Arnbak, 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, and Sharon Goldberg, Associate

professor in the Computer Science Department at Boston University, phD from Princeton University, B.A.S.c from University of Toronto/ “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad.” Working Paper. 27 June 2014. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1204&context=mttlr. [Premier]

3.1 Why US Traffic can Naturally be Routed Abroad.

The Internet was not designed around geopolitical borders; instead, its design reflects a focus on providing robust and reliable communications while, at the same time, minimizing cost. For this reason, network traffic between two endpoints located on US soil can sometimes be routed outside the US.

3.1.1 Interception in the Intradomain.

A network owned by a single organization (even an organization that is nominally “based” in the U.S. such as Yahoo! or Google) can be physically located in multiple jurisdictions. The revealed MUSCULAR/TURMOIL program illustrates how the N.S.A. exploited this by presuming authority under EO 12333 to acquire traffic between Google and Yahoo! servers located on foreign territory, collecting up to 180 million user records per month, regardless of nationality [17].5 Yahoo! and Google replicate data across multiple servers that periodically send data to each other, likely for the purpose of backup and synchronization. These servers are located in geographically diverse locations, likely to prevent valuable data from being lost in case of failures or errors in one location. The MUSCULAR/TURMOIL program collects the traffic sent between these servers: while this traffic can traverse multiple jurisdictions, it remains with the logical boundaries of the internal networks of Yahoo! and Google. Thus, we already have one example where loopholes under the legal regime of EO 12333 were exploited in the intradomain, i.e., within the logical boundaries of a network owned by a single organization.

XO 12333 ≠ Topical

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." Harvard National Security Journal, 6. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2409&context=articles. [Premier]

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.

Curtailing XO 12333 isn't topical—it surveils non-US persons

Arnbak and Goldberg 14 Axel Arnbak, 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, and Sharon Goldberg, Associate professor in the Computer Science Department at Boston University, phD from Princeton University, B.A.S.c from University of Toronto/ "Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting the Network Traffic Abroad." Working Paper. 27 June 2014. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1204&context=mttlr. [Premier]

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.

Section 702 = Topical

702 governs collection within the US

Schneier 15 Bruce Schneier, 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. "Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World." 2015. https://books.google.com/books/about/Data_and_Goliath.html?id=_grPBgAAQBAJ. [Premier]

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.**

Section 702 gathers U.S. person data

Bates 14 John Bates, 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. "Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act." Administrative Office of the United States Courts. 10 January 2014. http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf. [Premier]

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

FISA's internationality requirement is vague and allows targeting purely domestic groups

Harper 14 Nick, University of Chicago Law School, U.S. Department of Justice, Civil Division. "FISA's Fuzzy Line between Domestic and International Terrorism." University of Chicago Law Review, 81(3). Summer 2014.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclr81&div=35&id=&page=. [Premier]

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 dis- seminate.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 loose internationality requirement allows surveillance of domestic groups

Harper 14 Nick, University of Chicago Law School, U.S. Department of Justice, Civil Division. "FISA's Fuzzy Line between Domestic and International Terrorism." University of Chicago Law Review, 81(3). Summer 2014.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclr81&div=35&id=&page=. [Premier]

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 Jacob. "FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition" Litigation, Spring 2014, Vol. 40 No. 3 http://www.americanbar.org/publications/litigation_journal/2013-14/spring/fisa_authority_and_blanket_surveillance_gatekeeper_without_opposition.html. [Premier]

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**.

Section 702 ≠ Topical

Section 702 is strictly over foreign citizens

Mukasey 14 Michael Mukasey, former U.S. Attorney General, judge for the Southern District of New York, B.A. from Columbia, LL.B. from Yale. "Safe and SAFE AND SURVEILLED: FORMER U.S. ATTORNEY GENERAL MICHAEL B. MUKASEY ON THE NSA, WIRETAPPING, AND PRISM, National Security Law Journal. 25 March 2014. https://www.nslj.org/wp-content/uploads/3_NatlSecLJ_196-209_Mukasey.pdf. [Premier]

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 13 Brett, Business Insider's politics editor. "Here's The Law The Obama Administration Is Using As Legal Justification For Broad Surveillance." Business Insider. June 2013. http://www.businessinsider.com/fisa-amendments-act-how-prism-nsa-phone-collection-is-it-legal-2013-6. [Premier]

"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.

AT: Collection Overseas

It's domestic surveillance even if collection occurs overseas – geographic limits are impossible

Lee 13 Timothy, Senior Editor at Vox. "The NSA is trying to have it both ways on its domestic spying programs." Washington Post. 22 December 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/22/the-nsa-is-trying-to-have-it-both-ways-on-its-domestic-spying-programs/. [Premier]

But now the Internet has **made a hash of the tidy distinction** between foreign and domestic surveillance. Today, citizens of France, Brazil and Nigeria routinely use Facebook, Gmail, and other American online services to communicate. Americans make calls with Skype. And much Internet traffic between two foreign countries often passes through the United States.

The NSA has reacted to this changing communications landscape by trying to claim the best of both worlds. The FISA Amendments Act, passed in 2008, gave the NSA the power to compel domestic telecommunications providers to cooperate with the NSA's surveillance programs. Yet the NSA has resisted the transparency and judicial oversight that has traditionally accompanied domestic surveillance. They've argued that disclosing the existence of these programs would compromise their effectiveness. And they've argued that because the "targets" of surveillance are overseas, only limited judicial oversight by the secretive Foreign Intelligence Surveillance Court, not individualized Fourth Amendment warrants, were required.

But the NSA programs revealed by Snowden, including PRISM and the phone records program, look **more like domestic surveillance programs than foreign ones**. Like conventional domestic wiretaps, they rely on **compelling domestic firms to cooperate with surveillance**. Like conventional wiretaps, they sweep up information about the communications of Americans on American soil. And like domestic wiretaps, information collected by the NSA is sometimes shared with domestic law enforcement agencies for prosecution of Americans.

If the NSA is going to run what **amounts to a domestic surveillance program** that collects the **private information of Americans on American soil**, it's going to face pressure to subject that program to the same kind of oversight as other domestic surveillance program. That means disclosing the general characteristics of the program—but not the specific targets—to the public. And it means requiring individualized warrants, supported by probable cause, before the government can intercept the communications of Americans on American soil.

AT: Targets = Deliberate

Incidental collection is deliberate – Americans are actually the target

Goitein, 13 Elizabeth, co-directs the Liberty and National Security Program at New York University School of Law's Brennan Center for Justice. "The NSA's Backdoor Search Loophole." Boston Review. 2013. http://bostonreview.net/blog/elizabeth-goitein-nsa-backdoor-search-loophole-freedom-act. [Premier]

Even though the target must be a non-citizen, programmatic surveillance under section 702 sweeps up all international communications to, from, or about the target. This includes communications coming into or out of the United States. Granted, the NSA may capture these calls and e-mails only if it intends to acquire "foreign intelligence information." But the FAA defines this term so broadly—it encompasses any information relevant to the foreign affairs of the United States – that it would in theory permit the capture of almost all communications between Americans and their friends, relatives, or business associates overseas. The NSA refers to this as "incidental" collection, but there is nothing "incidental" about it. As officials made clear during the debates leading up to the enactment of section 702, communications involving Americans were "**the most important** to us."

Surveillance

Zero Day ≠ Topical

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. "NSA Mass Surveillance Programs - Unnecessary and Disproportionate." Electronic Frontier Foundation. 29 May 2014. https://www.eff.org/deeplinks/2014/05/unnecessary-and-disproportionate-how-nsa-violates-international-human-rights. [Premier]

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.

Disease Surveillance ≠ Topical

Domestic surveillance is distinct from disease surveillance.

EPIS n.d. Empire Pacific Investigative Service, an organization run by retired U.S. Federal Special Agents. "Los Angeles Domestic Surveillance Investigations." No Date. epis.us/services/domestic-surveillance-investigations/. [Premier]

SURVEILLANCE IN DEFINITION

Domestic Surveillance - Surveillance is the monitoring of the behavior, activities, or other changing information, usually **of people** and often in a surreptitious manner. It most usually refers to observation of individuals or groups by government organizations, but disease surveillance, for example, is monitoring the progress of a disease in a community.

Preventative Intent

"Surveillance" is monitoring with preventive intent

Lemos 10 André Lemos, Associate Professor at Faculty of Communication at Federal University of Bahia. "Locative Media and Surveillance at the Boundaries of Informational Territories." ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks. January 2010. https://www.researchgate.net/publication/290900628_Locative_Media_and_Surveillance_at_the_Boundaries_of_Informational_Territories. [Premier]

Although they often appear to be synonymous, it is **important to distinguish** between **informational control**, **monitoring** and **surveillance** so that the problem can be **better understood**. We consider control to be the supervision of activities, or actions normally associated with government and authority over people, actions and processes. Monitoring can be considered a form of observation to gather information with a view to making projections or constructing scenarios and historical records, i.e., the action of following up and evaluating data. Surveillance, however, can be defined as an act **intended to avoid something**, as an observation whose **purposes** are **preventive** or as behavior that is attentive, cautious or careful. It is interesting to note that in English and French the two words "vigilant" and "surveillance", each of which is spelt the same way and has the same meaning in both languages, are applied to someone who is particularly watchful and to acts associated with legal action or action by the police intended to provide protection against crime, respectively. We shall define surveillance as actions that imply control and monitoring in accordance with Gow, for whom surveillance "implies something **quite specific** as the **intentional** observation of someone's actions or the intentional gathering of personal information in order to observe actions taken in the past or future" (Gow, 2005, p. 8).

According to this definition, surveillance actions presuppose monitoring and control, but **not all forms of control and/or monitoring can be called surveillance**. It could be said that all forms of surveillance require two elements: **intent** with a view to avoiding causing something and **identification** of individuals or groups by **name. It seems** to me to be **difficult to say** that **there is surveillance if there is** no identification of the person under observation (anonymous) and **no preventive intent (avoiding something)**. To my mind it is an **exaggeration** to say, for example, that the system run by my cell phone operator that controls and monitors my calls is keeping me under surveillance. Here there is identification but **no intent**. However, it can certainly be used for that purpose. The Federal Police can request wiretaps and disclosure of telephone records to monitor my telephone calls. The same can be said about the control and monitoring of users by public transport operators. This is **part of the administrative routine** of the companies involved. Once again, however, the system can be used for surveillance activities (a suspect can be kept under surveillance by the companies' and/or police's safety systems). Note the example further below of the recently implemented "Navigo" card in France. It seems to me that the social networks, collaborative maps, mobile devices, wireless networks and countless different databases that make up the information society do indeed control and monitor and offer a real possibility of surveillance.

Collecting information without intent is just information gathering, which isn't topical.

Fuchs 11 Christian Fuchs, Professor of Social Media at the University of Westminster's Centre for Social Media Research. "New Media, Web 2.0 and Surveillance." Sociology Compass, 5(2). 1 February 2011. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1751-9020.2010.00354.x. [Premier]

Theoretical foundations of surveillance studies

'Living in ''surveillance societies'' may throw up challenges of a fundamental – ontological – kind' (Lyon 1994, 19). Social theory is a way of clarifying such ontological questions that concern the basic nature and reality of surveillance. An important ontological question is how to define surveillance. One can distinguish **neutral** concepts and **negative** concepts.

For Max Horkheimer, neutral theories 'define universal concepts under which all facts in the field in question are to be subsumed' (Horkheimer 1937 / 2002, 224). Neutral surveillance approaches define surveillance as the systematic collection of data about humans or non-humans. They argue that surveillance is a characteristic of all societies. An example for a well-known neutral concept of surveillance is the one of Anthony Giddens. For Giddens, surveillance is 'the coding of information relevant to the administration of subject populations, plus their direct supervision by officials and administrators of all sorts' (Giddens 1984, 183f). Surveillance means 'the collation and integration of information put to administrative purposes' (Giddens 1985, 46). For Giddens, all forms of organization are in need of surveillance in order to work. 'Who says surveillance says organisation' (Giddens 1981, xvii). As a consequence of his general surveillance concept, Giddens says that all modern societies are information societies (Giddens 1987, 27; see also: Lyon 1994, 27).

Basic assumptions of neutral surveillance concepts are:

• There are positive aspects of surveillance.

• Surveillance has two faces, it is enabling and constrainig.

• Surveillance is a fundamental aspect of all societies.

• Surveillance is necessary for organization.

• Any kind of systematic information gathering is surveillance.

Based on a neutral surveillance concept, all forms of online information storage, processing and usage in organizations are types of Internet surveillance. Examples include: the storage of company information on a company website, e-mail communication between employees in a governmental department, the storage of entries on Wikipedia, the online submission and storage of appointments in an e-health system run by a hospital or a general practitioner's office. The example shows that based on a neutral concept of surveillance, the notion of Internet surveillance is **fairly broad**.

Negative approaches see surveillance as a form of systematic information gathering that is **connected to** domination, **coercion**, the threat of using violence or the actual use of violence in order to attain certain goals and accumulate power, in many cases against the will of those who are under surveillance. Max Horkheimer (1947 / 1974) says that the 'method of negation' means 'the denunciation of everything that mutilates mankind and impedes its free development' (Horkheimer 1947 / 1974, 126). For Herbert Marcuse, negative concepts 'are an indictment of the totality of the existing order' (Marcuse 1941, 258).

The best-known negative concept of surveillance is the one of Michel Foucault. For Foucault, surveillance is a form of disciplinary power. Disciplines are 'general formulas of domination' (Foucault 1977, 137). They enclose, normalize, punish, hierarchize, homogenize, differentiate and exclude (Foucault 1977, 183f). The 'means of coercion make those on whom they are applied clearly visible' (Foucault 1977, 171). A person that is under surveillance 'is seen, but he does not see; he is the object of information, never a subject in communication' (Foucault 1977, 200). The surveillant panopticon is a 'machine of power' (Foucault 2007, 93f).

In my opinion, there are **important arguments** speaking against defining surveillance in a neutral way:

1. Etymology: The French word surveiller means to oversee, to watch over. It implies a hierarchy and is therefore connected to notions, such as watcher, watchmen, overseer and officer. Surveillance should therefore be conceived as technique of coercion (Foucault 1977, 222), as 'power exercised over him [an individual] through supervision' (Foucault 1994, 84).

2. Theoretical conflationism: Neutral concepts of surveillance put certain phenomena, such as taking care of a baby or the electrocardiogram of a myocardial infarction patient, on one analytical level with very different phenomena, such as preemptive state-surveillance of personal data of citizens for fighting terrorism or the economic surveillance of private data or online behaviour by Internet companies (Facebook, Google, etc.) for accumulating capital with the help of targeted advertising. Neutral concepts might therefore be used for legitimatizing coercive forms of surveillance by arguing that surveillance is ubiquitous and therefore unproblematic.

3. Difference between information gathering and surveillance: If surveillance is conceived as systematic information gathering, then no difference can be drawn between surveillance studies and information society studies and between a surveillance society and an information society. Therefore, given these circumstances, there are no grounds for claiming the existence of surveillance studies as discipline or transdiscipline (as argued, for example, by Lyon 2007)

4. The normalization of surveillance: If everything is surveillance, it becomes difficult to criticize coercive surveillance politically.

Given these **drawbacks** of neutral surveillance concepts, I prefer to define surveillance as a negative concept: surveillance is the collection of data on individuals or groups that are used so that **control** and **discipline** of behaviour can be exercised by the threat of being targeted by violence. A negative concept of surveillance allows drawing a **clear distinction** of what is and what is not Internet surveillance. Here are, based on a negative surveillance concept, some examples for Internet surveillance processes (connected to: harm, coercion, violence, power, control, manipulation, domination, disciplinary power, involuntary observation):

• Teachers watching private activities of pupils via webcams at Harriton High School, Pennsylvania.

• The scanning of Internet and phone data by secret services with the help of the Echelon system and the Carnivore software.

• Usage of full body scanners at airports.

• The employment of the DoubleClick advertising system by Internet corporations for collecting data about users' online browsing behaviour and providing them with targeted advertising.

• Assessment of personal images and videos of applicants on Facebook by employers prior to a job interview.

• Watching the watchers: corporate watch systems, filming of the police beating of Rodney King (LA 1992), YouTube video of the police killing of Neda Soltan (Iran 2009). There are other examples of information gathering that are oriented on care, benefits, solidarity, aid and co-operation. I term such processes monitoring. Some examples are:

• Consensual online video sex chat of adults.

• Parents observing their sleeping ill baby with a webcam that is connected to their PC in order to be alarmed when the baby needs their help.

• The voluntary sharing of personal videos and pictures from a trip undertaken with real life friends who participated in the trip by a user.

• A Skype video chat of two friends, who live in different countries and make use of this communication technology for staying in touch.

AT: Preventative Intent

Their definition reflects arbitrary NSA legalism – NSA practice dictates a broader definition

Greene and Rodriguez 14 David Greene is an EFF Senior Staff Attorney, and Katitza Rodriguez is an EEF International Rights Director. "NSA Mass Surveillance Programs - Unnecessary and Disproportionate." Electronic Frontier Foundation. 29 May 2014. https://www.eff.org/deeplinks/2014/05/unnecessary-and-disproportionate-how-nsa-violates-international-human-rights. [Premier]

Much of the expansive NSA surveillance revealed in the past year has been defended by the United States on the basis that the mere collection of communications data, even in troves, is not "surveillance" because a human eye never looks at it. Indeed, under this definition, the NSA also does not surveil a person's data by subjecting it to computerized analysis, again up until the point a human being lays eyes on it. The Principles, reflecting the human right to privacy, defines "surveillance" to include the monitoring, interception, collection, analysis, use, preservation, and retention of, interference with, or access to information that includes, reflects, or arises from or a person's communications in the past, present, or future. States should not be able to **bypass privacy protections** on the **basis of arbitrary definitions**.

Systematic

"Surveillance" must be systematic---one-shot, random recording isn't topical

Stefanick 11 Lorna Stefanick, Associate Professor in the Governance, Law, and Management Program in the Centre for State and Legal Studies at Athabasca University. "Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World." p. 129-130. Alabama University Press. 2011. https://books.google.com/books/about/Controlling_Knowledge.html?id=buJ4Bmk_2MUC. [Premier]

According to the report prepared for the Information Commissioner, surveillance can be thought of as a set of activities that share certain characteristics:

Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance. To break this down:

■ The attention is first *purposeful*; the watching has a point that can be justified, in terms of control, entitlement, or some other publicly agreed goal.

■ Then it is *routine*; it happens as we all go about our daily business, it's in the weave of life.

■ But surveillance is also ***systematic***; it is **planned** and carried out according to a **schedule** that is **rational, not merely random**.

■ Lastly, it is *focused*; surveillance gets down to details. While some surveillance depends on aggregate data, much refers to identifiable persons, whose data are collected, stored, transmitted, retrieved, compared, mined and traded." (Emphasis in the original.)

What this means is that **walking through a tourist area videotaping** your **surroundings with your Handycam** video recorder **is not considered surveillance** because it is a **one-off event** that records randomly selected things for your own pleasure. In contrast, a camera installed at a strategic spot along that same street to film the patrons who routinely come out of a local bar intoxicated and proceed to urinate on the street or vandalize local businesses is purposeful (identifying wrongdoers), routine, systematic, and focused. Similarly, a proud parent videotaping his child playing with her nanny in a park on a sunny Sunday afternoon would **not fit the definition** of surveillance. Installing a camera at a daycare to enable parents to view the interaction of their children with their caregivers on demand would be considered surveillance. Many parents insert the so-called "nanny cams" surreptitiously in items like teddy bears to ensure that their children are taken care of in a manner that they find appropriate. Instances of abuse caught by this surveillance have been posted to the Internet, creating predictable rage among those viewing the videos — an example of how panopticon surveillance can become synopticon surveillance. While the latter brings with it its own set of problems, it gives hope to those who fear that surveillance will result in the top-down surveillance described by George Orwell.

End

Total

To "end" surveillance means that surveillance cannot continue to exist.

Nebraska Court of Appeals 17 Nebraska Court of Appeals Advance Sheets 24 Nebraska Appellate Reports NORTHEAST NEB. PUB. POWER DIST. v. NEBRASKA PUB. POWER DIST. Cite as 24 Neb. App. 837. 27 June 2017. https://www.nebraska.gov/apps-courts-epub/public/viewAdvanced?docId=N00005437PUB. [Premier]

Affording the plain and ordinary meaning as an ordinary or reasonable person would understand it, the phrase "(ii) one year prior to the ending date of a previous reduction, whichever is later," we find that there is no "ending date of a previous reduction." Northeast provided notice of continuous, cumulative, and maximum reductions of 30 percent annually to the maximum reduction level of 90 percent of its monthly base demand and obligation under the WPC. The district court found: "The ending of previous reduction **cannot mean** that the reduction continues to exist. To 'end' means to terminate; a cessation; a point beyond which something does not continue, or which **ceases to exist**." We agree with the district court's conclusion given the context of this contract that the ordinary meaning of the term "ending date" is the date on which a previous reduction ends. Here, the proposed reductions will not end. They will each remain in place through the duration of the contract's term, which expires on January 1, 2022. The original 30-percent reduction that begins in 2018 will remain in place during 2019. Each additional reduction will be capped at 30 percent, and the total will be capped at 90 percent per the reduction provision. Since there was no "ending date of a previous reduction," subsection (ii) does no come into effect, and thus subsection (i) was applicable for every notice. However, the notice requirement of the contract capped each years' subsequent reduction to a 30-percent total, and at 90 percent from January 1, 2020, until the expiration of the WPC. Upon our review, we find that the district court did not err in its interpretation of the contract provisions and, therefore, did not err in granting summary judgment in favor of Northeast.

Framing

Extinction 1st

Extinction outweighs and turns structural violence

Matheny 7 Jason, Department of Health Policy and Management, Bloomberg School of Public Health. "Reducing the Risk of Human Extinction." Risk Analysis, Vol 27, No 5. 2007. [Premier]

We may be poorly equipped to recognize or plan for extinction risks (Yudkowsky, 2007). We may not be good at grasping the significance of very large numbers (catastrophic outcomes) or very small numbers (probabilities) over large timeframes. We struggle with estimating the probabilities of rare or unprecedented events (Kunreuther et al., 2001). Policymakers may not plan far beyond current political administrations and rarely do risk assessments value **the existence of future generations**.18 We may **unjustifiably** discount the value of future lives. Finally, extinction risks are market failures where an individual enjoys no perceptible benefit from his or her investment in risk reduction. Human survival may thus be a good requiring deliberate policies to protect. It might be feared that consideration of extinction risks would lead to a reductio ad absurdum: we ought to invest all our resources in asteroid defense or nuclear disarmament, instead of AIDS, pollution, world hunger, or other problems we face today. On the contrary, programs that create a healthy and content global population are likely to **reduce the probability** of global war or catastrophic terrorism. They should thus be seen as an **essential part** of a portfolio of risk-reducing projects. Discussing the risks of "nuclear winter," Carl Sagan (1983) wrote: Some have argued that the difference between the deaths of several hundred million people in a nuclear war (as has been thought until recently to be a reasonable upper limit) and the death of every person on Earth (as now seems possible) is only a matter of one order of magnitude. For me, the difference is considerably greater. Restricting our attention only to those who die as a consequence of the war conceals its full impact. If we are required to calibrate extinction in numerical terms, I would be sure to include the number of people in future generations who would not be born. A nuclear war **imperils all of our descendants,** for as long as there will be humans. Even if the population remains static, with an average lifetime of the order of 100 years, over a typical time period for the biological evolution of a successful species (roughly ten million years), we are talking about some **500 trillion** people yet to come. By this criterion, the stakes are one million times greater for extinction than for the more modest nuclear wars that kill "only" hundreds of millions of people. There are many other possible measures of the potential loss—including culture and science, the evolutionary history of the planet, and the significance of the lives of all of our ancestors who contributed to the future of their descendants. Extinction is the undoing of the human enterprise. In a similar vein, the philosopher Derek Parfit (1984) wrote: I believe that if we destroy mankind, as we now can, this outcome will be much worse than most people think. Compare three outcomes: 1. Peace 2. A nuclear war that kills 99% of the world's existing population 3. A nuclear war that kills 100% 2 would be worse than 1, and 3 would be worse than 2. Which is the greater of these two differences? Most people believe that the greater difference is between 1 and 2. I believe that the difference between 2 and 3 is very much greater . . . . The Earth will remain habitable for at least another billion years. Civilization began only a few thousand years ago. If we do not destroy mankind, these thousand years may be only a tiny fraction of the whole of civilized human history. The difference between 2 and 3 may thus be the difference between this tiny fraction and all of the rest of this history. If we compare this possible history to a day, what has occurred so far is only a fraction of a second. Human extinction in the next few centuries could reduce the number of future generations by thousands or more. We take extraordinary measures to protect some endangered species from extinction. It might be reasonable to take extraordinary measures to protect humanity from the same.19 To decide whether this is so requires more discussion of the methodological problems mentioned here, as well as research on the extinction risks we face and the costs of mitigating them.20

Err neg – scope neglect means you tend to ignore our impacts as extra 0's on the screen.

Bostrom and Cirkovic 08 Nick Bostrom is a Swedish-born philosopher at the University of Oxford known for his work on existential risk, the anthropic principle, human enhancement ethics, superintelligence risks, and the reversal test, Milan Ćirković is Senior Research Associate at the Astronomical Observatory of Belgrade and Assistant Professor of the Department of Physics at the University of Novi Sad in Serbia and Montenegro. "Global Catastrophic Risks." Oxford

University Press. 2008.
https://books.google.com/books/about/Global_Catastrophic_Risks.html?id=X5jdMyJKNL4C. [Premier]

5.9 Scope neglect Migrating birds (2000/20,000/200,000) die each year by d rowning in uncovered oil ponds, which the birds mistake for water bodies . These deaths could be prevented by covering the oil ponds with nets. How m uch money would you be willing to pay to provide the needed nets? Three groups of subjects considered three versions of the above question, asking them how high a tax increase they would accept to save 2,000, 20,000, or 200,000 birds. The response - known as Stated Willingness-to-Pay (SWTP) - had a mean of $80 for the 2000-bird group, $78 for 20,000 birds, and $88 for 200,000 birds (Desvousges et al., 1993). This phenomenon is known as scope insensitivity or scope neglect. Similar studies have shown that Toronto residents would a pay little more to clean up all polluted lakes in Ontario than polluted lakes in a particular region of Ontario (Kahneman, 1986); and that residents of four western US states would pay only 28% more to protect all fifty-seven wilderness areas in those states than to protect a single area (McFadden and Leonard, 1995). The most widely accepted explanation for scope neglect appeals to the affect heuristic. Kahneman et al. (1999, pp. 212-213) write: The story constructed by Desvouges et al. probably evokes for many readers a mental representation of a prototypical incident, perhaps an image of an exhausted bird, its feathers soaked in black oil, unable to escape. The hypothesis of valuation by prototype asserts that the affective value of this image will dominate expressions of the attitude to the problem - including the willingness to pay for a solution. Valuation by prototype implies extension neglect. Two other hypotheses accounting for scope neglect include purchase of moral satisfaction (Kahneman and Knetsch, 1992) and good cause dump (Harrison, 1992) . 'Purchase of moral satisfaction' suggests that people spend enough money to create a 'warm glow' in themselves, and the amount required is a property of the person's psychology, having nothing to do with birds. 'Good cause dump' suggests that people have some amount of money they are willing to pay for 'the environment', and any question about environmental goods elicits this amount. Scope neglect has been shown to apply to human lives. Carson and Mitchell (1995) report that increasing the alleged risk associated with chlorinated drinking water from 0.004 to 2.43 annual deaths per 1000 (a factor of 600) increased stated willingness to pay from $3.78 to $15.23 (a factor of four) . Baron and Greene (1996) found no effect from varying lives saved by a factor of ten. Fetherstonhaugh et al. (1997), in a paper titled 'Insensitivity to the value of human life: a study of psychophysical numbing', found evidence that our perception of human deaths, and valuation of human lives, obeys Weber's Law - meaning that we use a logarithmic scale. And indeed, studies of scope neglect in which the quantitative variations are huge enough to elicit any sensitivity at all, show small linear increases in Willingness-toPay corresponding to exponential increases in scope. Kahneman et al. (1999) interpret this as an additive effect of scope affect and prototype affect - the prototype image elicits most of the emotion, and the scope elicits a smaller amount of emotion which is added (not multiplied) with the first amount. Albert Szent-Gyorgyi, famous Hungarian physiologist and the discoverer of vitamin C, said: 'I am deeply moved if I see one man suffering and would risk my life for him. Then I talk impersonally about the possible pulverization of our big cities, with a hundred million dead. I am unable to multiply one man's suffering by a 100 million.' Human emotions take place within an analogous brain. The human brain cannot release enough neurotransmitters to feel emotion a 1000 times as strong as the grief of one funeral. A prospective risk going from 10,000,000 deaths to 100,000,000 deaths does not multiply by ten the strength of our determination to stop it. It adds one more zero on paper for our eyes to glaze over, an effect so small that one must usually jump several orders of magnitude to detect the difference experimentally

Util Bad

Utilitarianism destroys the sanctity of life and justifies moral atrocities.

Holt 95 Jim Holt is an American philosopher, author and essayist. “Morality, Reduced To Arithmetic.” The New York Times. 5 August 1995. https://www.nytimes.com/1995/08/05/opinion/morality-reduced-to-arithmetic.html. [Premier]

Can the deliberate massacre of innocent people ever be condoned? The atomic bombs dropped on Hiroshima and Nagasaki on Aug. 6 and 9, 1945, resulted in the deaths of 120,000 to 250,000 Japanese by incineration and radiation poisoning. Although a small fraction of the victims were soldiers, the great majority were noncombatants -- women, children, the aged. Among the justifications that have been put forward for President Harry Truman’s decision to use the bomb, only one is worth taking seriously -- that it saved lives. The alternative, the reasoning goes, was to launch an invasion. Truman claimed in his memoirs that this would have cost another half a million American lives. Winston Churchill put the figure at a million. Revisionist historians have cast doubt on such numbers. Wartime documents suggest that military planners expected around 50,000 American combat deaths in an invasion. Still, when Japanese casualties, military and civilian, are taken into account, the overall invasion death toll on both sides would surely have ended up surpassing that from Hiroshima and Nagasaki. Scholars will continue to argue over whether there were other, less catastrophic ways to force Tokyo to surrender. But given the fierce obstinacy of the Japanese militarists, Truman and his advisers had some grounds for believing that nothing short of a full-scale invasion or the annihilation of a big city with an apocalyptic new weapon would have succeeded. Suppose they were right. Would this prospect have justified the intentional mass killing of the people of Hiroshima and Nagasaki? In the debate over the question, participants on both sides have been playing the numbers game. Estimate the hypothetical number of lives saved by the bombings, then add up the actual lives lost. If the first number exceeds the second, then Truman did the right thing; if the reverse, it was wrong to have dropped the bombs. That is one approach to the matter -- the utilitarian approach. According to utilitarianism, a form of moral reasoning that arose in the 19th century, the goodness or evil of an action is determined solely by its consequences. If somehow you can save 10 lives by boiling a baby, go ahead and **boil that baby**. There is, however, an older ethical tradition, one rooted in Judeo-Christian theology, that takes a quite different view. The gist of it is expressed by St. Paul’s condemnation of those who say, “Let us do evil, that good may come.” Some actions, this tradition holds, can never be justified by their consequences; they are absolutely forbidden. It is always wrong to boil a baby even if lives are saved thereby. Applying this absolutist morality to war can be tricky. When enemy soldiers are trying to enslave or kill us, the principle of self-defense permits us to kill them (though not to slaughter them once they are taken prisoner). But what of those who back them? During World War II, propagandists made much of the “indivisibility” of modern warfare: the idea was that since the enemy nation’s entire economic and social strength was deployed behind its military forces, the whole population was a legitimate target for obliteration. “There are no civilians in Japan,” declared an intelligence officer of the Fifth Air Force shortly before the Hiroshima bombing, a time when the Japanese were popularly depicted as vermin worthy of extermination. The boundary between combatant and noncombatant can be fuzzy, but the distinction is not meaningless, as the case of small children makes clear. Yet is wartime killing of those who are not trying to harm us always tantamount to murder? When naval dockyards, munitions factories and supply lines are bombed, civilian carnage is inevitable. The absolutist moral tradition acknowledges this by a principle known as double effect: although it is always wrong to kill innocents deliberately, it is sometimes permissible to attack a military target knowing some noncombatants will die as a side effect. The doctrine of double effect might even justify bombing a hospital where Hitler is lying ill. It does not, however, apply to Hiroshima and Nagasaki. Transformed into hostages by the technology of aerial bombardment, the people of those cities were intentionally executed en masse to send a message of terror to the rulers of Japan. The practice of ordering the massacre of civilians to bring the enemy to heel scarcely began with Truman. Nor did the bomb result in casualties of a new order of magnitude. The earlier bombing of Tokyo by incendiary weapons killed some 100,000 people. What Hiroshima and Nagasaki did mark, by the unprecedented need for rationalization they presented, was the triumph of utilitarian thinking in the conduct of war. The conventional code of noncombatant immunity -- a product of several centuries of ethical progress among nations, which had been formalized by an international commission in the 1920’s in the Hague -- was swept away. A simpler axiom took its place: since war is hell, any means necessary may be used to end, in Churchill’s words, “the vast indefinite butchery.” It is a moral calculus that, for all its logical consistency, **offends** our deep-seated intuitions about **the sanctity of life** -- our conviction that a person is always to be treated as an end, never as a means. Left up to the warmakers, moreover, utilitarian calculations are susceptible to bad-faith reasoning: **tinker with the numbers enough and virtually any atrocity can be excused** in the national interest. In January, the world commemorated the 50th anniversary of the liberation of Auschwitz, where mass slaughter was committed as an end in itself -- the ultimate evil. The moral nature of Hiroshima is ambiguous by contrast. Yet in the postwar era, when governments do not hesitate to treat the massacre of civilians as just another strategic option, the bomb’s sinister legacy is plain: it has inured us to the idea of reducing innocents to instruments and morality to arithmetic.

Util Good

Consequentialism is necessary because complicity is just as bad as active harm.

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. "Ends, Means, and Politics," *Dissent*, Volume 49, Issue 2. Spring 2002. [Premier]

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**.

The value of privacy depends on the context—don't buy into their universal absolutes arguments.

Solove 7 Daniel Solove, an Associate Professor at George Washington University Law School and holds a J.D. from Yale Law. ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy." 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565. [Premier]

Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against. Thus, to understand privacy, we must conceptualize it and its value more pluralistically. Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting against each problem, and that value differs depending upon the nature of each problem.

Deontological absolutes create bad conceptions of privacy. They destroy our ability to truly advance privacy

Solove 2 Daniel Solove is an Associate Professor at George Washington University Law School and holds a J.D. from Yale Law School. "Conceptualizing Privacy." 2002. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103. [Premier]

Why should scholars and judges adopt my approach to conceptualizing privacy? To deal with the myriad of problems involving privacy, scholars and judges will have to adopt multiple conceptions of privacy, or else the old conceptions will lead them astray in finding solutions. The Court's 1928 decision in Olmstead v. United States345 epitomizes the need for flexibility in conceptualizing privacy. The Court held that the wiretapping of a person's home telephone (done outside a person's house) did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person's home.346 Justice Louis Brandeis vigorously dissented, chastising the Court for failing to adapt the Constitution to new problems: "[I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be."347 The Olmstead Court had clung to the outmoded view that the privacy protected by the Fourth Amendment was merely freedom from physical incursions. As a result, for nearly forty years, the Fourth Amendment failed to apply to wiretapping, one of the most significant threats to privacy in the twentieth century.348 Finally, in 1967, the Court swept away this view in Katz v. United States,349 holding that the Fourth Amendment did apply to wiretapping. These events underscore the wisdom of Brandeis's observations in Olmstead—the landscape of privacy is constantly changing, for it is shaped by the rapid pace of technological invention, and therefore, the law must maintain great flexibility in conceptualizing privacy problems. This flexibility is impeded by the use of an overarching conception of privacy. Trying to solve all privacy problems with a uniform and overarching conception of privacy is akin to using a hammer not only to insert a nail into the wall but also to drill a hole. Much of the law of information privacy was shaped to deal with particular privacy problems in mind. The law has often failed to adapt to deal with the variety of privacy problems we are encountering today. Instead, the law has attempted to adhere to overarching conceptions of privacy that do not work for all privacy problems. Not all privacy problems are the same, and different conceptions of privacy work best in different contexts. Instead of trying to fit new problems into old conceptions, we should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption? How does this disruption affect society and social structure? These are some of the questions that should be asked when grappling with privacy problems. In the remainder of this section, I will discuss several examples that illustrate these points.

Privacy 1st

Security risks only *may* cause violence - surveillance *definitely* does. Privacy is paramount for dignity and protecting our unique individuality.

Schneier 06 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. "The Eternal Value of Privacy." WIRED. 18 May 2006. http://www.wired.com/news/columns/1,70886-0.html. [Premier]

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.

Security 1st

The right to security must trump the right to privacy.

Himma 07 KENNETH EINAR. "Privacy Versus Security: Why Privacy is Not an Absolute Value or Right." *San Diego Law Review*. 2007 http://poseidon01.ssrn.com/delivery.php?ID=946099113093066103077074112016017090015022028045089092075001073099001099109106114127011017012000106100015114101076020123093078010050012092072093113078096021081008038034055090107126078091116028103066027088072124015085097094100087114086001099009078&EXT=pdf&TYPE=2. [Premier]

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.

Affirmative

Privacy

Link – Constitutionality

NSA seizures are inconsistent with democracy and the constitution.

Barnett 15 Randy Barnett, Carmack Waterhouse Professor of Legal Theory, Georgetown University Law Center. Director, Georgetown Center for the Constitution. "Why the NSA Data Seizures Are Unconstitutional." Harvard Journal of Law and Public Policy. 2015. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2671&context=facpub. [Premier]

Let me conclude by noting that, without the recent leaks, the American public would have no idea of the existence of these programs, and it still cannot be certain of their scope.72 Every day seems to bring new revelations about domestic surveillance by federal agencies. The secrecy of these surveillance programs is **inconsistent with a republican form of government** in which the citizens are the principals or masters, and those in government their agents or servants. For the people to control their servants, they must know what their servants are doing.

Moreover, until these two district courts found—over the government's objections—that citizens had standing to challenge the constitutionality of the bulk-data seizure programs, 73 their constitutionality had been assessed solely in secret by the FISC that Congress established to scrutinize the issuance of particular business record subpoenas and warrants.74

The secrecy of these programs, and the proceedings by which their constitutionality is being assessed, make it impossible to hold elected officials and appointed bureaucrats accountable. Internal governmental checks, and even secret congressional oversight, are no substitute for the sovereign people being the ultimate judge of their servants' conduct in office. But such judgment and control is impossible without the information that secret programs conceal.

If these blanket seizures of privately-held data are upheld as constitutional, it would constitute an unprecedented legal and constitutional sea change. It is not a policy that should emerge from an advisory panel of judges to which the people are not privy. The American people are no longer the subjects of King George and his general warrants. Nor should we be subjected to these modern-day general warrants by those who are supposed to be our servants, not our masters.

Link – Erosion

Indiscriminate wide-scale NSA Surveillance erodes privacy rights and violates the constitution.

Sinha 14 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. "With Liberty to Monitor All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy." Human Rights Watch. July 2014. http://www.hrw.org/node/127364. [Premier]

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.

These privacy violations are more dangerous than any risk of terrorism, which is magnified by the fact that surveillance fails to prevent attacks.

Schneier 14 Bruce Schneier, 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. "Essays: How the NSA Threatens National Security." Schneier On Security. 6 January 2014. https://www.schneier.com/essays/archives/2014/01/how_the_nsa_threaten.html. [Premier]

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.

Impact – Intrinsic Good

Privacy outweighs is an intrinsic good – you should reject attempts to "weigh" utilitarian impacts against the right because those calculations are shaped by differences in power.

Solove 07 Daniel Solove is an Associate Professor at George Washington University Law School and holds a J.D. from Yale Law School. ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy." San Diego Law Review, Vol. 44. 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565. [Premier]

It is time to return to the **nothing to hide argument**. The reasoning of this argument is that when it comes to government surveillance or use of personal data, there is no privacy violation if a person has nothing sensitive, embarrassing, or illegal to conceal. Criminals involved in illicit activities have something to fear, but for the vast majority of people, their activities are not illegal or embarrassing. Understanding privacy as I have set forth reveals the flaw of the nothing to hide argument at its roots. Many commentators who respond to the argument attempt a direct refutation by trying to point to things that people would want to hide. But the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not want to hide. As Bruce Schneier aptly notes, the nothing to hide argument stems from a faulty "premise that privacy is about hiding a wrong."75 The deeper problem with the nothing to hide argument is that it myopically views privacy as a form of concealment or secrecy. But understanding privacy as a plurality of related problems demonstrates that concealment of bad things is just one among many problems caused by government programs such as the NSA surveillance and data mining. In the categories in my taxonomy, several problems are implicated. The NSA programs involve problems of information collection, specifically the category of surveillance in the taxonomy. Wiretapping involves audio surveillance of people's conversations. Data mining often begins with the collection of personal information, usually from various third parties that possess people's data. Under current Supreme Court Fourth Amendment jurisprudence, when the government gathers data from third parties, there is no Fourth Amendment protection because people lack a "reasonable expectation of privacy" in information exposed to others.76 In United States v. Miller, the Supreme Court concluded that there is no reasonable expectation of privacy in bank records because "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."77 In Smith v. Maryland, the Supreme Court held that people lack a reasonable expectation of privacy in the phone numbers they dial because they "know that they must convey numerical information to the phone company," and therefore they cannot "harbor any general expectation that the numbers they dial will remain secret."78 As I have argued extensively elsewhere, the lack of Fourth Amendment protection of third party records results in the government's ability to access an extensive amount of personal information with minimal limitation or oversight.79 Many scholars have referred to information collection as a form of surveillance. Dataveillance, a term coined by Roger Clarke, refers to the "systemic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."80 Christopher Slobogin has referred to the gathering of personal information in business records as "transaction surveillance."81 Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy.82 Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity. The nothing to hide argument focuses primarily on the information collection problems associated with the NSA programs. It contends that limited surveillance of lawful activity will not chill behavior sufficiently to outweigh the security benefits. One can certainly quarrel with this argument, but one of the difficulties with chilling effects is that it is often very hard to demonstrate concrete evidence of deterred behavior.83 Whether the NSA's surveillance and collection of telephone records has deterred people from communicating particular ideas would be a difficult question to answer. Far too often, discussions of the NSA surveillance and data mining define the problem solely in terms of surveillance. To return to my discussion of metaphor, the problems are not just Orwellian, but Kafkaesque. The NSA programs are problematic even if no information people want to hide is uncovered. In The Trial, the problem is not inhibited behavior, but rather **a suffocating powerlessness and vulnerability** created by the court system's use of personal data and its exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability. One such harm, for example, which I call aggregation, emerges from the combination of small bits of seemingly innocuous data.84 When combined, the information becomes much more telling about a person. For the person who truly has nothing to hide, aggregation is not much of a problem. But in the stronger, less absolutist form of the nothing to hide argument, people argue that certain pieces of information are not something they would hide. Aggregation, however, means that by combining pieces of information we might not care to conceal, the government can glean information about us that we might really want to conceal. Part of the allure of data mining for the government is

its ability to reveal a lot about our personalities and activities by sophisticated means of analyzing data. Therefore, without greater transparency in data mining, it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed. Moreover, data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity. Another problem in the taxonomy, which is implicated by the NSA program, is the problem I refer to as exclusion.85 Exclusion is the problem caused when people are prevented from having knowledge about how their information is being used, as well as barred from being able to access and correct errors in that data. The NSA program involves a massive database of information that individuals cannot access. Indeed, the very existence of the program was kept secret for years.86 This kind of information processing, which forbids people's knowledge or involvement, resembles in some ways a kind of due process problem. It is a structural problem involving the way people are treated by government institutions. Moreover, it creates a power imbalance between individuals and the government. To what extent should the Executive Branch and an agency such as the NSA, which is relatively insulated from the political process and public accountability, have a significant power over citizens? This issue is not about whether the information gathered is something people want to hide, but rather about the power and the structure of government. A related problem involves "secondary use." Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent. The Administration has said little about how long the data will be stored, how it will be used, and what it could be used for in the future. The potential future uses of any piece of personal information are vast, and without limits or accountability on how that information is used, it is hard for people to assess the dangers of the data being in the government's control. Therefore, the problem with the nothing to hide argument is that it focuses on just one or two particular kinds of privacy problems—the disclosure of personal information or surveillance—and not others. It assumes a particular view about what privacy entails, and it sets the terms for debate in a manner that is often unproductive. It is important to distinguish here between two ways of justifying a program such as the **NSA surveillance** and data mining program. The first way is to not recognize a problem. This is how the nothing to hide argument works—it denies even the existence of a problem. The second manner of justifying such a program is to acknowledge the problems but contend that the **benefits** of the NSA program **outweigh the privacy harms.** The first justification influences the second, because the low value given to privacy is based upon a narrow view of the problem. The key misunderstanding is that the nothing to hide argument views privacy in a particular way—as a form of secrecy, **as the right to hide things.** But there are many other types of harm involved beyond exposing one's secrets to the government. Privacy problems are often difficult to recognize and redress because they create a panoply of types of harm. Courts, legislators, and others look for particular types of harm to the exclusion of others, and their narrow focus blinds them to seeing other kinds of harms. One of the difficulties with the nothing to hide argument is that it looks **for a visceral kind of injury** as opposed to **a structural one.** Ironically, this underlying conception of injury is shared by both those advocating for greater privacy protections and those arguing in favor of the conflicting interests to privacy. For example, law professor Ann Bartow argues that I have failed to describe privacy harms in a compelling manner in my article, A Taxonomy of Privacy, where I provide a framework for understanding the manifold different privacy problems.87 Bartow's primary complaint is that my taxonomy "frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease."88 Bartow claims that the taxonomy **does not have "enough 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 categories of tort law. Most privacy problems lack dead bodies. Of course, there are exceptional cases such as the murders of Rebecca Shaeffer and Amy Boyer. Rebecca Shaeffer was an actress killed when a stalker obtained her address from a Department of Motor Vehicles record.90 This incident prompted Congress to pass the Driver's Privacy Protection Act of 1994.91 Amy Boyer was murdered by a stalker who obtained her personal information, including her work address and Social Security number, from a database company.92 These examples aside, there is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized. Horrific cases are not typical, and the purpose of my taxonomy is to explain why most privacy problems are still harmful despite this fact. Bartow's objection is actually very similar to the nothing to hide argument. Those advancing the nothing to hide argument have in mind a particular kind of visceral privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Bartow's **quest for horror stories** represents a similar desire to find visceral privacy harms. The problem is that not all privacy harms are like this. At the end of the day, privacy is not a horror movie, and demanding more palpable harms will be difficult in many cases. Yet there is still a harm worth addressing, **even if it is not sensationalistic.** In many instances, privacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up. In this way, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Bartow wants to point to a major spill, but gradual pollution by a multitude of different actors often creates worse problems. The law frequently struggles with recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury.93 For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies. The federal agencies used the data to study airline security.94 A group of passengers sued Northwest Airlines for disclosing their personal information. One of their claims was that Northwest Airlines breached its contract with the passengers. In Dyer v. Northwest Airlines Corp., the court rejected the contract claim because "broad statements of company policy do not generally give rise to contract claims," the passengers never claimed they relied upon the policy or even read it, and they "failed to allege any contractual damages arising out of the alleged breach."95 Another court reached a similar conclusion.96 Regardless of the merits of the decisions on contract law, the cases represent a difficulty with the legal system in addressing privacy problems. The disclosure of the passenger records represented a "breach of confidentiality."97 The problems caused by breaches of confidentiality do not merely consist of individual emotional distress; they involve a violation of trust within a relationship. There is a strong social value in ensuring that promises are kept and that trust is maintained in relationships between businesses and their customers. The problem of secondary use is also

implicated in this case.98 Secondary use involves data collected for one purpose being used for an unrelated purpose without people's consent. The airlines gave passenger information to the government for an entirely different purpose beyond that for which it was originally gathered. Secondary use problems often do not cause financial, or even psychological, injuries. Instead, the harm is one of power imbalance. In Dyer, data was disseminated in a way that ignored airline passengers' interests in the data despite promises made in the privacy policy. Even if the passengers were unaware of the policy, there is a social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data. Such a state of affairs can leave nearly all consumers in a powerless position. The harm, then, is less one to particular individuals than it is a structural harm. A similar problem surfaces in another case, Smith v. Chase Manhattan Bank.99 A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that the information would remain confidential. The court held that even presuming these allegations were true, the plaintiffs could not prove any actual injury: [T]he "harm" at the heart of this purported class action, is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm. The complaint does not allege any single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail.100 The court's view of harm, however, did not account for the breach of confidentiality. When balancing privacy against security, the privacy harms are often characterized in terms of injuries to the individual, and the interest in security is often characterized in a more broad societal way. The security interest in the NSA programs has often been defined improperly. In a Congressional hearing, Attorney General Alberto Gonzales stated: Our enemy is listening, and I cannot help but wonder if they are not shaking their heads in amazement at the thought that anyone would imperil such a sensitive program by leaking its existence in the first place, and smiling at the prospect that we might now disclose even more or perhaps even unilaterally disarm ourselves of a key tool in the war on terror.101 The balance between privacy and security is often cast in terms of whether a particular government information collection activity should or should not be barred. The issue, however, often is not whether the NSA or other government agencies should be allowed to engage in particular forms of information gathering; rather, it is what kinds of oversight and accountability we want in place when the government engages in searches and seizures. The government can employ nearly any kind of investigatory activity with a warrant supported by probable cause. This is a mechanism of oversight—it forces government officials to justify their suspicions to a neutral judge or magistrate before engaging in the tactic. For example, electronic surveillance law allows for wiretapping, but limits the practice with judicial supervision, procedures to minimize the breadth of the wiretapping, and requirements that the law enforcement officials report back to the court to prevent abuses.102 It is these procedures that the Bush Administration has ignored by engaging in the warrantless NSA surveillance. The question is not whether we want the government to monitor such conversations, but whether the Executive Branch should adhere to the appropriate oversight procedures that Congress has enacted into law, or should covertly ignore any oversight. Therefore, the security interest should not get weighed in its totality against the privacy interest. Rather, what should get weighed is the extent of marginal limitation on the effectiveness of a government information gathering or data mining program by imposing judicial oversight and minimization procedures. Only in cases where such procedures will completely impair the government program should the security interest be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one. Far too often, the balancing of privacy interests against security interests takes place in a manner that severely shortchanges the privacy interest while **inflating the security interests**. Such is the logic of the nothing to hide argument. When the argument is unpacked, **and its underlying assumptions examined** and challenged, we can see how it **shifts the debate to its terms**, in which it draws power from its unfair advantage. It is time to pull the curtain on the nothing to hide argument. Whether explicit or not, conceptions of privacy underpin nearly every argument made about privacy, even the common quip "I've got nothing to hide." As I have sought to demonstrate in this essay, understanding privacy as a pluralistic conception reveals that we are often talking past each other when discussing privacy issues. By focusing more specifically on the related problems under the rubric of "privacy," we can better address each problem rather than ignore or conflate them. 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 in government surveillance** and data mining programs. When engaged with 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.

Freedom and dignity are ethically prior to security.

Cohen 14 Elliot D. Ph.D., ethicist and political analyst, editor in chief of the International Journal of Applied Philosophy. "Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance." 2014. https://link.springer.com/book/10.1057/9781137408211. [Premier]

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.

Impact – Constitutionality

The Constitution comes before any impact to be "weighed."

Smith 14 Peter J. Smith IV, attorney for the law firm LUKINS & ANNIS and Lead Council for This brief was was signed by the entire legal team. "APPELLANT'S REPLY BRIEF in the matter of Smith v. Obama – before the United States Ninth Circuit Court of Appeals." Electronic Frontier Foundation. 16 October 2014. https://www.eff.org/document/smiths-reply-brief. [Premier]

The government argues that it would be more convenient for law enforcement if the courts established a bright-line rule that extinguished all privacy in information shared with others. See Gov't Br. 40. The government is surely right about this. The Bill of Rights exists, however, not to serve governmental efficiency but to safeguard individual liberty. Cf. Bailey v. United States, 133 S. Ct. 1031, 1041 (2013) ("**'[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment**.'" (quoting Mincey v. Arizona, 437 U.S. 385, 393 (1978))); Riley, 134 S. Ct. at 2493 ("Our cases have historically recognized that **the warrant requirement is** 'an important working part of our machinery of government,' **not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.**'" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971))). Notably, the government made the same appeal for a bright-line rule in Jones and Maynard, see, e.g., Brief for the United States at 13, Jones, 132 S. Ct. 945, but the Supreme Court and D.C. Circuit rejected it.

Impact – Slippery Slope

Privacy is a gateway right since it protects 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." Human Rights Watch. 21 January 2014. http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance. [Premier]

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.

Racism

Link – Islamophobia

FISA surveillance is a form of islamophobia.

Lennard 14 Natasha Lennard, author for Vice News also a freelancer for The New York Times's City Blog. "The NSA's Racist Targeting of Individuals Is as Troubling as Indiscriminate Surveillance." Vice. June 9 2014. https://news.vice.com/article/the-nsas-racist-targeting-of-individuals-is-as-troubling-as-indiscriminate-surveillance. [Premier]

Revelations of the National Security Agency's massive surveillance programs have highlighted how millions of ordinary internet and phone users — that is, non-criminal targets — have had their communications data swept up by a vast, indiscriminate dragnet. This has occasioned justifiable outrage, but the reaction has overshadowed discussion of how the NSA targets actual individuals — a process that, it turns out, can be quite **discriminatory.**

As I noted last week, if our national security state's dangerously loose determination of what constitutes an "imminent threat" is any indication, we should be as troubled by the NSA's targeting of particular people as we are by its non-targeted spying. The latest disclosure from The Intercept clearly illustrates why.

According to documents leaked by Edward Snowden, the NSA has been spying on five distinguished Muslim-Americans under a law — the Foreign Intelligence Surveillance Act (FISA) — that is meant to target international terrorists or foreign agents. The inclusion of the email accounts of these five people in a spreadsheet listing the targeted accounts of more than 7,000 others belies the NSA's claim that it's in the business of marking only terrorist suspects.

Here are the agency's suspected "terrorists": Faisal Gill, who was appointed to (and thoroughly vetted by) the Department of Homeland Security under President George W. Bush; Asim Ghafoor, an attorney who has defended clients suspected of terrorism; Hooshang Amirahmadi, an Iranian-American professor of public policy and international development at Rutgers University; Agha Saeed, founder and chairman of the American Muslim Alliance and a former political science professor at California State University; and Nihad Awad, the executive director of the Council on American-Islamic Relations.

This is anti-Muslim discrimination pure and simple. While the NSA's broad data collection is disturbingly total and unspecific, its targeted spying is evidently racist. Another leaked document punctuates this point with a dull, disgusting thud: a 2005 training document explaining how to "properly format internal memos to justify FISA surveillance" offers a sample memo that uses "Mohammed Raghead" as the name of a fictitious terrorism suspect.

Your NSA at work, ladies and gentlemen!

As the existence of this document makes clear, legality is a tortured issue at the heart national security misdeeds. NSA agents are trained to ensure that their surveillance practices fall within the letter of the law — and the law here is at fault, shaped not by a spirit of justice but by surveillance-state paranoia. The Intercept report does not skirt around this point:

Indeed, the government's ability to monitor such high-profile Muslim-Americans — with or without warrants — suggests that the most alarming and invasive aspects of the NSA's surveillance occur not

because the agency breaks the law, but because it is able to exploit the law's permissive contours. "The scandal is what Congress has made legal," says Jameel Jaffer, an ACLU deputy legal director. "The claim that the intelligence agencies are complying with the laws is just a distraction from more urgent questions relating to the breadth of the laws themselves."

This latest Snowden leak adds a new dimension to the troubling stream of NSA revelations, illuminating an even more insidious aspect of the government's surveillance practices. We know that through dragnet data hoarding programs like PRISM we are all always-already potential suspects. We are all watched. But who falls under the NSA microscope? Who gets to be the needles in the haystack, the targeting of which provides the official justification of total surveillance? Who gets to be "Mohammed Raghead"?

Well, that's top-secret government business. Don't worry, though — it's legal.

Warrantless surveillance boosts a distinct form of racial, religious, and ethnic discrimination.

Unegbu 13 Cindy C. Unegbu - J.D. Candidate, Howard University School of Law. "National Security Surveillance on the Basis of Race, Ethnicity, and Religion: A Constitutional Misstep." Howard Law Journal. Fall 2013. https://heinonline.org/HOL/LandingPage?handle=hein.journals/howlj57&div=15&id=&page=. [Premier]

Picture this: you live in a society in which the government is allowed to partake in intrusive surveillance measures without the institutionalized checks and balances upon which the government was founded. In this society, the government pursues citizens who belong to a particular race or ethnicity, practice a certain religion, or have affiliations with specific interest groups. Individuals who have these characteristics are subject to surreptitious monitoring, which includes undercover government officials disguising themselves as community members in order to attend various community events and programs. The government may also place these individuals on watch lists, even where there is no evidence of wrongdoing. These watch lists classify domestic individuals as potential or suspected terrorists and facilitate the monitoring of their personal activity through various law enforcement agencies for an extended period of time. This "hypothetical" society is not hypothetical at all; in fact, **it is the current state of American surveillance.** The government's **domestic** spying activities have progressed to intrusive levels, **primarily due to** an increased **fear of terrorism**. n1 This fear has resulted in governmental intelligence efforts that are focused on political activists, racial and religious minorities, and immigrants. n2 [*435] The government's domestic surveillance efforts are not only geared toward suspected terrorists and those partaking in criminal activity, but reach any innocent, non-criminal, non-terrorist national, all **in the name of national security.** The government's power to engage in suspicionless surveillance and track innocent citizens' sensitive information has been granted through the creation and revision of the National Counterterrorism Center n3 and the FBI's (Federal Bureau of Investigation) Domestic Investigations and Operations Guide. n4 The grant of surveillance power has resulted in many opponents, including those within the current presidential administration, who challenge the order for numerous reasons. n5 These reasons include the inefficiency of storing citizens' random personal information for extended periods of time, n6 the broad unprecedented authority granted to this body of government without proper approval from Congress, n7 and the constitutional violations due to the deprivation of citizens' rights. n8 [*436] This Comment argues that the wide-sweeping surveillance authority granted to the government results in a violation of the Fourteenth Amendment's Equal Protection Clause due to far-reaching domestic monitoring practices. Surveillance practices, such as posing as members of the community and placing individuals on watch lists without suspicion of terrorist activity, result in the impermissible monitoring of individuals on the basis of their **race or ethnicity**. These practices, although done in the name of national security, an established compelling government interest, violate the Equal Protection Clause of the Fourteenth Amendment because they are not narrowly tailored to the stated interest. The procedures are not narrowly tailored to the interest of national security because of the **over-inclusiveness of the measures**.

Warrantless mass surveillance is racist. Vote Aff to prioritize these under-represented impacts in public debates.

Kumar and Kundnani 15 Deepa Kumar is an associate professor of Media Studies and Middle East Studies at Rutgers University, and Arun Kundnani is research fellow at the International Centre for Counter-Terrorism. "Race, surveillance, and empire." International Socialist Review. Issue 96. Spring 2015. http://isreview.org/issue/96/race-surveillance-and-empire. [Premier]

Beginning in June 2013, a series of news articles based on whistle-blower Edward Snowden's collection of documents from the National Security Agency (NSA) took the world by storm. Over the course of a year, the Snowden material provided a detailed account of the **massive extent of NSA's warrantless data collection**. What became clear was that the NSA was involved in the mass collection of online material. Less apparent was how this data was actually used by the NSA and other national security agencies. Part of the answer came in July 2014 when Glenn Greenwald and Murtaza Hussain published an article that identified specific targets of NSA surveillance and showed how individuals were being placed under surveillance despite there being no reasonable suspicion of their involvement in criminal activity.1 **All** of those named as targets were prominent Muslim Americans. The following month, Jeremy Scahill and Ryan Devereaux published another story for The Intercept, which revealed that under the Obama administration the number of people on the National Counterterrorism Center's no-fly list had increased **tenfold** to 47,000. Leaked classified documents showed that the NCC maintains a database of terrorism suspects worldwide—the Terrorist Identities Datamart Environment—which contained a million names by 2013, double the number four years earlier, and increasingly includes biometric data. This database includes 20,800 persons within the United States who are **disproportionately concentrated** in Dearborn, Michigan, with its significant Arab American population.2 By any objective standard, these were major news stories that ought to have attracted as much attention as the earlier revelations. Yet the stories barely registered in the corporate media landscape. The "tech community," which had earlier expressed outrage at the NSA's mass digital surveillance, seemed to be indifferent when details emerged of the targeted surveillance of Muslims. The explanation for this reaction is not hard to find. While many object to the US government collecting private data on "ordinary" people, Muslims tend to be seen as reasonable targets of suspicion. A July 2014 poll for the Arab American Institute found that 42 percent of Americans think it is justifiable for law enforcement agencies to profile Arab Americans or American Muslims.3 In what follows, we argue that the **debate** on national security surveillance that has emerged in the United States since the summer of 2013 is woefully inadequate, due to its failure to place questions of race and empire at the center of its analysis. It is racist ideas that form the basis for the ways national security surveillance is organized and deployed, racist fears that are whipped up to legitimize this surveillance to the American public, and the disproportionately targeted racialized groups that have been most effective in making sense of it and organizing opposition. This is as true today as it has been historically: race and state surveillance are intertwined in the history of US capitalism. Likewise, we argue that the history of national security surveillance in the United States is inseparable from the history of US colonialism and empire.

Link – Antiblackness

NSA surveillance is racist towards African Americans – warrants aren't required for unreasonable search and seizure.

Cyril 15 Malika Amala Cyril, founder and executive director of the Center for Media Justice (CMJ) and co-founder of the Media Action Grassroots Network, a national network of 175 organizations working to ensure media access, rights, and representation for marginalized communities. "Black America's State of Surveillance." Progressive. 30 March 2015. http://www.progressive.org/news/2015/03/188074/black-americas-state-surveillance. [Premier]

My mother was not the only black person to come under the watchful eye of American law enforcement for perceived and actual dissidence. Nor is dissidence always a requirement for being subject to spying. Files obtained during a break-in at an FBI office in 1971 revealed that African Americans, J. Edger Hoover's largest target group, didn't have to be perceived as dissident to warrant surveillance. They just had to be black. As I write this, the same philosophy is driving the increasing adoption and use of surveillance technologies by local law enforcement agencies across the United States.

Today, media reporting on government surveillance is laser-focused on the revelations by Edward Snowden that millions of Americans were being spied on by the NSA. Yet my mother's visit from the FBI reminds me that, from the slave pass system to laws that deputized white civilians as enforcers of Jim Crow, black people and other people of color have **lived for centuries with surveillance practices** aimed at maintaining a racial hierarchy.

It's time for journalists to tell a new story that does not start the clock when privileged classes learn they are targets of surveillance. We need to understand that data has historically been overused to repress dissidence, monitor perceived criminality, and perpetually maintain an impoverished underclass.

In an era of big data, the Internet has increased the speed and secrecy of data collection. Thanks to new surveillance technologies, law enforcement agencies are now able to collect massive amounts of indiscriminate data. Yet legal protections and policies have not caught up to this technological advance.

Concerned advocates see mass surveillance as the problem and protecting privacy as the goal. Targeted surveillance is an obvious answer—it may be discriminatory, but it helps protect the privacy perceived as an earned privilege of the inherently innocent.

The trouble is, targeted surveillance frequently includes the indiscriminate collection of the private data of people targeted by race but not involved in any crime.

For targeted communities, there is little to no expectation of privacy from government or corporate surveillance.

Instead, we are watched, either as criminals or as consumers. We do not expect policies to protect us. Instead, we've birthed a complex and coded culture—from jazz to spoken dialects—in order to navigate a world in which spying, from AT&T and Walmart to public benefits programs and beat cops on the block, is as much a part of our built environment as the streets covered in our blood.

In a recent address, New York City Police Commissioner Bill Bratton made it clear: "2015 will be one of the most significant years in the history of this organization. It will be the year of technology, in which we literally will give to every member of this department technology that would've been unheard of even a few years ago."

Predictive policing, also known as "Total Information Awareness," is described as using advanced technological tools and data analysis to "preempt" crime. It utilizes trends, patterns, sequences, and affinities found in data to make determinations about when and where crimes will occur.

This model is deceptive, however, because it presumes data inputs to be neutral. They aren't. In a racially discriminatory criminal justice system, surveillance technologies reproduce injustice. Instead of reducing discrimination, predictive policing is a face of what author Michelle Alexander calls the "New Jim Crow"—a de facto system of separate and unequal application of laws, police practices, conviction rates, sentencing terms, and conditions of confinement that operate more as a system of social control by racial hierarchy than as crime prevention or punishment.

In New York City, the predictive policing approach in use is "Broken Windows." This approach to policing places an undue focus on quality of life crimes—like selling loose cigarettes, the kind of offense for which Eric Garner was choked to death. Without oversight, accountability, transparency, or rights, predictive policing is just high-tech racial profiling—indiscriminate data collection that drives discriminatory policing practices.

As local law enforcement agencies increasingly adopt surveillance technologies, they use them in three primary ways: to listen in on specific conversations on and offline; to observe daily movements of individuals and groups; and to observe data trends. Police departments like Bratton's aim to use sophisticated technologies to do all three.

They will use technologies like license plate readers, which the Electronic Frontier Foundation found to be disproportionately used in communities of color and communities in the process of being gentrified.

They will use facial recognition, biometric scanning software, which the FBI has now rolled out as a national system, to be adopted by local police departments for any criminal justice purpose.

They intend to use body and dashboard cameras, which have been touted as an effective step toward accountability based on the results of one study, yet storage and archiving procedures, among many other issues, remain unclear.

They will use Stingray cellphone interceptors. According to the ACLU, Stingray technology is an invasive cellphone surveillance device that mimics cellphone towers and sends out signals to trick cellphones in the area into transmitting their locations and identifying information. When used to track a suspect's cellphone, they also gather information about the phones of countless bystanders who happen to be nearby.

The same is true of domestic drones, which are in increasing use by U.S. law enforcement to conduct routine aerial surveillance. While drones are currently unarmed, drone manufacturers are considering arming these remote-controlled aircraft with weapons like rubber bullets, tasers, and tear gas.

They will use fusion centers. Originally designed to increase interagency collaboration for the purposes of counterterrorism, these have instead become the local arm of the intelligence community. According

to Electronic Frontier Foundation, there are currently seventy-eight on record. They are the clearinghouse for increasingly used "suspicious activity reports"—described as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." These reports and other collected data are often stored in massive databases like e-Verify and Prism. As anybody who's ever dealt with gang databases knows, it's almost impossible to get off a federal or state database, even when the data collected is incorrect or no longer true.

Predictive policing doesn't just lead to racial and religious profiling—it relies on it. Just as stop and frisk legitimized an initial, unwarranted contact between police and people of color, almost 90 percent of whom turn out to be innocent of any crime, suspicious activities reporting and the dragnet approach of fusion centers target communities of color. One review of such reports collected in Los Angeles shows approximately 75 percent were of people of color.

This is the future of policing in America, and it should terrify you as much as it terrifies me. Unfortunately, it probably doesn't, because my life is at far greater risk than the lives of white Americans, especially those reporting on the issue in the media or advocating in the halls of power.

One of the most terrifying aspects of high-tech surveillance is the invisibility of those it disproportionately impacts.

The NSA and FBI have engaged local law enforcement agencies and electronic surveillance technologies to spy on Muslims living in the United States. According to FBI training materials uncovered by Wired in 2011, the bureau taught agents to treat "mainstream" Muslims as supporters of terrorism, to view charitable donations by Muslims as "a funding mechanism for combat," and to view Islam itself as a "Death Star" that must be destroyed if terrorism is to be contained. From New York City to Chicago and beyond, local law enforcement agencies have expanded unlawful and covert racial and religious profiling against Muslims not suspected of any crime. There is no national security reason to profile all Muslims.

At the same time, almost 450,000 migrants are in detention facilities throughout the United States, including survivors of torture, asylum seekers, families with small children, and the elderly. Undocumented migrant communities enjoy few legal protections, and are therefore subject to brutal policing practices, including illegal surveillance practices. According to the Sentencing Project, of the more than 2 million people incarcerated in the United States, more than 60 percent are racial and ethnic minorities.

But by far, **the widest net is cast over black communities.** Black people alone represent 40 percent of those incarcerated. More black men are incarcerated than were held in slavery in 1850, on the eve of the Civil War. Lest some misinterpret that statistic as evidence of greater criminality, a 2012 study confirms that black defendants are at least 30 percent more likely to be imprisoned than whites for the same crime.

This is not a broken system, it is a system working perfectly as intended, to the detriment of all. The NSA could not have spied on millions of cellphones if it were not already spying on black people, Muslims, and migrants.

As surveillance technologies are increasingly adopted and integrated by law enforcement agencies today, racial disparities are being made invisible by a media environment that has failed to tell the story of surveillance in the context of structural racism.

Reporters love to tell the technology story. For some, it's a sexier read. To me, freedom from repression and racism is far sexier than the newest gadget used to reinforce racial hierarchy. As civil rights protections catch up with the technological terrain, reporting needs to catch up, too. Many journalists still focus their reporting on the technological trends and not the racial hierarchies that these trends are enforcing.

Martin Luther King Jr. once said, "Everything we see is a shadow cast by that which we do not see." Journalists have an obligation to tell the stories that are hidden from view.

We are living in an incredible time, when migrant activists have blocked deportation buses, and a movement for black lives has emerged, and when women, queer, and trans experiences have been placed right at the center. The decentralized power of the Internet makes that possible.

But the Internet also makes possible the high-tech surveillance that threatens to drive structural racism in the twenty-first century.

We can help black lives matter by ensuring that technology is not used to cement a racial hierarchy that leaves too many people like me dead or in jail. Our communities need partners, not gatekeepers.

Together, we can change the cultural terrain that makes killing black people routine. We can counter inequality by ensuring that both the technology and the police departments that use it are democratized. We can change the story on surveillance to raise the voices of those who have been left out.

There are no voiceless people, only those that ain't been heard yet. Let's birth a new norm in which the technological tools of the twenty-first century create equity and justice for all—so all bodies enjoy full and equal protection, and the Jim Crow surveillance state exists no more.

Impact – Ethics

Reject this discrimination as an *unacceptable wrong* that *must be rejected* as an end onto itself.

Shamsi et al. 14 Hina Shamsi is a lecturer-in-law at Columbia Law School, where she teaches a course in international human rights. "The Perversity of Profiling." ACLU. 14 April 2014. https://www.aclu.org/blog/perversity-profiling. [Premier]

Using expanded authorities that permit investigations **without** actual **evidence of wrongdoing**, the FBI has also **targeted minority communities** for interviews based on race, ethnicity, national origin, and religion. It has used informants to conduct surveillance in community centers, mosques, and other public gathering places and against people exercising their First Amendment right to worship or to engage in political advocacy. And among America's minority communities, "flying while brown" soon joined "driving while black" as a truism of government-sanctioned discrimination and stigma. It's hard to overstate the damage done to the FBI's relationship with minorities, particularly American Muslims. The damage, however, has spread further. When **federal** law enforcement leads in discriminatory profiling, state and local law enforcement will follow. Nowhere is that clearer than in New York City, where the NYPD – which is twice the size of the FBI – launched a massive program of **discriminatory surveillance** and investigation of American Muslims, mapping the places where they carry out daily activities and sending informants to spy on mosques and Muslim community organizations, student groups, and businesses. After the Associated Press broke a series of stories describing this program in stark and shocking detail, the NYPD defended itself, **arguing that it was only doing what the FBI was permitted to do.** Again, it's hard to overstate the harm. From the ACLU's work with New York's Muslim communities, we know that a generation of youth is growing up fearful of its local police force, scared to exercise the rights to freedom of worship, speech, and association. Fortunately, the issuance of the revised Guidance on Race has been delayed and both the Justice Department and the civil rights community have a crucial opportunity to put a spotlight on the FBI, which vigorously opposes those fighting for equality. According to the New York Times, the FBI's argument seems to be that it needs to identify where Somalis live to investigate potential Somali terrorism suspects. But that argument **must be rejected** for the same reason that **we reject it in other contexts**. Many mass shooters are young white males, yet we rightly don't map where whites live or send informants to majority white communities to ferret out potential mass shooters. Put another way, the FBI's argument presumes what the Ashcroft Guidance "emphatically rejects": that crime can be prevented by the **mass stereotyping** of entire communities. Not only is that **wrong**, it is a ham-handed approach that squanders resources that should properly be devoted to investigating actual wrongdoing.

Defeating racism is a prerequisite to ethics.

Memmi 2k Albert, Professor Emeritus of Sociology @ U of Paris. "Naiteire, Racism." Translated by Steve Martinot, p. 163-165. [Premier]

The struggle against racism will be long, difficult, without intermission, without remission, probably never achieved, yet for this very reason, it is a struggle to be undertaken without surcease and without concessions. One cannot be indulgent toward racism. One cannot even let the monster in the house, especially not in a mask. To give it merely a foothold means to augment the bestial part in us and in other people which is to diminish what is human. To accept the racist universe to the slightest degree is to endorse fear, injustice, and violence. It is to accept the persistence of the dark history in which we still largely live. It is to agree that the outsider will always be a possible victim (and which [person] man is not [themself] himself an outsider relative to someone else?). Racism illustrates in sum, the inevitable

negativity of the condition of the dominated; that is it illuminates in a certain sense the entire human condition. The anti-racist struggle, difficult though it is, and always in question, is nevertheless one of the prologues to the ultimate passage from animality to humanity. In that sense, we cannot fail to rise to the racist challenge. However, it remains true that one's moral conduct only emerges from a choice: one has to want it. It is a choice among other choices, and always debatable in its foundations and its consequences. Let us say, broadly speaking, that the choice to conduct oneself morally is the condition for the establishment of a human order for which racism is the very negation. This is almost a redundancy. One cannot found a moral order, let alone a legislative order, on racism because racism signifies the exclusion of the other and his or her subjection to violence and domination. From an ethical point of view, if one can deploy a little religious language, racism is "the truly capital sin."fn22 It is not an accident that almost all of humanity's spiritual traditions counsel respect for the weak, for orphans, widows, or strangers. It is not just a question of theoretical counsel respect for the weak, for orphans, widows or strangers. It is not just a question of theoretical morality and disinterested commandments. Such unanimity in the safeguarding of the other suggests the real utility of such sentiments. All things considered, we have an interest in banishing injustice, because injustice engenders violence and death. Of course, this is debatable. There are those who think that if one is strong enough, the assault on and oppression of others is permissible. But no one is ever sure of remaining the strongest. One day, perhaps, the roles will be reversed. All unjust society contains within itself the seeds of its own death. It is probably smarter to treat others with respect so that they treat you with respect. "Recall," says the bible, "that you were once a stranger in Egypt," which means both that you ought to respect the stranger because you were a stranger yourself and that you risk becoming once again someday. It is an ethical and a practical appeal – indeed, it is a contract, however implicit it might be. In short, **the refusal of racism is the condition for all theoretical and practical morality**. Because, in the end, the ethical choice commands the political choice. A just society must be a society accepted by all. If this contractual principle is not accepted, then only conflict, violence, and destruction will be our lot. If it is accepted, we can hope someday to live in peace. True, it is a wager, but the stakes are irresistible.

Tech Industry

Link – General

NSA surveillance destroys productivity and growth by undermining ALL tech related industries by destroying confidence in the integrity of data services.

Kehl et al. 14 Danielle Kehl, Kevin Bankston, Robyn Greene & Robert Morgus, analysts at New America's Open Technology Institute. "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity." New America's Open Technology Institute. July 2014 Policy Paper. https://static.newamerica.org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveilance_Costs_Final.pdf. [Premier]

"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. 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 II. Direct Economic Costs to American Companies "Last year's national security leaks have also had a commercial and financial impact on American technology companies that have provided these records. They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global marketplace damaged. -Rep. Bob Goodlatte, Chairman of the House Judiciary Committee " 8 Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity 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 In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014, 25 percent of respondents indicated that they were moving data outside of the U.S. as a result of the NSA revelations. New America's Open Technology Institute 9 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 Frankly I think the government blew it... The government response was, ‘Oh don’t worry, we’re not spying on any Americans.’ Oh, wonderful: that’s really helpful to companies trying to serve people around the world, and that’s really going to inspire confidence in American internet companies.” -Mark Zuckerberg, CEO of Facebook ,, 10 Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity 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 competiveness.58

Link – Cloud Computing

NSA surveillance is crushing U.S. cloud-computing – decks competitiveness and spills over to the entire tech sector

Donohue 18 Lauren, Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law. "High Technology, Consumer Privacy, and U.S. National Security." *Symposium Articles*, American University Business Law Review, 4(1). 2018. https://digitalcommons.wcl.american.edu/aublr/vol4/iss1/3/. [Premier]

I. ECONOMIC IMPACT OF NSA PROGRAMS

The NSA programs, and public awareness of them, have had an immediate and **detrimental impact on the U.S. economy**. They have cost U.S. companies **billions of dollars** in lost sales, even as companies have seen their **market shares decline**. American multinational corporations have had to develop new products and programs to offset the revelations and to build consumer confidence. At the same time, foreign entities have seen revenues increase. Beyond the immediate impact, the revelation of the programs, and the extent to which the NSA has penetrated foreign data flows, has undermined U.S. trade agreement negotiations. It has spurred data localization efforts around the world, and it has raised the spectre of the future role of the United States in Internet governance. Even if opportunistic, these shifts signal an immediate and **long-term impact of the NSA programs**, and public knowledge about them, **on the U.S. economy**.

A. Lost Revenues and Declining Market Share

Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private. Perhaps nowhere is this **more apparent** than in **cloud computing**.

Previously, approximately 50% of the worldwide cloud computing revenues derived from the United States. The domestic market thrived: between 2008 and 2014, it more than tripled in value. But within weeks of the Snowden leaks, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft's Azure were losing business. By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information. In January 2014 a survey of Canadian and British businesses found that one quarter of the respondents were **moving their data outside the United States**.

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. 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 confidence in data held by U.S. companies. The monetary impact of the NSA programs extends **beyond cloud computing** to the **high technology industry**. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs. Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had **dropped by 50**% since the leaks began. Also in June, the German government announced that because of Verizon's complicity in the NSA program, it

would end its contract with the company, which had previously provided services to a number of government departments. As a senior analyst at the Information Technology and Innovation Foundation explained, "It's clear to every single tech company that this is affecting their bottom line. The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros.

Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance.26 Salesforce.com made a similar announcement in March 2014.27 Google moved to encrypt terms entered into its browser.28 In June 2014 it took the additional step of releasing the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.29 The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.30 Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products.3'

Foreign technology companies, in turn, are seeing **revenues increase**. Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers' personal information. Its customer base increased 34% in the aftermath of the Snowden leaks. Mateo Meier, CEO of Artmotion, Switzerland's biggest offshore data hosting company, reported that within the first month of the leaks, the company saw a 45% rise in revenue. Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is through an official court order demonstrating guilt or liability; there are no exceptions for the United States. In April 2014, Brazil and the EU, which previously used U.S. firms to supply undersea cables for transoceanic communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process.36 OpenText, Canada's largest software company, now guarantees customers that their data remains outside the United States. Deutsche Telekom, a cloud computing provider, is similarly gaining more customers. Numerous **foreign companies** are marketing their **products as "NSA proof'** or "safer alternatives" to those offered by U.S. firms, gaining market share in the process.

Link – Studies

The best and newest research confirms that surveillance causes a chilling effect.

Marthews and Tucker 15 Alex, National Chair at Restore the Fourth, and Catherine, PhD in economics and professor of Marketing at MIT. "Government Surveillance and Internet Search Behavior." 17 February 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564. [Premier]

This study is the first to provide **substantial empirical documentation** of a chilling effect, both domestically in the shorter term and internationally in the longer term, that appears to be related to increased awareness of government surveillance online. Furthermore, this chilling effect appears in countries other than the US to apply to search behavior that is not strictly related to the government but instead forms part of the private domain.

Our findings have the following policy implications. From an economic perspective, our finding that there was an effect on international Google users' browsing behavior has potential policy implications for the effects of government surveillance on international commerce. **From a US competitive standpoint, the longer-run effect observed on international Google users' search behavior indicates that knowledge of US government surveillance of Google could indeed affect their behavior**. At the most limited end of the spectrum, it could steer them away from conducting certain searches on US search engines; at the most severe end of the spectrum, they might choose to use non-US search engines. Such effects may not be limited simply to search engines. For example, as Google's services are embedded in a large array of products, it could potentially hinder sales of Android-enabled mobile phones. Though preliminary attempts are being made to work towards initial measures of the economic impact of surveillance revelations (Dinev et al., 2008), no systematic study yet exists. All we can do, within the context of our data, is to indicate that on the basis of the effects we find, the strong possibility of **substantial economic effects** exists, and to suggest that such potential adverse economic impacts should be incorporated into the thinking of policy makers regarding the appropriateness of mass surveillance programs.

There are limitations to the generalizability of our findings. First, we are not sure how the results generalize outside of the search domain towards important tech industries such as the rapidly growing US cloud computing industry. Second, we are not sure how the revelations affected search on Google's major competitors, such as Bing and Yahoo! Search. It may be that the effect on their services was lessened by reduced media focus on them relative to Google in the light of the PRISM revelations and potentially the extent to which users anticipated that their servers may be located outside of the US. Third, our results are focused on the effects of revelations about government surveillance as opposed to the direct effects of government surveillance per se. Notwithstanding these limitations, we believe that our study provides an important first step in understanding the potential for effects of government surveillance practices on commercial outcomes and international competitiveness.

Link – Data Localization

NSA surveillance has triggered data localization, which destroys the international economy. It increases costs for every part of the economy, erodes innovation, and reverses the efficiencies of digital commerce.

Hill 14 Jonah Force, technology and international affairs consultant based in San Francisco and a Fellow of the Global Governance Futures program. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders." January 2014. SSRN Electronic Journal.
https://www.researchgate.net/publication/272306764_The_Growth_of_Data_Localization_Post-Snowden_Analysis_and_Recommendations_for_US_Policymakers_and_Business_Leaders. [Premier]

Over the course of recent decades, and principally since the commercialization of the Internet in the early 1990s, governments around the world have struggled to address the wide range of logistical, privacy, and security challenges presented by the rapid growth and diversification of digital data. The mounting online theft of intellectual property, the growth of sophisticated malware, and the challenges involved in regulating the flow, storage, and analysis of data have all – to varying degrees – increasingly challenged governments' ability to respond with effective policy. Until recently, these data management issues were left to the men and women of computer science departments, advocates for technology companies, and to the few government attorneys and bureaucrats responsible for overseeing Internet and data regulation. In the wake of former NSA contractor Edward Snowden's disclosures, however, which revealed to the global public the scale and intensity of intelligence collection online, data security and privacy issues have now become front-page headlines and the topics of dinner-table conversation the world over. As a result, governments are increasingly feeling compelled to do something they see as meaningful – if not outright drastic – to protect their citizens and their businesses from the many challenges they perceive to be threatening their nation's data and privacy. Of the various responses under consideration, perhaps none has been more controversial – or more deeply troubling to American businesses – than the push to enact laws that force the "localization" of data and the infrastructure that supports it. These are laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal situs of operations and management. By keeping data stored within national jurisdictions, or by prohibiting data from traveling through the territory or infrastructure of "untrustworthy" nations or those nations' technology companies, the argument goes, data will be better protected, and surveillance of the kind orchestrated by the NSA curtailed. Today, more than a dozen countries, 1 both developed and developing, have introduced or are actively contemplating introducing data localization laws. The laws, restrictions, and policies under consideration are diverse in their strategies and effects. Some proposals would enforce limitations for data storage, data transfer, and data processing; others require the local purchasing of ICT equipment for government and private sector procurements. There are proposals for mandatory local ownership of data storage equipment, limitations on foreign online retailers, and forced local hiring. Proposals of this sort are not historically unprecedented. Indeed, forms of data localization policies have been actively in place in many countries for years, including in the United States, where sensitive government data, such as certain classified materials, must be maintained within the servers of domestic companies. Broader

localization rules, which apply to all citizen data, have tended to be pursued by authoritarian governments such as Russia, China, and Iran, for which data localization laws have been viewed as an effective means to control information and to monitor the activities of their citizens.2 PostSnowden, however, even democratic countries are now seriously considering these more expansive data localization measures. Most notably, Brazil, Germany, and India– countries that have witnessed some of the most virulent anti-NSA reactions –are now contemplating enacting significant data localization laws. The EU is also contemplating localization within its area of authority.3 This is a deeply troubling development – not just for the technology firms of the United States who stand to lose customers and contracts as a result of these policies,4 but also for all the nations, firms, and individual Internet users who rely on the Web for economic trade and development, communications, and civic organizing. Not only do data localization policies fail to achieve their stated goals, they introduce a host of unintended consequences. **By restricting data flows and competition between firms, localization will likely bring up costs for Internet users and businesses, may retard technological innovation and the Internet's "generativity**," 5 **may reduce the ability of firms to aggregate services and data analytics through cloud services, and will surely curb freedom of expression and transparency globally. Ironically, data localization policies will likely degrade – rather than improve – data security for the countries considering them, making surveillance, protection from which is the ostensible reason for localization, easier for domestic governments (and perhaps even for foreign powers) to achieve**. Restricted routing, often a core component of data localization rules, may be technically infeasible without initiating a significant overhaul of the Internet's core architecture and governance systems, which itself would have significant negative effects. And perhaps most worrying, data localization policies – if implemented on a wide international scale – could have the effect of profoundly fragmenting the Internet,6 turning back the clock on the integration of global communication and ecommerce, and putting into jeopardy the myriad of societal benefits that Internet integration has engendered.

Impact – Competitiveness

That undermines US global technological leadership.

Castro and McQuinn 15 Daniel Castro works at the Center for Data Innovation, Government Technology, The Information Technology & Innovation Foundation, worked at the U.S. Government Accountability Office, went to Carnegie Mellon, and Alan McQuinn works at the Federal Communications Commission, previously had the Bill Archer Fellowship at the University of Texas. "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness." Benton Institute. June 2015. https://www.benton.org/headlines/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness. [Premier]

When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its **global technology leadership** to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy.

This has occurred over the last few years as the U.S. government has done relatively little to address the rising commercial challenge to U.S. technology companies, all the while putting intelligence gathering first and foremost. Indeed, policy decisions by the U.S. intelligence community have **reverberated throughout the global economy**. If the U.S. tech industry is to remain the leader in the global marketplace, then the U.S. government will need to set a new course that balances economic interests with national security interests. The cost of inaction is not only short-term economic losses for U.S. companies, but a wave of protectionist policies that will systematically weaken U.S. technology competiveness in years to come, with impacts on economic growth, jobs, trade balance, and national security through a weakened industrial base. Only by taking **decisive steps to reform its digital surveillance activities** will the U.S. government enable its tech industry to effectively compete in the global market.

Competitiveness decline causes great power war – empirics.

Baru 09 Sanjaya is a Professor at the Lee Kuan Yew School in Singapore. "Geopolitical Implications of the Current Global Financial Crisis." Strategic Analysis, Volume 33, Issue 2. March 2009. pages 163 – 168. [Premier]

Hence, economic policies and performance do have strategic consequences. In the modern era, the idea that strong economic performance is the foundation of power was argued most persuasively by historian Paul Kennedy. 'Victory (in war)', Kennedy claimed, 'has repeatedly gone to the side with more flourishing productive base'.3 Drawing attention to the interrelationships between economic wealth, technological innovation, and the ability of states to efficiently mobilize economic and technological resources for power projection and national defence, Kennedy argued that nations that were able to better **combine military and economic strength** scored over others. 'The fact remains', Kennedy argued, 'that **all of the major shifts in the world's military-power balance have followed alterations in the productive balances**; and further, that the rising and falling of the various empires and states in the international system has been confirmed by the outcomes of the major Great Power wars, where victory

has always gone to the side with the greatest material resources'. In Kennedy's view, the geopolitical consequences of an economic crisis, or even decline, would be transmitted through a nation's inability to find adequate financial resources to simultaneously sustain economic growth and military power.

Impact – Data Services

Data services key to poverty reduction, global growth, and trade between the US and Europe – specifically, it lifts over a hundred million out of poverty.

Hill 14 Jonah Force, technology and international affairs consultant based in San Francisco and a Fellow of the Global Governance Futures program. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders." January 2014. SSRN Electronic Journal.
https://www.researchgate.net/publication/272306764_The_Growth_of_Data_Localization_Post-Snowden_Analysis_and_Recommendations_for_US_Policymakers_and_Business_Leaders. [Premier]

Economic Growth Objectives Not Well Served Data localization (most especially, as a ban on foreign firms operating local servers) appeals to those political and business leaders who hope to give domestic technology firms a competitive advantage. It also appeals to those leaders who believe that that competitive advantage will, over time, lead to the development of a strong technology sector, following what might be thought of as a "China developmental model," in which early domestic protectionism is tapered off as local firms find their competitive edge. But again, the benefits of this kind of policy (which generally only advantage certain favored local companies) are outweighed by its drawbacks. By prohibiting foreign firms from operating in country, or by making operations prohibitively expensive for foreign firms, governments are dramatically limiting the options available to local consumers. This includes small businesses that often require the cheaper and more advanced services that only international firms can provide. Indeed, even non tech-related industries that nevertheless rely on IT services, such as advanced manufacturing, are likely to see that their costs rise and their efficiencies deteriorate as a consequence of Internet protectionism in the guise of localization. These costs may not be trivial. The European Centre for International Political Economy has estimated that if and when cross-border data flows between the U.S. and EU are seriously disrupted (assuming existing models for cross-border transfer and processing of data, such as the Safe Harbor and BCRs108 are disrupted), the negative impact on EU GDP could reach -0.8% to -1.3%, and EU services exports to the United States could drop by as much as -6.7% due to loss of competitiveness.109 Developing countries, too, would likely suffer. There, **Internet access and data services are significant drivers of economic growth**. According to several important studies on the issue, **access to the Internet can dramatically reduce the effect on developing countries of geographical isolation from major exports markets**.110And, according to a Deloitte study, e**xpanding access to the 4 billion people who live in developing countries to levels developed economies currently enjoy would increase productivity in those areas by as much as 25 percent, add $2.2 trillion in additional GDP**, increase the GDP growth rate by 72 percent, add more than **140 million new jobs, and lift 160 million people out of extreme poverty.** 111 Certainly, the cost inherent in localization alone will not forestall all of these positive developments, but it would retard them. To leaders in developing nations such as India and Brazil, where data localization measures are under serious consideration, these potential adverse economic impacts ought to give serious pause. Less directly, but perhaps even more critically as a long-term matter, data localization adversely affects the Internet's capacity for productivity by reducing the Internet's "network effect" and "generativity.112" **By placing limitations on which firms can participate in the network, data localization reduces the overall size of the network, which, according to network theory as well as**

Metcalfe's Law (which states that the value of a communications network is proportional to the number of users of the system), **would bring up both costs and the overall innovative potential of the aggregated network.** Consider big data analytics, for example, which often involves the transfer of data from numerous sources without regard to geography and can have major benefits for society.113 B***y severing the ties between nations and the data that can be collected an analyzed, data localization* vastly diminishes t*he capacity for new discoveries and for new solutions to some of the world's most pressing problems***. Certainly, there are good reasons for supporting local Internet infrastructure development. Developing local Internet infrastructure has been shown to help to keep costs down (by avoiding having to send data afar unnecessarily and by providing greater options in pricing negotiations) and to keep service available when connectivity to the outside would is disrupted. 114 **Governments can and should invest in building up local capabilities. But restricting data flows and preventing foreign competition are not the ways to facilitate that type of local development**. Decisions regarding where to store data and how it should be handled – except in the rare cases of national security or other special privacy cases (for example, there may be good reasons for medical data and the like to be given special treatment) – should be driven by efficiencies, not by political expediency.

Impact – Economy

High tech bolsters the US economy by multiplying investment and spilling across sectors.

Donohue 18 Lauren, Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law. "High Technology, Consumer Privacy, and U.S. National Security." *Symposium Articles*, American University Business Law Review, 4(1). 2018. https://digitalcommons.wcl.american.edu/aublr/vol4/iss1/3/. [Premier]

High technology is central to the U.S. economy. A recent study by the Bay Area Economic Council Institute sought to ascertain how important the high tech industry is just for the U.S. labor market. It found that not only are high-tech jobs critical for generating employment in other sectors, but that growth in the hightech sector has increasingly been happening in areas of great economic and geographic diversity, suggesting that the high-tech industry is not limited to one ethic, social, or economic strata. High-technology has been one of the fastest-growing sectors: between 2004 and 2012, the employment growth in high-tech outpaced private sector growth by a ratio of 3:1. Jobs in Science, Technology, Engineering, and Mathematics (STEM) outpaced job gains across all occupations by a ratio of 27:1. 98 Employment predictions put the demand for high-tech workers to increase 16.2% 2011 to 2020, with STEM employment increasing 13.3% during the same period.99 The study found that the generation of jobs in high-technology had farreaching effects. In addition to the income gains generated by innovation, productivity and a global marketplace, high-technology industrial growth generated other types of jobs. Health care, education, law, restaurants, hotels and personal services, as well as goods-producing construction sectors grew in tandem with high tech, largely because of a local multiplier effect: "For each job created in the local high-tech sector," the study concluded, "approximately 4.3 jobs are created in the local non-tradable sector in the long run."100 Even as early as 2002, the National Science Foundation found that the global market for high-technology goods is growing at a swifter rate than for other manufactured goods. More than this, "high-technology industries are driving economic growth around the world." This study built on one released in 1995 by the National Academies, which had looked carefully at the role and importance of high tech companies in the U.S. economy.102 Indeed, study after study reflects the importance of high-technology in the U.S. economy. In 2015, a Brookings study found that "advanced industries" (which include high-technology, STEM, and industries, like aerospace, which are heavily dependent on advanced technologies), "represent a sizable economic anchor for the U.S. economy."103 **They led the post-recession recovery**. Brookings found that with only 9 percent of the total U.S. employment, advanced industries produce some $2.7 trillion per year—around 17% of the country's GDP. Further, about 60 percent of U.S. exports are tied to this sector, with 2.2 jobs being created domestically for every new advanced industry job. In sum, "Directly and indirectly. . . the sector supports almost 39 million jobs—**nearly one-fourth of all U.S. employment**."104

Internet Freedom

Link – Fracturing

Failure to curtail NSA surveillance causes internet fracturing and undermines the global structure.

Meinrath 13 Sascha, vice president of the New America Foundation and director of the Open Technology Institute. "The Future of the Internet: Balkanization and Borders." Time. 11 October 2013. http://ideas.time.com/2013/10/11/the-future-of-the-internet-balkanization-and-borders. [Premier]

Brazilian President Dilma Rouseff's recent indictment of the United States' cyberspying practices has profound global repercussions for the U.S vision of a borderless, open Internet. What makes this backlash especially potent and lamentable is that it is being fueled not by democracies that oppose American ideals, but rather by allies that resent Washington's betrayal of its own overarchingly positive vision. Advertisement Rouseff's offensive to change Internet governance follows reports that the National Security Agency's watchful eye could see as far as her Palácio do Planalto in Brasília. According to leaked documents, the United States has been surveilling Rousseff's email, intercepting internal government communications, and spying on the country's national oil company. After canceling an official visit to meet with President Obama in Washington, Rousseff took to the podium at the U.N.'s General Assembly to call on other countries to disconnect from U.S. Internet hegemony and develop their own sovereign Internet and governance structures. Rousseff's move could lead to a powerful chorus—one that would transform the Internet of the future from a global commons to a fractured patchwork severely limited by the political boundaries on a map. Brazil is one of a handful of countries—including Indonesia, Turkey, and India—that have wavered in the debate over whether to develop an international framework to govern the Internet, one that would replace the role that the United States has played as chief Internet steward. Traditionally, that debate has featured America in the role as champion of a free and open Internet, one that guarantees the right of all people to freely express themselves. Arguing against that ideal: repressive regimes that have sought to limit connectivity and access to information. The NSA's actions have shifted that debate, alienating key Internet-freedom allies and emboldening some of the most repressive regimes on the planet. Think of it as an emerging coalition between countries that object to how the United States is going about upholding its avowed principles for a free Internet, and countries that have objected to those avowed principles all along. Our close allies in the European Union, for instance, are now considering revoking data-sharing agreements with the United States and requiring American website providers to prominently warn Europeans that their data is subject to U.S. government surveillance. Meanwhile, repressive regimes like Iran, Syria, and China are wresting control of information over their networks, poisoning popular applications and services, and undermining the foundations for the Internet's open, interconnected structure. NSA misdeeds undoubtedly further embolden these regimes to do as they please. The motivations of those nations questioning America's de facto control over the global Internet may vary, but their responses are all pointing in the same troubling direction: toward a Balkanized Internet. Today, the Internet is in danger of becoming like the European train system, where varying voltage and 20 different types of signaling technologies force operators to stop and switch systems or even to another locomotive, resulting in delays, inefficiencies, and higher costs. Netizens would fall under a complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights. And much as different signaling hampers the movement of people and the trade of physical goods, an Internet within such a complex jurisdictional structure would certainly hamper modern economic activity. The NSA has opened a Pandora's box that treats "citizens" and "foreigners" differently (even defining both groups in myriad different ways). Its rules also impose geo-locational-based jurisdictional mandates (based upon the route of your Internet traffic or the location of the data services and databases you use). They also include requirements based upon ownership; the location of a company's headquarters may lead to surveillance mandates covering services and infrastructure in other countries. This creates tremendous technical challenges for startups and entrepreneurs—who will have to overcome impossible compatibility hurdles just to get up and running—stifling innovation at a moment when we need greater economic momentum, not dead weight. Already, a German citizen accessing a New York City data center via a Chinese fiber line may find her data covered by an array of conflicting legal requirements requiring privacy and active surveillance at the same time. Fracturing the Internet undermines Internet freedom as well. The basic principle at the heart of Article 19 of the Universal Declaration of Human Rights—protecting the right to freedom of opinion, expression, and the opportunity to participate in the

information society—is at risk. Brazil may not be pressing to assert control over everything online or censor its own people, or spy on them, but plenty of other countries with darker motives are cheering Brazil on. The U.S. has done a disservice to all people already living and working under repressive regimes by creating a new international norm that massive-scale surveillance is acceptable. As others adopt the U.S. model, particularly in areas where movements for fundamental freedoms are burgeoning and fighting against oppression, there will be even less access to basic communications, hampering the ability to interact online outside of the regime's control and censorship. Furthermore, the NSA has made a remarkably myopic tradeoff—overreaching its legal authorities for a slight boost in signals intelligence today that will lead to massive problems in response. Even before all the recent revelations of NSA misbehavior, the United States was already facing calls for a more "democratic" global system of Internet regulation that gave other countries more say in setting rules. Now, for the sake of a free Internet, it is imperative for Washington to move fast to restore a belief that America is a trustworthy Internet steward. It's time for bold leadership to defend our core principles. Reforms need to go far beyond pro-forma reviews carried out by intelligence and administration insiders. There are precedents for the United States' exercising restraint in order to advance larger interests. As a country, we agreed to stop atmospheric testing of nuclear weapons, not to stockpile or deploy chemical weapons, and not to militarize outer space. There must be a cyberspace equivalent of this restraint—a restoration of balance that prioritizes civil rights, not surveillance, as vital to (inter)national security. Is the benefit of spying on Brazil's oil company worth the cost of antagonizing the people of our hemisphere's second-largest democracy and giving China and Russia the moral high ground in debates over how people around the world should access information? Do we really want a world where this behavior is normalized and where it's acceptable for every country to surveil and hack indiscriminately? The answer to that question seems pretty clear. Today we need bold reforms from Washington—we need to curtail our unhealthy addiction to surveillance and covert hacking. Only by being radically transparent about the scope of current activities and ceasing activities that transgress national norms will we regain global trust and shift the rather bleak trajectory we are currently on.

Link – Hypocrisy

The US *can* alter global practices that threaten internet freedom – but only when US image is seen as less hypocritical.

Wong 13 Cynthia M. Wong is the senior researcher on the Internet and human rights for Human Rights Watch. "Surveillance and the Corrosion of Internet Freedom." The Huffington Post. 30 July 2013. http://www.hrw.org/news/2013/07/30/surveillance-and-corrosion-internet-freedom. [Premier]

Defenders of US and UK surveillance programs argue that collecting metadata is not as problematic as "listening to the content of people's phone calls" or reading emails. This is misleading. Technologists have long recognized that metadata can reveal incredibly sensitive information, especially if it is collected at large scale over long periods of time, since digitized data can be easily combined and analyzed. The revelations have also exposed glaring **contradictions** about the **US Internet freedom agenda.** This has emboldened the Chinese state media, for example, to cynically denounce US hypocrisy, even as the Chinese government continues to censor the Internet, infringe on privacy rights, and curb anonymity online. Though there is hypocrisy on both sides, the widening rift between US **values** and **actions** has real, unintended human rights consequences. For the human rights movement, the Internet's impact on rights crystalized in 2005 after we learned that Yahoo! uncritically turned user account information over to the Chinese government, leading to a 10-year prison sentence for the journalist Shi Tao. The US government forcefully objected to the Chinese government's actions and urged the tech industry to act responsibly. In the end, that incident catalyzed a set of new human rights standards that pushed some companies to improve safeguards for user privacy in the face of government demands for data. **US support was critical back then**, but it is hard to imagine the government having the same influence or credibility now. The mass surveillance scandal has damaged the US government's ability to press for better corporate practices as technology companies expand globally. It will also be more difficult for companies to resist overbroad surveillance mandates if they are seen as complicit in mass US infringements on privacy. Other governments will feel more entitled to ask for the same cooperation that the US receives. We can also expect governments around the world to pressure companies to store user data locally or maintain a local presence so that governments can more easily access it, as Brazil and Russia are now debating. While comparisons to the Chinese government are overstated, there is reason to worry about the broader precedent the US has set. Just months before the NSA scandal broke, India began rolling out a centralized system to monitor all phone and Internet communications in the country, without much clarity on safeguards to protect rights. This development is chilling, considering the government's problematic use of sedition and Internet laws in recent arrests. Over the last few weeks, Turkish officials have condemned social media as a key tool for Gezi Park protesters. Twitter has drawn particular ire. Now the government is preparing new regulations that would make it easier to get data from Internet companies and identify individual users online. The Obama administration and US companies could have been in a strong position to push back in India and Turkey. Instead, the US has provided these governments with a roadmap for conducting secret, mass surveillance and conscripting the help of the private sector.

Impact – Global Economy

Washington will inevitably push for global Internet freedom – but US image is vital. The Internet freedom agenda's key to the Global Economy.

Kalathil 10 Shanthi Kalathil, Adjunct Faculty and Adjunct Lecturer in the Communication, Culture, and Technology (CCT) Master of Arts Program at Georgetown University. "Internet Freedom: A Background Paper." Aspen Institute. October 2010. http://www.aspeninstitute.org/sites/default/files/content/images/Internet_Freedom_A_Background_Paper_0.pdf. [Premier]

As use of the Internet has grown exponentially around the world, so too have concerns about its defining attribute as a free and open means of communication. Around the world, countries, companies and citizens are grappling with thorny issues of free expression, censorship and trust. With starkly different visions for the Internet developing, this era presents challenges—and also opportunities—for those who wish to ensure the Internet remains a **backbone of** liberty and **economic growth. U.S. officials have made clear their vision for the Internet**'s future. President Obama, in a speech before the UN General Assembly, said that **the U.S. is committed** to promoting new communication tools, "so that people are empowered to connect with one another and, in repressive societies, to do so with security. We will support a free and open Internet, so individuals have the information to make up their own minds." His words were reinforced by FCC Chairman Julius Genachowski: "It is essential that we preserve the open Internet and stand firmly behind the right of all people to connect with one another and to exchange ideas freely and without fear."1 Indeed, a free, widely accessible Internet stands **at the heart of** both global communication and **global commerce.** Internet freedom enables dialogue and direct diplomacy between people and civilizations, facilitating the exchange of ideas and culture while bolstering trade and economic growth. Conversely, censorship and other blockages stifle both expression and innovation. When arbitrary rules privilege some and not others, the investment climate suffers. Nor can access be expanded if end users have no trust in the network. However, making reality live up to aspirations for Internet freedom can prove difficult. Numerous global initiatives—spearheaded by governments, private sector and civil society—are attempting to enshrine the norms, principles and standards that will ensure the Internet remains a public space for free expression. At the same time, other norms are fast arising—particularly those defined by authoritarian countries that wish to splinter the Internet into independently controlled fiefdoms. Even as Internet access has expanded around the world, many governments are attempting to control, regulate and censor the Internet in all its forms: blogs, mobile communication, social media, etc. Such governments have devoted vast resources to shaping the Internet's development within their own borders, and they are now seeking to shape the Internet outside their borders as well. Indeed, Internet experts are worried that national governments of all stripes will increasingly seek to extend their regulatory authority over the global Internet, culminating in a balkanized Internet with limited interoperability. Hence, the next few years present a distinct window of opportunity to elevate the principles of the free exchange of ideas, knowledge and commerce on the Internet. While U.S. leadership within this window is vital, a global effort is necessary to ensure that these norms become a standard part of the Internet's supporting architecture.

Impact – Laundry List

Free Internet failure causes extinction from a laundry list of threats.

Eagleman 10 David Eagleman, neuroscientist at Baylor College of Medicine, where he directs the Laboratory for Perception and Action and the Initiative on Neuroscience and Law and author of Sum (Canongate). " Six ways the internet will save civilization." Wired. 9 November 2010. http://www.wired.co.uk/magazine/archive/2010/12/start/apocalypse-no. [Premier]

Many great civilizations 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 Pompeiians 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 civilization. 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.

Impact – Democracy Promotion

US global democracy promotion is inevitable. Success in the internet freedom agenda is key to a successful push.

Fontaine et al. 11 Richard Fontaine, President of the Center for a New American Security (CNAS). "Internet Freedom A Foreign Policy Imperative in the Digital Age." Center for a New American Security. June 2011 http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf. [Premier]

The United States has a long history of providing diplomatic and financial support for the promotion of human rights abroad, including the right to free expression. While **each** presidential administration emphasizes human rights to differing degrees, during recent decades they have all consistently held that human rights are a key U.S. interest. Promoting freedom of the Internet expands human rights support into cyberspace, an environment in which an ever-greater proportion of human activity takes place. The United States advocates for freedom of the Internet because it accords not only with American values, but also with rights America believes are intrinsic to all humanity. For years, the U.S. government has programmatically and rhetorically supported **democracy promotion** abroad. The State Department routinely disburses millions of dollars in funding for democracy-building programs around the world, many of which are aimed explicitly at expanding free expression. Presidential and other speeches regularly refer to the American belief in the universality of this right; to cite but one example, a March 2011 White House statement on Syria noted that, "The United States stands for a set of universal rights, including the freedom of expression and peaceful assembly."8 The Obama administration's 2010 National Security Strategy specifically called for marshaling the Internet and other information technologies to support freedom of expression abroad,9 and the Bush administration adopted a policy of maximizing access to information and ideas over the Internet.10 America's interest in promoting freedom via the Internet comes from the same fundamental belief in democratic values and human rights. Despite inevitable inconsistencies and difficult tradeoffs, the United States continues to support democracy. The Bush administration's 2006 National Security Strategy committed to support democratic institutions abroad through transformational diplomacy.11 President Obama, after entering office with an evident desire to move away from the sweeping tone of his predecessor's "freedom agenda," nevertheless told the U.N. General Assembly in 2009 that "there are basic principles that are universal; there are certain truths which are self-evident – and the United States of America will never waver in our efforts to stand up for the right of people everywhere to determine their own destiny."12 To the extent that supporting Internet freedom advances America's democracy-promotion agenda, the rationale for promoting online freedom is clear. However, cause and effect are not perfectly clear and the United States must choose its policies under conditions of uncertainty. Both the Bush and Obama administrations have wagered that by promoting global Internet freedom the United States will not only operate according to universal values but will promote tools **that** may, on balance, **benefit societies over the autocrats that oppress them**. Secretary of State Hillary Rodham Clinton urged countries to "join us in the bet we have made, a bet that an open Internet will lead to stronger, more prosperous countries."13 **Given the evidence we discuss throughout this report, this bet is one worth making.**

Global democracy consolidation checks inevitable extinction.

Diamond '95 Larry, Senior Fellow at the Hoover Institution. "Promoting Democracy in the 1990s." Wilson Center. December 1995. http://www.wilsoncenter.org/subsites/ccpdc/pubs/di/fr.htm. [Premier]

This hardly exhausts the lists of threats to our security and well-being in the coming years and decades. In the former Yugoslavia nationalist aggression tears at the stability of Europe and could easily spread. The flow of illegal drugs intensifies through increasingly powerful international crime syndicates that have made common cause with authoritarian regimes and have utterly corrupted the institutions of tenuous, democratic ones. **Nuclear, chemical, and biological weapons continue to proliferate. The very source of life on Earth, the global ecosystem, appears increasingly endangered**. Most of **these** new and unconventional **threats** to security are associated with or aggravated by the weakness or **absence of democracy**, with its provisions for legality, accountability, popular sovereignty, and openness. LESSONS OF THE TWENTIETH

CENTURY The experience of this century offers important lessons. **Countries that govern themselves in a** truly **democratic fashion do not go to war with one another. They do not aggress against their neighbors** to aggrandize themselves or glorify their leaders. **Democratic governments do not ethnically "cleanse" their own populations, and they are much less likely to face ethnic insurgency. Democracies do not sponsor terrorism against one another. They do not build weapons of mass destruction** to use on or to threaten one another. **Democratic countries** form more reliable, open, and enduring trading partnerships. In the long run they offer better and more stable climates for investment. They **are more environmentally responsible** because they must answer to their own citizens, who organize to protest the destruction of their environments. **They are better bets** to honor international treaties since they value legal obligations and because their openness makes it much more difficult to breach agreements in secret. Precisely because, within their own borders, they respect competition, civil liberties, property rights, and the rule of law, democracies are the only reliable foundation on which a new world order of international security and prosperity can be built.

Whistleblowing

Link – Programs

The insider threat program will be abused by agencies and used to undercut and intimidate potential federal whistleblowers – the reach of the program affects all federal employees creating a chilling effect

Higham 14 Scott, Higham writer for the Washington Post. "Intelligence security initiatives have chilling effect on federal whistleblowers, critics say." Washington Post. 23 July 2014. https://www.washingtonpost.com/world/national-security/intelligence-security-initiatives-have-chilling-effect-on-federal-whistleblowers-critics-say/2014/07/23/c9dfd794-0ea0-11e4-8341-b8072b1e7348_story.html. [Premier]

The Insider Threat Program and a continuous monitoring initiative under consideration in the intelligence community were begun by the Obama administration after the leaks of classified information by former NSA contractor Edward Snowden and Army Pvt. Chelsea Manning, and the Navy Yard shootings by Aaron Alexis, who used his security clearance to gain access to the base. The programs are designed to prevent leaks of classified information by monitoring government computers and employees' behavior. Grassley said the episode with the FBI illustrates how federal agencies are setting up internal security programs without giving careful consideration to whether they could **dissuade whistleblowers** from coming forward. "The **I**nsider **T**hreat **P**rogram has the potential for **taking the legs out from underneath all** of the whistleblower protections we have," Grassley said in a recent interview. Greg Klein, the head of the FBI's Insider Threat Program, and McDonough, the congressional affairs agent, did not return calls seeking comment. An FBI spokesman said the bureau does not plan to register whistleblowers. He said there was a misunderstanding about the nature of the briefing with staff members for Grassley, Judiciary Committee Chairman Patrick J. Leahy (D-Vt.) and a law enforcement official who is assigned to the Senate panel. The spokesman noted that the FBI has a whistleblower training program for employees and a whistleblower protection office. "We recognize the importance of protecting the rights of whistleblowers," FBI spokesman Paul Bresson said. Grassley is part of a growing chorus of lawmakers on Capitol Hill and attorneys for whistleblowers who warn that the **I**nsider **T**hreat **P**rogram and the potential intelligence community initiative threaten to undermine federal workers' ability to report wrongdoing without retaliation. Together, the programs cover millions of federal workers and contractors **at every government agency**. In February, Director of National Intelligence James R. Clapper Jr. testified before the Senate Armed Services Committee that a system was being considered to continuously monitor the behavior of employees with security clearances "on the job as well as off the job." A senior intelligence official said a continuous monitoring program, mandated under the Intelligence Authorization Act and signed into law by President Obama on July 7, is being set up and initially will include federal employees who hold top-secret security clearances. The official said there are no plans to monitor employees after hours while they are using non-government computer systems. "I think **it's time to put up the caution light here,"** said Sen. Ron Wyden (D-Ore.), a member of the Senate Intelligence Committee. While Wyden included a provision in the most recent Intelligence Authorization Act that would prohibit retaliation against whistleblowers, he said he remains concerned about the impact of the threat programs. "This really has the potential for abuse, and I think it **could have a chilling effect on the public's right to know and effective oversight of our government**," Wyden said. Dan Meyer, the head of the Intelligence Community Whistleblowing & Source Protection program, created last year as part of the Office of Intelligence Community Inspector General, said he is working to ensure that employees who want to report wrongdoing can do so anonymously and without reprisal. "The critical thing is to maintain confidentiality," Meyer said. He said he is preparing training materials for intelligence officers and spreading the word that employees can come to him anonymously through third parties. If an employee has verifiable information about wrongdoing, a presidential directive takes effect, providing employees with protection against retaliation. "We are in the process of making a systematic, cultural change and getting everyone on board," Meyer said. After Manning's disclosures to WikiLeaks four years ago, Obama signedExecutive Order 13587, directing government agencies to assess how they handle classified information. On Nov. 28, 2010, the Office of the National Counterintelligence Executive issued a memo to senior government agency officials, advising them to identify insider threats. The memo suggested using psychiatrists and sociologists to assess changes in employees' behavior. "What metrics do you use to measure 'trustworthiness' without alienating employees?" the counterintelligence office asked the agency chiefs. "Do you use a psychiatrist or sociologist to measure: relative happiness as a means to gauge trustworthiness? Despondence and grumpiness as a means to gauge waning trustworthiness?" "It will only increase hostility between the government and really serious federal employees who are trying to improve the system," said Lynne Bernabei, a partner at Bernabei & Wachtel in Washington who has been representing whistleblowers for nearly 30 years. "Turning the security apparatus against its own people is not going to work." Whistleblower lawyers said they understand the need to protect classified information but think some of the new programs go too far. "There are legitimate reasons for employers to be on the lookout for people who might be leaking classified information, but **this will obviously have a chilling effect on employees who might want to blow the whistle**," said Jason Zuckerman, who served as the senior legal adviser to the U.S. Office of Special Counsel, the federal agency charged with protecting whistleblowers, and now represents whistleblowers nationwide. Michael German, a former undercover FBI agent and whistleblower, called the Insider Threat Program a "dangerous" initiative.

Link – Journalism

Status quo mass surveillance chills journalism and crushes government accountability.

Wong 15 Cynthia M. Wong is the senior researcher on the Internet and human rights for Human Rights Watch. "Internet at a Crossroads: How Government Surveillance Threatens How We Communicate." Human Rights Watch. 2015. http://www.hrw.org/world-report/2015/essays/internet-crossroads. [Premier]

A joint report published by Human Rights Watch and the American Civil Liberties Union in July 2014 documented the insidious effects of **large-scale** surveillance on the practice of journalism and law in the US. Interviews with dozens of journalists showed that increased surveillance, combined with tightened measures to prevent leaks and government contact with media, are intimidating sources, keeping them from talking to journalists (even about unclassified topics of public concern) out of fear that they could face retaliation, lose their security clearances or jobs, or even face prosecution. Ultimately, **this is having a detrimental impact on** the amount and quality of news **coverage,** particularly on matters related to national security, intelligence, and law enforcement. This effect **undermines** the role of the fourth estate in **holding government to account.** Steve Coll, staff writer for the New Yorker and dean of the Graduate School of Journalism at Columbia University, explained: "Every national security reporter I know would say that the atmosphere in which professional reporters seek insight into policy failures [and] bad military decisions is just much tougher and much chillier." Public understanding of national security policies that are carried out in our name **is essential** to the functioning of healthy democracies and open societies.

Indiscriminate collection hampers aggressive journalism on bad national security decisions.

Sinha 14 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. "With Liberty to Monitor All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy." Human Rights Watch. July 2014. http://www.hrw.org/node/127364. [Premier]

Every national security reporter I know would say that the atmosphere in which professional reporters seek insight into policy failures [and] bad military decisions is just **much tougher and** much **chillier.** – Steve Coll, staff writer for The New Yorker and Dean of the Graduate School of Journalism at Columbia University, February 14, 2014 Numerous US-based journalists covering intelligence, national security, and law enforcement describe the current reporting landscape as, in some respects, the most difficult they have ever faced. "This is the worst I've seen in terms of the government's efforts to control information," acknowledged Jonathan Landay, a veteran national security and intelligence correspondent for McClatchy Newspapers.68 "It's a terrible time to be covering government," agreed Tom Gjelten, who has worked with National Public Radio for over 30 years.69 According to Kathleen Carroll, senior vice president and executive editor of The Associated Press, "We say this every time there's a new occupant in the White House, and it's true every time: each is more secretive than the last."70 Journalists are struggling harder than ever before to protect their sources, and sources are more reluctant to speak. This environment makes reporting both slower and less fruitful. Journalists interviewed for this report described the difficulty of obtaining sources and covering sensitive topics in an atmosphere of uncertainty about the range and effect of the government's power over them. Both surveillance and leak investigations loomed large in this context—especially to the extent that there may be a relationship between the two. More specifically, many journalists see the government's power as menacing because they know little about when various government agencies share among themselves information collected through surveillance, and when they deploy that information in leak [what they] will do with it," observed James Asher, Washington Bureau Chief for McClatchy Co., the third largest newspaper group in the country.72 One Pulitzer Prize-winning reporter for a newspaper noted that even a decrease in leak prosecutions is unlikely to help, "unless we [also] get clear lines about what is collectable and usable."73 Others agreed. "I'm pretty worried that NSA information will make its way into leak investigations," said one investigative journalist for a major outlet.74 A reporter who covers national defense expressed concern about the possibility of a "porous wall" between the NSA and the Department of Justice, the latter of which receives referrals connected to leak investigations.75 Jonathan Landay wondered whether the government might analyze metadata records to identify his contacts.76 A national security

reporter summarized the situation as follows: “Do we trust [the intelligence] portion of the government’s knowledge to be walled off from leak investigations? That’s not a good place to be.”77 While most journalists said that their difficulties began a few years ago, particularly with the increase in leak prosecutions, our interviews confirmed that for many journalists largescale surveillance by the US government **contributes substantially to the new challenges they encounter.** The government’s large-scale collection **of metadata** and communications makes it significantly more difficult for them to protect themselves and their sources, to confirm details for their stories, and ultimately **to inform the public.**

Impact – Corruption

Surveillance erodes meaningful checks on inappropriate government officials. It spills beyond national security into many policy issues.

Brown 14 Bruce Brown. Counsel of Record. "Reporters Committee for Freedom of the Press Amicus Brief." Electronic Frontier Foundation. 9 Sept 2014. https://www.eff.org/document/rcfp-smith-amicus-brief. [Premier]

In a report that former Washington Post executive editor Leonard Downie Jr. wrote for the Committee to Protect Journalists, numerous journalists said surveillance programs and leak prosecutions deter sources from speaking to them. Comm. To Protect Journalists, The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America 3 (Oct. 10, 2013), http://bit.ly/1c3Cnfg. In the report, Associated Press senior managing editor Michael Oreskes commented: "There's no question that sources are looking over their shoulders. Sources are more jittery and more standoffish, not just in national security reporting. A lot of skittishness is at the more routine level." Id. Washington Post national security reporter Rajiv Chandrasekaran said: "**One of the most pernicious effects is the chilling effect created across government on matters that are less sensitive but certainly in the public interest as a check on government and elected officials.**" Id. Discussing the NSA surveillance programs, New York Times investigative reporter and three-time Pulitzer Prize winner David Barstow stated, "I have absolutely **no doubt** whatsoever that **stories have not gotten done because of this.**" Jamie Schuman, The Shadows of the Spooks, The News Media and the Law, Fall 2013, at 9.

Aggressive press is vital to check corrupt governance practices. It builds more accountable governance.

Sinha 14 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. "With Liberty to Monitor All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy." Human Rights Watch. July 2014. http://www.hrw.org/node/127364. [Premier]

In recent decades, the press has played an **important role in checking government**, and **in particular, the intelligence community.**225 That has not always been the case. Betty Medsger, a former Washington Post reporter whose series of stories in 1971 first revealed the FBI's targeting of dissenters, recalled that there was "very little investigative work" before her articles appeared.226 Even her FBI stories derived from documents stolen by activists, rather than through Medsger's cultivation of sources inside the intelligence community. "I was given these files. I didn't have clever techniques. Nobody was trying to develop inside sources until then."227 Tim Weiner, a Pulitzer Prize-winning reporter for the New York Times, who also won a National Book Award for his history of the CIA, offered an earlier timeline for the development of investigative journalism on the intelligence community, observing that "serious investigative reporting into the CIA started in the mid-1960's, and then seriously expanded a decade later."228 Phil Bennett elaborated: The growth of the intelligence community and of a more critical, more adversarial press occurred in tandem, on overlapping timelines. Although there have been state secrets since the founding of the Republic, the current institutional structure that manufactures and protects those secrets emerged near the end of World War II and the beginning of the Cold War. For the most part, at first journalists did little to contest the government's monopoly on secrets. But the Vietnam War led some journalists to see secrecy as a tool for the government to deceive the public. The Pentagon Papers case ratified this view. Disclosing government secrets then became a central part of the birth of modern investigative reporting. This has carried over to the digital era.229 Ultimately, the government's own investigations into the intelligence community in the mid-1970s—most famously among them, the Church Committee in the Senate—provided **a sound basis** for ongoing and active investigative work by journalists on the intelligence community ever since.230 **Those inquiries revealed significant** and widespread **misconduct by the intelligence community** dating back decades. By offering the public significant and early insight into objectionable practices by the FBI, Medsger's stories formed a major part of the environment that gave rise to those investigations,231 complementing pressure resulting from the Vietnam War and Seymour Hersh's 1974 reporting on the CIA.232 But coverage of the intelligence community has **recently** (once again) become more challenging to undertake. "It seems to me that at some point it became very difficult again to cover these institutions and get inside sources," Medsger observed.233 Many journalists who spoke to us expressed a strong commitment to their work, and were unwilling to be dissuaded from continued efforts to cover increasingly difficult beats. "I'm not in any way going to stop reporting," remarked Adam Goldman. "In most cases, I am not the vulnerable one," added Steve Aftergood.234 Peter Maass also identified a silver lining: "Even though it's harder, it's also very exciting.

We're being given an amazing opportunity to do exciting work that could help shape society for years to come."235 Nevertheless, the effects that **surveillance** and leak investigations have had on coverage are working to undermine **effective** democratic participation and governance. "**What makes government better is** our **work exposing information**," argued Dana Priest, a Pulitzer Prize-winning national security reporter at the Washington Post.236 "It's not just that it's harder for me to do my job, though it is. **It** also **makes the country less safe. Institutions work less well, and it increases the risk of corruption. Secrecy works against all of us."**237 Charlie Savage added, "**National security journalism is especially important for a functioning,** democratically **accountable system**."238 Steve Coll agreed as well, noting, "**There's a real loss to the public**, the voters. For James Asher, "The role of the press is to be challenging and critical."240 It is thus inherently important for journalists to seek out certain information that the government treats as sensitive and, when appropriate, share it with the public. Kathleen Carroll also emphasized the responsibility typically demonstrated by journalists who work on national security topics. "This is not a bunch of bratty journalists trying to undermine legitimate government operations," she argued. Moreover, though she believes "that a government's actions on behalf of the people it serves should be public, [m]ost news organizations [including her outlet, the Associated Press] will recognize that certain things the government is doing need to remain secret, at least for now. The disputes take place because the government idea of what should remain secret **is much more sweeping."**241

Impact – Environment

Whistleblower protections are necessary for the environment – failure means the collapse of the planet and humanity from environmental deterioration

Warren 15 Christopher K. Warren, Senior Note Editor. "Blowing The Whistle On Environmental Law: How Congress Can Help The EPA Enlist Private Resources In The Fight To Save The Planet." Boston College Environmental Affairs Law Review. 195. 2015. https://lawdigitalcommons.bc.edu/ealr/vol42/iss1/7/. [Premier]

The changing environment may be one of **the most pressing threat**s **in** all of **human history**. n196 **Climate change, dwindling fresh drinking water supplies, and exposure to toxic elements pose serious health concerns to human beings, and have the potential to jeopardize the future of humanity**. n197 Greater preventative, mitigating, and remedial actions are needed to prevent these threats from spiraling out of control and creating devastating effects, and it will take an effort--both public and private--of massive proportions to achieve such prevention. n198 Given the scope of the problem, every effort should be made to incentivize widespread participation in the enforcement of environmental protection measures. n199 The government should not only devote public resources to this fight, but also actively recruit, promote, and support assistance from private citizens, and provide resources that will incentivize such a program. n200 A. Problems with the Current Enforcement Regime 1. Public Resources Alone Are Not Enough Public resources alone will be insufficient to combat the environmental challenges that the United States now faces. n201 The federal and state governments and their agencies are simply ill equipped to effectively ascertain, ad-dress, and reverse the environmental problems now being confronted. n202 [*217] The government lacks sufficient financial resources to adequately address all of the threats to the environment, and even if it had adequate resources, its scope of **expertise is inadequate.** n203 In fact, the government's resources are so limited that it cannot even enforce the statutory regulations that it currently has in place by addressing every reported violation. n204 **It is nearly impossible**, for example, for the Environmental Protection Agency (EPA) to monitor every source of pollution or project that poses a threat to the environment. n205 Detecting such violations requires not only financial wherewithal, but also the **technical expertise** and understanding to clearly identify every breach of a statute or regulation. n206 Further, private resources appear to be necessary to combat the alignment of the economic interests of the federal government, the states, and private industry. n207 Many states attempt to foster a favorable operating arena for industry by engaging in a race to the bottom for lax environmental regulations meant lure businesses into their economies. n208 In such instances, state and private economic interests run counter the overall public welfare that the federal government is trying to protect. n209 Further, government agencies responsible for enforcing environmental statutes may also have deep ties to industry as a result of agency-capture, which run counter to the government's own goals. n210 **In order to account for these shortcomings**, **citizens must be given a more meaningful opportunity to assist in** the **enforcement of statutes** that protect public welfare. n211 2. The Inadequacy of Citizen Suit Provisions for Enforcement The government's current efforts to enlist private resources into the fight to protect the environment have primarily been made through citizen suit provisions. n212 Citizen suit provisions, however, have many weaknesses that largely [*218] render them ineffective at recruiting private resources that significantly aid in the protection of the environment. n213 One of the major problems with citizen suits is that they fail to sufficiently improve the public's ability to detect violations. n214 The moving party in most citizen suits is most often a large, well-funded private group, and such parties generally lack specific knowledge of wrongdoing by a given violator. n215 They must work to uncover violations just as any public agency or government prosecutor would. n216 Further, although citizen suits may add more eyes to look for alleged violations, they do not achieve the necessary effect of incentivizing those with actual knowledge of specific violations to come forward. n217 Citizen suits can also be ineffective because they have the potential to promote environmentally counterproductive cooperation between prosecutors, agencies and industry. n218 Hurdles contained in citizen suits, such as the requirement that a citizen suit be dropped if the government diligently prosecutes the matter, may foster lax enforcement. n219 This is because pro-industry governmental actors may simply pursue minimal corrective measures against an industry violator, inhibiting the full compliance generally sought in a successfully waged citizen suit. n220 Perhaps most importantly from the perspective of potential whistleblowers, citizen suits also fail to adequately incentivize whistleblowers and their counsels to engage in these suits by aligning their interests with the government's. n221 Citizen suits do not provide any financial reward to plaintiffs and merely provide injunctive relief or damages paid to the government. n222 In some [*219] cases, plaintiffs who bring these suits are even barred from even recovering attorney's fees, regardless of whether or not bringing the suit achieves the desired result. n223 B. Advantages of Whistleblower Programs Whistleblower programs provide assistance to the U.S. government and regulatory agencies by aligning public and private interests. n224 When private instruments of justice are undertaken in the interest of the common good, they can produce beneficial tools, such as legal talent, investigative resources, and inside information. n225 Wrongdoing can often be difficult to detect, and therefore, **an**

insider with intimate knowledge of a company or a potentially liable party's actions, **can be invaluable** in prosecuting enforcement actions without expending prohibitively large amounts of resources. n226

Impact – Nukes

Leaks key to make sure nuclear plants correct security and safety issues – bureaucracy and cover-ups make official channels useless – only we have empirics.

Sullivan 11 John, expert on nuclear power programs in the US and contributor for ProPublica. "Whistleblowers Say Nuclear Regulatory Commission Watchdog Is Losing Its Bite." 26 June 2011. https://www.propublica.org/article/whistleblowers-say-nuclear-regulatory-commission-watchdog-is-losing-its-bar. [Premier]

But rather than accept Mulley's findings, the inspector general's office rewrote them. The revised report shifted much of the blame to the plant's owner, Exelon, instead of NRC procedures. And instead of designating it a public report and delivering it to Congress, as is the norm, the office put it off-limits. A reporter obtained it only after filing a Freedom of Information Act request. The Fukushima nuclear disaster in Japan has thrust the NRC's role as industry overseer squarely in the spotlight, but another critical player in U.S. nuclear safety is the NRC's Office of the Inspector General, an independent agency that serves as watchdog to the watchdog. Now, Mulley and one other former OIG employee have come forth with allegations that the inspector general's office buried the critical Byron report and dropped an investigation into whether the NRC is relying on outdated methods to predict damage from an aircraft crashing into a plant. The inspector general's office, they assert, has shied away from challenging the NRC at exactly the wrong time, with many of the country's 104 nuclear power plants aging beyond their 40-year design life and with reactor meltdowns at Fukushima rewriting the definition of a catastrophic accident. "We're in the nuclear power business. It's not a trivial business; it's public health and safety," said Mulley, who won the agency's top awards and reviewed nearly every major investigation the office conducted before he retired as the chief investigator three years ago. "We have to have somebody that's going to look over the NRC's shoulder and make sure they were fulfilling their obligations," he said. Inspector General Hubert T. Bell declined to comment, but Joseph McMillan, the assistant inspector general for investigations, said the office has continued to vigorously pursue cases. He confirmed that the aircraft crash case has been closed but said it was proper. Regarding the Byron case, McMillan acknowledged disagreements but said: "I stand by the work we have done." The U.S. nuclear industry can point to an enviable safety record -- no member of the public has ever been injured by an accident at a plant. Nonetheless, critics point to issues like the NRC's drawn-out effort to enforce fire rules as evidence that the five-member commission and the agency it runs are **too close to the industry**. The inspector general's office has traditionally filled a key oversight role, conducting dozens of investigations that have changed how the NRC regulates nuclear waste, fire protection and security, among other things. Its regular reports to Congress cover waste, fraud and agency performance. Many federal agencies have similar independent offices to ferret out wrongdoing and improve efficiency. The NRC's was established in 1989 and has been led for the past 15 years by Bell, who was appointed by President Clinton after nearly three decades in the Secret Service. 'Everything Seems to Die' In the office's history, Mulley has left a big mark. For years, he documented how the NRC **dropped the ball** on the handling of nuclear fuel and security in nuclear plants. His reports on defective fire barriers led to congressional hearings and ultimately to a **complete overhaul of** the agency's **fire** protection **regulations**. He retired in 2008 as a senior-level assistant for investigations but continued work as an OIG consultant for two more years. Before he retired, Bell and a deputy wrote that Mulley was "so thorough and knowledgeable of all aspects of investigations, that even NRC management recognizes the value added to having Mr. Mulley's expertise on all cases." Mulley is not alone in his concerns about the inspector general's office. Another former employee told ProPublica that the office has become reluctant to probe **anything that could be** come **controversial** or raise difficult questions for the NRC. "They don't want to do anything," said the ex-employee, who left out of dissatisfaction with the direction of the office and asked not to be named to protect his current job. "Everything just seems to die." The former employee told ProPublica that the OIG's office had dropped an inquiry in to whether the NRC could accurately predict the damage to a plant from an airplane crash, and Mulley confirmed his account, saying the office received a tip in 2007 that the NRC was using an **outdated method**. Because a **wrong prediction could lead to insufficient protection** for the plants, the inspector general's office opened an investigation, Mulley said. "We went to several experts who said that thing is antiquated, you can't use it," he said. Mulley said that the NRC's experts insisted that their method was accurate. He said the aim of the investigation was not to prove that the NRC experts were wrong but to show there was a dispute and question whether the NRC should update its predictions. "In my mind, the OIG was not going to resolve it," he said. "It raised a valid question." The 2001 terrorist attacks drew attention to the potential hazard of an aircraft crash for nuclear plants, and afterward the NRC and nuclear industry examined whether new precautions were needed. The main industry trade group, the Nuclear Energy Institute, commissioned studies that showed U.S. plants could sustain a direct hit from a modern airliner without any radiation release. Following 9/11, the NRC adopted a rule requiring nuclear operators to take steps to minimize possible damage from major natural disasters or an aircraft crash. Two years ago, the commission required new licensees to assess whether their reactors could withstand an airliner crash. Eliot Brenner, an NRC spokesman, said the agency's method of evaluating the risk to plants has been thoroughly checked and relies on "realistic threat parameters." McMillan said that OIG completed its investigation into the crash prediction issue and that the case was closed to the file, meaning that **no report was issued**. The decision to forgo a report usually means that the inspector general found **no** public **safety concerns**. McMillan declined to comment on the report or to describe any conclusions. He said it was available only through a Freedom of Information Act request, which ProPublica filed today. The Byron Plant's Rusty Pipe On Oct. 19, 2007, a worker using a wire brush to clean a thick coating of rust from the massive steel pipe **ripped completely through** the metal. Water shot out, triggering a 12-day shutdown of the plant's two reactors located outside Rockford, Ill. The 24-inch pipe was part of the plant's Essential Service Water System, a network of eight huge pipes that carries water to cool emergency equipment. During an accident, it can be critical because it protects the generators and pumps that keep the reactor from overheating. "It's a safety-related system," Mulley said. "If it doesn't operate, you can't operate the plant." After the pipe ruptured, the NRC assigned a special inspection team to find out whether Exelon could have prevented it. Mulley put together a four-person team to start a parallel investigation into whether the NRC inspectors should have caught the problem beforehand. His team interviewed workers and NRC inspectors assigned to the Byron plant since the early 1990s. They concentrated heavily on the inspectors' actions in 2007, when Byron engineers began scrutinizing pipe sections, called risers, that were partly buried in concrete in a below-ground vault. Plant engineers performed ultrasonic tests on the thickness of the risers. Originally, the pipe walls were three-eighths of an inch thick, but over the span of three tests, engineers stepped the acceptable thickness down to three-hundredths of an inch -- equivalent to seven sheets of paper. Mulley's team found that the NRC's on-site inspectors **had not checked** the Byron **engineers' work** even though repeated drops in safety margin should have been a red flag. Corrosion in Byron's essential water system had been discussed in plant meetings, and because testing the risers required repeated use of a crane to gain access, inspectors should have suspected something. "The NRC is supposed to -- if they're overseeing this thing -- take a look at it and say, 'Oh, wait a minute, what's going on?'" Mulley said. "But obviously, they didn't look at that one." Mulley found that NRC's on-site inspectors had repeated opportunities to check the pipes over the years but had not done so. In interviews, the inspectors told Mulley's investigators that they had been busy with other work. Although inspectors had preformed a required number of equipment checks, Mulley's report found that their inability to set priorities was a weakness in the inspection program. The NRC, it turns out, had received a warning about a similar pipe break at the Vendellos nuclear plant in Spain, Mulley's team discovered. Peter B. Lyons, then an NRC commissioner, had even mentioned the Vendellos break in a speech, saying the agency was on top of the problem. But the word was never sent to NRC inspectors in the field, Mulley found. "I don't think anybody up there was purposely saying, 'Hey, this is not so important,'" Mulley said of the Vendellos information. "I think they knew it was important. I think they intended to. I don't think anybody followed up on it, and then it falls into the cracks." Report Revised, Kept From Public Because the Byron incident touched broadly on NRC inspection policies, Mulley opened his case as an Event Inquiry -- a report normally intended for release to Congress and the public. He stayed on after retirement to complete it, submitting it in 2009 with some tough conclusions. The NRC "provided little meaningful regulatory oversight of corrosion of piping in the Byron essential service water system, one of Byron's most risk significant systems," his version states. Moreover, the NRC "did not take full advantage of lessons learned" from Vendellos. Mulley said no one raised questions. " The report languished for a year," he said. "Nobody ever got back to me once to let me know, although I emailed them asking what's going on, what's happening with this thing." Then, in September 2010, the inspector general's office issued a new version. Mulley's draft had been **thoroughly rewritten**, and although the

facts were similar, the conclusions were not. The report said NRC oversight "was not successful" and that guidance for inspectors "was not specific enough," but pointedly blamed Exelon for the inspectors' failings. "Although the (NRC) resident inspectors carried out routine oversight responsibilities in accordance with agency requirements, the licensee's failure to analyze a problem correctly resulted in the resident inspector's lack of awareness of a significant problem," it states. By contrast, Mulley's version squarely faults NRC inspectors and procedures. "From 2000 to 2007, the NRC did not conduct any documented inspection activity of essential service water piping," it states, while inspectors "provided no regulatory review ... to support the licensee's lowering of the acceptable minimum wall thickness" in the piping. The revised report did not mention Vendellos or the NRC's failure to inform inspectors about it. And instead of being issued publicly, the report was classified for internal use only. "I was amazed," Mulley said. "This had never happened before in all my years." Mulley said the official report left out systemic problems his team uncovered and was not published so that shortcomings in NRC oversight would be hidden from the public and Congress. "I think changes that could have been made, pressure that could have been applied to improve the process, improve our oversight, are not going to be done," Mulley said. 'We Stand by the Report' Byron Nuclear Plant (Jeff Haynes/AFP/Getty Images)Brenner, the NRC spokesman, said the commission has upgraded procedures as a result of its own review of the Byron incident. In particular, he said inspectors were told to prioritize inspections of areas that had limited access and of equipment that repeatedly degraded, like the pipes at Byron. McMillan declined to answer any specific questions about the Byron report because the matter has been referred to the Council of the Inspectors General on Integrity and Efficiency, which has the authority to investigate allegations of wrongdoing against inspectors general. He said he believed the Byron case was handled appropriately. "We can have disagreements over how the reports are handled," he said, "but at the end of the day, we stand by the report." A spokesman for the council's integrity committee said he could not comment. Marshall Murphy, an Exelon spokesman, also declined to comment. The company previously has said it improved procedures after the pipe rupture at Byron. The significance of a strong, independent inspector general is not lost on the NRC, which is struggling with how to respond to the Fukushima accident after a special agency task force called for a potentially far-reaching reworking of regulations covering catastrophic events. Commission Chairman Gregory Jaczko, who has come under fire recently for pushing too fast on reforms, reflected on the inspector general's role in a statement last month. The office, Jaczko said, "plays an important role in enabling the American people to continue to have confidence that my focus as chairman -- and the entire agency's focus -- is on effectively carrying out the NRC's vital safety mission." Mulley said that mission is too vital for him to remain silent. "I am coming forward because I spent my entire life, most of my professional life, doing this," he said. "We get the power to write these reports, we get the power to talk to you. We've got the power to go to (Capitol) Hill, at least keep it in line a little bit as much as we can." **We can't be every place but at least try to keep them in line and** I think **it's vital**.

Accidents at nuclear reactors risk extinction – meltdowns outweigh nuke war.

Lendman 11 Stephen Lendman (Research Associate of the Centre for Research on Globalization). "Nuclear Meltdown in Japan." The People's Voice. 13 March 2011. http://www.thepeoplesvoice.org/TPV3/Voices.php/2011/03/13/nuclear-meltdown-in-japan. [Premier]

For years, Helen Caldicott warned it's coming. In her 1978 book, "Nuclear Madness," she said: "As a physician, I contend that nuclear technology threatens life on our planet with **extinction**. If present trends continue, the air we breathe, the food we eat, and the water we drink will soon be contaminated with enough radioactive pollutants to pose a potential health hazard far greater than any plague humanity has ever experienced." More below on the inevitable dangers from commercial nuclear power proliferation, besides added military ones. On March 11, New York Times writer Martin Fackler headlined, "Powerful Quake and Tsunami Devastate Northern Japan," saying: "The 8.9-magnitude earthquake (Japan's strongest ever) set off a devastating tsunami that sent walls of water (six meters high) washing over coastal cities in the north." According to Japan's Meteorological Survey, it was 9.0. The Sendai port city and other areas experienced heavy damage. "Thousands of homes were destroyed, many roads were impassable, trains and buses (stopped) running, and power and cellphones remained down. On Saturday morning, the JR rail company" reported three trains missing. Many passengers are unaccounted for. Striking at 2:46PM Tokyo time, it caused vast destruction, shook city skyscrapers, buckled highways, ignited fires, terrified millions, annihilated areas near Sendai, possibly killed thousands, and caused a nuclear meltdown, its potential catastrophic effects far exceeding quake and tsunami devastation, almost minor by comparison under a worst case scenario. On March 12, Times writer Matthew Wald headlined, "Explosion Seen at Damaged Japan Nuclear Plant," saying: "Japanese officials (ordered evacuations) for people living near two nuclear power plants whose cooling systems broke down," releasing radioactive material, perhaps in far greater amounts than reported. NHK television and Jiji said the 40-year old Fukushima plant's outer structure housing the reactor "appeared to have blown off, which could suggest the containment building had already been breached." Japan's nuclear regulating agency said radioactive levels inside were 1,000 times above normal. Reuters said the 1995 Kobe quake caused $100 billion in damage, up to then the most costly ever natural disaster. This time, from quake and tsunami damage alone, that figure will be dwarfed. Moreover, under a worst case core meltdown, all bets are off as the entire region and beyond will be threatened with permanent contamination, making the most affected areas unsafe to live in. On March 12, Stratfor Global Intelligence issued a "Red Alert: Nuclear Meltdown at Quake-Damaged Japanese Plant," saying: Fukushima Daiichi "nuclear power plant in Okuma, Japan, appears to have caused a reactor meltdown." Stratfor downplayed its seriousness, adding that such an event "does not necessarily mean a nuclear disaster," that already may have happened - the ultimate nightmare short of nuclear winter. According to Stratfor, "(A)s long as the reactor core, which is specifically designed to contain high levels of heat, pressure and radiation, remains intact, the melted fuel can be dealt with. If the (core's) breached but the containment facility built around (it) remains intact, the melted fuel can be....entombed within specialized concrete" as at Chernobyl in 1986. In fact, that disaster killed nearly one million people worldwide from nuclear radiation exposure. In their book titled, "Chernobyl: Consequences of the Catastrophe for People and the Environment," Alexey Yablokov, Vassily Nesterenko and Alexey Nesterenko said: "For the past 23 years, it has been clear that **there is a danger greater than nuclear weapons** concealed within nuclear power. Emissions from this one reactor **exceeded a hundred-fold** the radioactive contamination of the bombs dropped on Hiroshima and Nagasaki." "No citizen of any country can be assured that he or she [they] can be protected from radioactive contamination. **One** nuclear **reactor can pollute half the globe**. Chernobyl fallout covers the entire Northern Hemisphere." Stratfor explained that if Fukushima's floor cracked, "it is highly likely that the melting fuel will burn through (its) containment system and enter the ground. This has never happened before," at least not reported. If now occurring, "containment goes from being merely dangerous, time consuming and expensive to nearly impossible," making the quake, aftershocks, and tsunamis seem mild by comparison. Potentially, millions of lives will be jeopardized. Japanese officials said Fukushima's reactor container wasn't breached. Stratfor and others said it was, making the potential calamity far worse than reported. Japan's Nuclear and Industrial Safety Agency (NISA) said the explosion at Fukushima's Saiichi No. 1 facility could only have been caused by a core meltdown. In fact, 3 or more reactors are affected or at risk. Events are fluid and developing, but remain very serious. The possibility of an extreme catastrophe **can't** be discounted. Moreover, independent nuclear safety analyst John Large told Al Jazeera that by venting radioactive steam from the inner reactor to the outer dome, a reaction may have occurred, causing the explosion. "When I look at the size of the explosion," he said, "it is my opinion that there could be a very large leak (because) fuel continues to generate heat." Already, Fukushima way exceeds Three Mile Island that experienced a partial core meltdown in Unit 2. Finally it was brought under control, but coverup and denial concealed full details until much later. According to anti-nuclear activist Harvey Wasserman, Japan's quake fallout may cause nuclear disaster, saying: "This is a very serious situation. If the cooling system fails (apparently it has at two or more plants), the super-heated radioactive fuel rods will melt, and (if so) you could conceivably have an explosion," that, in fact, occurred. As a result, massive radiation releases may follow, impacting the entire region. "**It could be** literally **an apocalyptic event**. The reactor could blow." If so, Russia, China, Korea and most parts of Western Asia will be affected. Many thousands will die, potentially millions under a worse case scenario, including far outside East Asia. Moreover, at least five reactors are at risk. Already, a 20-mile wide radius was evacuated. What happened in Japan can occur anywhere. Yet Obama's proposed budget includes $36 billion for new reactors, a shocking disregard for global safety. Calling Fukushima an "apocalyptic event," Wasserman said "(t)hese nuclear plants have to be shut," let alone budget billions for new ones. It's unthinkable, he said. If a similar disaster struck California, nuclear fallout would affect all America, Canada, Mexico, Central America, and parts of South America.

Cybersecurity

Link – Overreach

NSA surveillance of American companies undercuts cybersecurity by building in vulnerabilities.

Kehl 14 Danielle Kehl is a Policy Analyst at New America's Open Technology Institute. "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity." New America's Open Technology Institute. 19 July 2014. https://www.newamerica.org/oti/policy-papers/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/. [Premier]

In addition to influencing standards-setting bodies, the NSA also goes straight to American and international tech companies to ensure that it can exploit vulnerabilities in their products. The NSA spends $250 million a year—more than 20 times what it spends on the much-discussed PRISM program—on a project to develop relationships with companies in order to weaken standards and convince them to insert backdoors into their products. According to documents released by ProPublica, the NSA's SIGINT Enabling Project "actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection."262 The Fiscal Year 2013 budget documents indicate that the goals of the project include inserting vulnerabilities into commercial encryption systems, IT networks, and communications devices as well as making it easier to exploit next generation encryption used for 4G wireless networks. The documents reference "continued partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses" and other relationships with commercial IT providers.263 One of the goals for that year is to "shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS [Central Security Service]."264 Programs like SIGINT Enabling are a central piece of the NSA's covert strategy to weaken commercial encryption, demonstrating how the agency switched from a public approach for a government mandate in the 1990s to developing a set of private partnerships with the tech industry over the past two decades. "Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on," explains Bruce Schneier. "If the back door is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program."265

Beyond SIGINT Enabling, the NSA appears to have other programs aimed at leveraging private sector relationships to insert and maintain vulnerabilities in commercial products as well. According to The Guardian, the NSA's Commercial Solutions center—the program which offers technology companies an opportunity to have their security products assessed and presented to prospective government buyers266—is also quietly used by the NSA to "leverage sensitive, co-operative relationships with specific industry partners" to insert vulnerabilities into those security tools.267 Similarly, a general classification guide details the relationships between industry partners and the NSA, as well as the agency's ability to modify commercial encryption software and devices to "make them exploitable" and obtain otherwise proprietary information about the nature of company's cryptographic systems.268 Even before SIGINT Enabling was disclosed, The Guardian reported that the NSA worked with Microsoft directly to circumvent the encryption on popular services including Skype, Outlook, and SkyDrive,269 although Microsoft denies those allegations.270 New information has also come to light about

backdoors planted in foreign-bound network routers from companies like Cisco, apparently without the knowledge of the companies that sell them.271 Cisco CEO John Chambers also spoke out after the May 2014 revelations that the NSA had inserted backdoors into network routers, writing a letter to the Obama Administration asking it to curtail the NSA's surveillance activities and institute reforms that rein in its seemingly-unchecked power.272 In a blog post, Cisco's Senior Vice President Mark Chandler wrote, "We comply with US laws… we ought to be able to count on the government to then not interfere with the lawful delivery of our products in the form in which we have manufactured them. To do otherwise, and to violate legitimate privacy rights of individuals and institutions around the world, undermines confidence in our industry."273

The existence of these programs, in addition to undermining confidence in the Internet industry, creates real security concerns. The SIGINT Enabling budget request suggests that the secrecy of the endeavor acts as a safeguard against any security concerns about the manufactured vulnerabilities, including an assurance that "to the consumer and other adversaries, however, the systems' security remains intact."274 This assertion relies on the false assumption that if the program is not made public, then others will never discover or exploit those vulnerabilities—and that the program's benefits outweigh the cost.275 Stephanie Pell, a non-resident fellow at the Center for Internet and Society at Stanford Law School and a former prosecutor at the Department of Justice, explains in a recent paper that "building in back door access…inevitably produces security vulnerabilities" because such back doors "create additional 'attack surfaces.'"276 And as security researcher Dr. Susan Landau noted in testimony to Congress, "building wiretapping [capabilities] into communications infrastructure creates serious risk that the communications system will be subverted either by trusted insiders or skilled outsiders, including foreign governments, hackers, identity thieves and perpetrators of economic espionage.277 Furthermore, creating a back door in an encrypted communications service requires access to the unencrypted data, which means that "if and when security flaws in the system are discovered and exploited, the worst case scenario will be unauthorized access to users' communications… [W]hen compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users."278

The fact that only the NSA was supposed to know about these backdoors does not alleviate the concerns. Matthew Green, a cryptography researcher at Johns Hopkins University, warned in The New York Times that "the risk is that when you build a back door into systems, you're not the only one to exploit it," since anyone else who discovers the weakness, including U.S. adversaries, can exploit it as well.279 These risks are not theoretical; there are numerous examples where technologies intended to facilitate lawful intercepts of communications have created additional vulnerabilities and security holes that have been exploited by unauthorized actors.280 As the white paper from the Institute of Electrical and Electronics Engineers concludes, "While the debate over how we should value both privacy and security is important, it misses a critical point: The United States might have compromised both security and privacy in a failed attempt to improve security."281

Link – Trust

Backdoors have created a truth problem between the NSA and private companies – they aren't willing to follow standards for security.

Sasso 14 Brandan Sasso, technology reporter for National Journal. and National Journal. "The NSA Isn't Just Spying on Us, It's Also Undermining Internet Security." The Atlantic. 29 April 2014. https://www.theatlantic.com/politics/archive/2014/04/the-nsa-isnt-just-spying-on-us-its-also-undermining-internet-security/457038/. [Premier]

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."•

The White House's cybersecurity coordinator said that disclosing security flaws "usually makes sense."

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. The National Security Agency (NSA) headquarters at Fort Meade, Maryland (AFP/Getty Images)

"When you want to go into partnership with somebody and work on serious issues — such as cybersecurity — you want to know you're being told the truth,"• Black said.

Google and one other cybersecurity firm discovered "Heartbleed"• — a critical flaw in a widely used Internet encryption tool — in March. The companies notified a few other private-sector groups about the problem, but no one told the U.S. government until April.

"Information you share with the NSA might be used to hurt you as a company,"• warned Ashkan Soltani, a technical consultant who has worked with tech companies and helped The Washington Post with its coverage of the Snowden documents.

He said that company officials have historically discussed cybersecurity issues with the NSA, but that he wouldn't be surprised if those relationships are now strained. He pointed to news that the NSA posed as Facebook to infect computers with malware.

"That does a lot of harm to companies' brands,"• Soltani said.

The NSA's actions have also made it difficult for the U.S. to set international norms for cyberconflict. For several years, the U.S. has tried to pressure China to scale back its cyberspying operations, which allegedly steal trade secrets from U.S. businesses.

Jason Healey, the director of the Cyber Statecraft Initiative at the Atlantic Council, said the U.S. has "militarized cyber policy."•

"The United States has been saying that the world needs to operate according to certain norms,"• he said. "It is difficult to get the norms that we want because it appears to the rest of the world that we only want to follow the norms that we think are important."•

Vines, the NSA spokeswoman, emphasized that the NSA would never hack into foreign networks to give domestic companies a competitive edge (as China is accused of doing).

"We do not use foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of — or give intelligence we collect to — U.S. companies to enhance their international competitiveness or increase their bottom line,"• she said.

Jim Lewis, a senior fellow with the Center for Strategic and International Studies, agreed that NSA spying to stop terrorist attacks is fundamentally different from China stealing business secrets to boost its own economy.

He also said there is widespread misunderstanding of how the NSA works, but he acknowledged that there is a "**trust problem** — justified or not."•

He predicted that rebuilding trust with the tech community will be one of the top challenges for Mike Rogers, who was sworn in as the new NSA director earlier this month.

Link – China Coop

NSA overreach makes cyber-surveillance cooperation with China impossible.

Donohue 18 Lauren, Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law. "High Technology, Consumer Privacy, and U.S. National Security." *Symposium Articles*, American University Business Law Review, 4(1). 2018. https://digitalcommons.wcl.american.edu/aublr/vol4/iss1/3/. [Premier]

Online warfare between China and the United States simmered in the background, until in early 2013 the Obama Administration began to make it center stage. In January 2013, the New York Times reported that Chinese hackers had infiltrated its computers following a threat that if the paper insisted on publishing a story about its prime minister, consequences would follow.17 The following month, a security firm, Mandiant, revealed that the Chinese military unit 61398 had stolen data from U.S. companies and agencies.118 In March 2013 President Obama's National Security Advisor publicly **urged China to reduce its surveillance efforts**-after which classified documents leaked to the public demonstrated the extent to which China had infiltrated U.S. government servers. Two months later, the National Security Advisor flew to China to lay the groundwork for a summit, in which cyber surveillance would prove center stage. Two days before the Obama-Xi meeting was scheduled to take place, The Guardian ran the first story on the NSA programs. On June 7, when Obama raised the question of Chinese espionage, Xi responded by quoting The Guardian and suggesting that the **U.S. should not be lecturing the Chinese about surveillance**. Although differences may mark the two countries' approaches (e.g., in one case for economic advantage, in the other for political or security advantage), the **broader translation** for the global community has been one in which the **United States has lost the high ground to try to restrict cyber-surveillance.**

A final point is worth noting in this context. To the extent that non-U.S. companies are picking up customers and business overseas, the United States' ability to conduct surveillance may be further harmed-thus going directly to the country's national security interests. In other words, it may be in the country's best interests to keep traffic routed through U.S. companies, which would allow the national security infrastructure, with appropriate legal process, to access the information in question. The apparent **overreach of the NSA**, however, may end up driving much of the traffic elsewhere, making it harder for the United States to **obtain the information needed to protect the country** against foreign threats.

Chinese cyberattack is likely - will shut down US power grids and critical infrastructure

Lenzner 14 Robert Lenzner is National Editor of Forbes magazine. "Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid." Forbes. 28 November 2014. http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid. [Premier]

Welcome to the increasingly dangerous world of cyber-warfare. The latest nightmare; a western intelligence agency of unknown origin (according to the Financial Times of London) is infecting the internet service providers and sovereign telecoms operations of Russia, Saudi Arabia, Iran, Mexico and

Ireland. To what end is not known, though the cyber security company Symantec calls the malware extremely sophisticated.

Then, there are the criminal elements, who have been hacking into the credit card details of JP Morgan Chase (76 million customers' names), and retailers like Home Depot, Target and EBay. Or the attempts going on by ne'er-do-well nations to break down the control of energy plants and factories, at times by criminal elements that act like stalking horses for sovereign nations up to no good.

I wrote about this phenomenon a decade ago for Forbes magazine ("The Next Threat") and raised the problem of private industry, especially public utilities, needing to invest major capital into establishing cyber defenses against the very real possibility that our enemies could break into the internet connections of urban public utilities and cause chaos and massive economic injury by closing down the public's access to electricity. Threats existed as well against the operations of infrastructure projects like dams, gas pipelines and transportation systems.

A DOD research facility in New Mexico plainly showed me how the nation's public utility system could be penetrated and closed down via their internet connection. Apparently, we have made little or no progress in the past decade of defending our artificial light and energy.

It appears that our enemies (read competitors) have made exceedingly greater progress in their sophisticated cyber-warfare techniques than we have achieved in defending ourselves. Now comes Admiral Michael Rogers, the head of the National Security Agency and the U.S. Cyber Command, who **warned last week that China and perhaps two other unnamed nations had "the ability to launch a cyber attack that could shut down the entire U.S. power grid and other critical infrastructure."**

Such a dire possibility should well have gotten a wider prominent play in the media. Yet Admiral Rogers underscored that software detected in China could seriously damage our nation's economic future by interfering with the electric utility power companies that the citizens of New York, Dallas, Chicago, Detroit and other urban centers require as the basic life blood of survival. This possibility is a great deal more dangerous than stealing 76 million names from JP Morgan Chase.

This not a Sci-Fi fantasy being perpetrated as a hoax on the American public. The NSA head flatly predicted that "it is only a matter of the when, not the if, that we are going to see something traumatic." He admitted NSA was watching multiple nations invest in this dangerous capability. He called the danger a "coming trend," where our vulnerability will be equivalent to a hole in our software systems that are unseen by the multinational company, the public utility, the telecom giant, the defense manufacturer, the Department of Defense.

NATO took the threat seriously enough to organize mock cyber-wargame trials in Estonia several days ago that indicated the western nations are aware of the need to fight on a new battlefield where the enemy cannot be seen physically. It was the largest digital warfare exercise ever attempted, a trial run to test dealing with a new non-military threat to global security.

Consider the financial damage to our nation from an attack that could shut down the power systems of major cities. As Forbes pointed out a decade ago, there was a very great need to spend the money building firewalls around our infrastructure's internet communications network. We are in worse shape today, since NSA chief Rogers plainly told the congressional intelligence committee last week "the

Chinese intelligence services that conduct these attacks have little to fear because we have no practical deterrents to that threat."

The cyber threat is real. America had better wake up to the need to defend the cogwheels of our economy from the electronic reconnaissance attacking our industrial control systems. Public opinion needs to be aroused by the media and security officials into a threat that no one can see as it is invisible. It is not Soviet missiles we fear, but inroads by nation states and criminal elements fronting for them. Our cyber command capabilities are as crucial as our Special Forces in beating back ISIS and other Islamic terrorists.

Impact – Grid

Grid attacks take out command and control – causes retaliation and nuclear war

Tilford 12 Robert, 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-coa. [Premier]

To make matters worse a cyber attack that can take out a civilian power grid, for example could also cripple 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 (see video: Pentagon declares war on cyber attacks http://www.youtube.com/watch?v=_kVQrp_D0kY&feature=relmfu). 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.

Soft Power

Link – Credibility

Restricting NSA surveillance is key to soft power – current surveillance is destroying US credibility

Donahue 14 Eileen, visiting scholar at Stanford University's Freeman Spogli Institute for International Studies, former U.S. ambassador to the United Nations Human Rights Council. "Why the NSA undermines national security." Reuters. 6 March 2014. http://blogs.reuters.com/great-debate/2014/03/06/why-nsa-surveillance-undermines-national-security/. [Premier]

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.

Unrestrained NSA surveillance undermines US soft power and prevents it from maintaining influence amid shrinking material power gap.

Quinn 13 Adam, Senior lecturer in international politics at the University of Birmingham in Birmingham, Britain. "NSA revelations threaten Obama's soft power and America's global influence." CS Monitor. 29 October 2013. http://www.csmonitor.com/Commentary/Opinion/2013/1029/NSA-revelations-threaten-Obama-s-soft-power-and-America-s-global-influence. [Premier]

For presidents, like sports-team managers, the tough weeks tend to outnumber the jubilant. But even by the standards of an unforgiving job, Barack Obama could be forgiven for feeling unusually buffeted of late. Many of the blows have come on the domestic front, with the all-consuming stand-off of the government shutdown segueing into frantic efforts to defend and repair the roll-out of Obamacare amid charges of fatal technological incompetence. But if he were tempted to seek solace in the autonomy of foreign policy – as modern presidents have been wont to do – there has been little consolatory triumph to be found. In August and September, he was caught in a mighty tangle over Syria, threatening military strikes over its chemical weapons use before being hamstrung first by Britain's refusal to join the charge and then by the reluctance of his own Congress. The legacy of that mess continues to work itself out in unpredictable ways, such as increasingly public tensions between the United States and Saudi Arabia, hitherto one of its more solid allies. Though the eventual Russian-orchestrated deal to remove Syria's chemical weapons was a respectable one given the circumstances, the episode as a whole spoke of an America straining to translate its power into influence, or to maintain, a united front among its friends. Recommended: 3 views on NSA reform Now the rolling scandal over National Security Agency (NSA) surveillance, triggered by the mass leak of secrets by Edward Snowden, has entered another phase of intensity, this time centered on Europe. Revelations that the US tapped the phone of German Chancellor Angela Merkel, operated numerous "listening posts" on European soil, and sucked up vast quantities of communications data from millions of citizens across Europe have broken in the press. Public expressions of displeasure have been forthcoming, including a European Union statement. Taken together, these vignettes of public dissension will be enough to make many ask the question: Is the US losing its influence even over its allies? Is this just a tricky moment for a particular president, or is it a harbinger of a broader trend? 3 views on NSA reform GALLERY Monitor Political Cartoons PHOTOS OF THE DAY Photos of the weekend Global shift First, the necessary caveats: Enduring alliance relationships resemble long marriages, in that the mere presence of moments of strain, or even audible arguments, cannot be taken as evidence of imminent separation. Looking back over the longer-term history of America's relations with its allies, episodes such as the Vietnam War, the "Euromissile" crisis of the 1980s, and the controversial interventions in the former Yugoslavia in the 1990s demonstrate that sharp differences of opinion and conflicting priorities are no radical, new state of affairs. And however unhappy they may be with their recent treatment, it is not obvious that countries such as Germany, France, or Saudi Arabia have anywhere to go if they did decide the time had come to tout for alternative alliance partners. It is not entirely clear how European annoyance might manifest in ways that have practical importance. It is true the Europeans have it in their power to threaten progress on the Transatlantic Trade and Investment Partnership process, but it is not clear that such an action would harm the US more than Europe itself. In short, even if they are disgruntled, necessity may ultimately prove a sufficient force to help them get over it. The reason present friction between the US and its allies carries greater weight, however, is that it arises in the context of a global shift in power away from the US and its established allies and toward new powers. The prospect of "American decline" in terms of relative international power is the focus of a great deal of debate over both substance and semantics. But the central fact is that even the part of the US's own intelligence apparatus charged with long-term foresight regards it as established that, within 20 years, the world will have transitioned from the "unipolar" American dominance of the first post-cold war decades to a world in which multiple centers of power must coexist. The center of economic gravity has already shifted markedly toward Asia during the last decade. This certainly does not mean any

single new power is about to rise to replace the US as a hegemonic force. Nor does it mean the US will be going anywhere: The scale of its existing advantages across a range of fronts – military, economic, institutional – is sufficiently great that it is assured a prominent place at the table of whatever order may come. What it does mean is that Americans must presently be engaged in thinking carefully about how best to leverage their advantages to retain the maximum possible influence into the future. If they cannot continue to be first among equals in managing the world order, they will wish at least to ensure that order is one that runs in line with their own established preferences. Soft power Many of those who are optimistic about the ability of the US to pull off this project of declining power without declining influence place emphasis on two things: the extent to which the US has soft power due to widespread admiration for its political and cultural values, and the extent to which it has locked in influence through the extent of its existing networks of friends and allies. Even if these advantages cannot arrest America's decline on harder metrics, if played properly, they can mitigate its consequences and secure an acceptable future. Shoring up support from like-minded countries such as those of Europe ought to be the low-hanging fruit of such an effort. So the current problems do harm on both fronts. It will be difficult to maintain the allure of soft power if global opinion settles on the view that American political discord has rendered its democracy dysfunctional at home, or that its surveillance practices have given rein to the mores of a police state. And it will be harder to preserve American status through the force of its alliances if its politicians' economic irresponsibility (for example, publicly contemplating a default on American national debt) or scandals over surveillance or drone strikes alienate their public or cause their leaders to question the extent to which they really are on the same side as the US.

Link – Propoganda

NSA metadata collection hurts US soft power – it's used for propaganda by competitors

Arkedis 13 Jim, senior fellow at the Progressive Policy Institute. "PRISM is bad for American soft power." The Atlantic. 19 June 2013. http://www.theatlantic.com/international/archive/2013/06/prism-is-bad-for-american-soft-power/277015/. [Premier]

There was a foreign policy angle to Truman's civil rights awakening, too. In the ideological battle pitting democracy against communism, the Soviet Union began to churn out propaganda saying that Jim Crow proved America's inability to live up to its own fundamental values on human rights. The argument was effective, argues Caley Robertson of Colby University: segregation was frustrating the United States' attempts to export democracy during the Cold War. In other words, Jim Crow was damaging America's soft power, defined by Harvard professor Joseph Nye as a country's ability to achieve its aims through attraction rather than coercion. Which brings us to PRISM, the NSA program that collects meta-data from Americans' telephone and online communications. I am a former Department of Defense intelligence analyst. I have never used PRISM, and do not know if it existed during my tenure. However, I have used NSA databases, and became aware of two ironclad truths about the agency: First, its data is a critical intelligence tool; and second, that access to databases by non-NSA intelligence analysts is highly controlled. It's like buying drugs (so I'm told): you need "a guy" on the inside who passes you the goods in the shadows, then disavows any connection to you. In addition to being useful and tightly controlled, PRISM is, of course, legal by the letter of the law. Its existence is primarily justified by the "business records" clause in the PATRIOT Act, and President Obama has argued that the legislation has been authorized by "bipartisan majorities repeatedly," and that "it's important to understand your duly elected representatives have been consistently informed on exactly what we're doing." Salvation from excessive government snooping would seem to lie at the ballot box. Fair enough. But in the immediate wake of September 11, Americans questioned little of what their government would do to keep them safe. Just four months after the attacks in January 2002, Gallup reported that fully half of Americans would support anti-terrorism measures even if they violated civil liberties. Times have changed. As soon as August 2003, Gallup found just 29 percent of Americans were willing to sacrifice civil liberties for security. By 2009, a CBS poll concluded only 41 percent of Americans had even heard or read about the PATRIOT Act, and 45 percent of those believed the law endangered their civil liberties. A Washington Post poll from April 2013--after the Boston marathon attacks but before PRISM's disclosure-- found 48 percent of Americans feared the government would go too far in compromising constitutional rights to investigate terrorism. And following the Edward Snowden leaks, 58 percent were against the government collecting phone records. Not a total reversal, but certainly trending in one direction. This shift has existed in a vacuum of public debate. Prior to the PRISM leaks, the last time domestic government surveillance made headlines was in very late 2005 and early 2006, following revelations that the Bush administration was wiretapping Americans without a warrant. Despite the scandal, the PATRIOT Act was quickly reauthorized by March 2006. The Bush administration did announce the end of warrantless wiretapping in 2007, and he moved the program under jurisdiction of the FISA court , a panel of Supreme Court-appointed judges who approve domestic surveillance requests. To call the FISA court a rubber stamp is an understatement. This year, it has rejected a grand total of 11 warrant requests out of--wait for it--33,996 applications since the Carter administration. The PATRIOT Act's reauthorization wouldn't come up again until 2009. By then, public uproar over warrantless wiretapping had long since receded, and the year's debate played out as a relatively quite inside-baseball scuffle between civil liberties groups and the Hill. When the law came up for its next presidential signature in 2011, it was done quietly by autopen--a device that imitates Obama's John Hancock--from France. Shifting attitudes and quiet reauthorization flies in the face of the standard the president has set for himself. In a 2009 speech at the National Archives, Obama emphasized the importance of the consent of the governed in security affairs, "I believe with every fiber of my being that in the long run we cannot keep this country safe unless we enlist the power of our most fundamental values... My administration will make all information available to the American people so that they can make informed judgments and hold us accountable." The president's inability to live up to this ideal is particularly jarring as he defends PRISM. Following the leaks, he's said he is pushing the intelligence community to release what it can, and rightly insists that the NSA is not listening in on Americans' phone calls. Those are helpful steps, but should have been raised during the National Archives speech just months into his administration, not six months into his second term. Director of National Intelligence James Clapper continues to argue that disclosure of collection methods will give America's enemies a "'playbook' to avoid detection." That's thin gruel. First, America's enemies are already aware of the NSA's extensive electronic

surveillance capabilities. That's why Osama Bin Laden and deceased al Qaeda in Iraq leader Abu Musab al Zarqawi used a complex network of couriers rather than electronic communications. It's typical operational security of truly dangerous operatives. Second, Obama stated as recently as late May that the threat from al Qaeda's core operatives has decreased significantly, shifting to less deadly cells scattered throughout the Middle East and North Africa. The lack of public debate, shifting attitudes towards civil liberties, insufficient disclosure, and a decreasing terrorist threat demands that collecting Americans' phone and Internet records must meet the absolute highest bar of public consent. It's a test the Obama administration is failing. This brings us back to Harry Truman and Jim Crow. Even though PRISM is technically legal, the lack of recent public debate and support for aggressive domestic collection is hurting America's soft power. The evidence is rolling in. The China Daily, an English-language mouthpiece for the Communist Party, is having a field day, pointing out America's hypocrisy as the Soviet Union did with Jim Crow. Chinese dissident artist Ai Wei Wei made the link explicitly, saying "In the Soviet Union before, in China today, and even in the U.S., officials always think what they do is necessary... but the lesson that people should learn from history is the need to limit state power." Even America's allies are uneasy, at best. German Chancellor Angela Merkel grew up in the East German police state and expressed diplomatic "surprise" at the NSA's activities. She vowed to raise the issue with Obama at this week's G8 meetings. The Italian data protection commissioner said the program would "not be legal" in his country. British Foreign Minister William Hague came under fire in Parliament for his government's participation.

Impact – Diplomacy

Soft power is necessary to solve transnational problems – provides diplomatic solutions

Nye 18 Joseph S. Nye, Jr is a professor at Harvard and served until recently as North American chair of the Trilateral Commission. "Asia after Trump." ASPI Strategist. 10 April 2018. https://www.aspistrategist.org.au/asia-after-trump/. [Premier]

The following year, David Rockefeller and Zbigniew Brzezinski created the Trilateral Commission, which meets once a year to discuss such problems. Contrary to conspiracy theories, the commission has little power; but, like other informal channels of 'track two' diplomacy, it allows private citizens to explore ways to **manage thorny issues**. The results can be found in its publications and on its website.

In Singapore, there was no consensus about Asia after Trump. For example, Indian and Chinese members held different positions about the role of China's 'Belt and Road' infrastructure projects. Some Asians and Americans differed over the prospects for a successful resolution of the **Korean nuclear crisis**, as well as the larger question of whether a **China–US war** is inevitable. And some Europeans wondered whether the current global uncertainty reflects the rise of China or the rise of Trump.

My own guess, which I warned the group might be wrong, is that **the US can recover its leadership after** the **Trump** years if it relearns the lessons of using power with others as well as over others. In other words, the US will have to use its **soft power** to create networks and institutions that will allow it to cooperate with China, India, Japan, Europe and others to **deal with transnational problems**—for example, **monetary stability, climate change, terrorism and cybercrime**—that no country can solve unilaterally. That will require overcoming the unilateral policies and attitudes associated with the rise of Trump.

The US can overcome the damage Trump has done to soft power

Nye 18 Joseph S. Nye, Jr is a professor at Harvard and served until recently as North American chair of the Trilateral Commission. "Asia after Trump." ASPI Strategist. 10 April 2018. https://www.aspistrategist.org.au/asia-after-trump/. [Premier]

A country's soft power comes primarily from three sources: its culture (when it is attractive to others), its political values such as democracy and human rights (when it lives up to them), and its policies (when they are seen as legitimate because they are framed with some humility and awareness of others' interests). How a government behaves at home (for example, protecting a free press), in international institutions (consulting others and multilateralism) and in foreign policy (promoting development and human rights) can affect others by the influence of its example. In all of these areas, Trump has reversed attractive American policies.

Fortunately, America is **more than** either **Trump or the government**. Unlike hard-power assets (such as armed forces), many soft-power resources are separate from the government and are only partly

responsive to its purposes. In a liberal society, government cannot control the culture. Indeed, the absence of official cultural policies can itself be a source of attraction. Hollywood movies like The Post, which showcase independent women and press freedom, can attract others. So, too, can the charitable work of US foundations or the benefits of freedom of inquiry at American universities.

It is true that firms, universities, foundations, churches and other non-governmental groups develop soft power of their own which may reinforce or be at odds with official foreign policy goals. And all of these private sources of soft power are likely to become increasingly important in the global information age. That is all the more reason for governments to make sure that their own actions and policies create and reinforce rather than undercut and squander their soft power.

Domestic or foreign policies that appear hypocritical, arrogant, indifferent to others' views, or based on a narrow conception of national interests can **undermine soft power**. For example, the steep decline in the attractiveness of the US in opinion polls conducted after the invasion of Iraq in 2003 was a reaction to the Bush administration and its policies, rather than to the US generally.

The Iraq War was not the first government policy that made the US unpopular. In the 1970s, many people around the world objected to the US war in Vietnam, and America's global standing reflected the unpopularity of that policy. When the policy changed and the memories of the war receded, the US recovered much of its lost soft power. Similarly, in the aftermath of the Iraq War, the US managed to recover much of its soft power in most regions of the world (though less so in the Middle East).

Skeptics might still argue that the rise and fall of American soft power does not matter much, because countries cooperate out of self-interest. But this argument misses a crucial point: cooperation is a matter of degree, and the degree is affected by attraction or repulsion. Moreover, the effects of a country's soft power extend to non-state actors—for example, by aiding or impeding recruitment by terrorist organisations. In an information age, success depends not only on whose army wins, but also on whose story wins.

One of the greatest sources of America's soft power is the **openness of its democratic processes**. Even when mistaken policies reduce its attractiveness, **America's ability to criticise and correct its mistakes makes it attractive** to others at a deeper level. When protesters overseas were marching against the Vietnam War, they often sang 'We Shall Overcome', the anthem of the US civil rights movement.

America, too, will almost certainly overcome. Given past experience, there is every reason to hope that the **US will recover its soft power after Trump**.

Efficiency

Link – Cost

Experts agree – squo surveillance is counterproductive and wastes money

Ward 15 Stan. "NSA swamped with data overload also trashes the Constitution." Best VPN. 18 May 2015. https://www.bestvpn.com/blog/19187/nsa-swamped-with-data-overload-also-trashes-the-constitution/. [Premier]

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 to 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 Peter, Journalist for The Intercept. "Inside NSA, Officials Privately Criticize "Collect It All" Surveillance." The Intercept. 28 May 2015. https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/. [Premier]

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."

Link – Info Overload

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

Gross 13 Grant, reporter for PC World. "Critics question whether NSA data collection is effective." PC World. 25 June 2013. http://www.pcworld.com/article/2042976/critics-question-whether-nsa-data-collection-is-effective.html. [Premier]

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 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.

Democracy

Link – Hypocrisy

Excessive surveillance destroys U.S. freedom –Has impacts world wide

Clarke 13 Richard A Clarke, former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. "Liberty and Security in a Changing World." 12 December 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. [Premier]

Protecting Democracy, Civil Liberties, and the Rule of Law. Free debate within the United States is essential to the long-term vitality of American democracy and helps bolster democracy globally. Excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government. All parts of the government, including those that protect our national security, must be subject to the rule of law. Wholly apart from the Fourth Amendment, how should the United States treat non-United States persons when they are outside the United States? To understand the legal distinction between United States persons and non-United States persons, it is important to recognize that the special protections that FISA affords United States persons grew directly out of a distinct and troubling era in American history. In that era, the United States government improperly and sometimes unlawfully targeted American citizens for surveillance in a pervasive and dangerous effort to manipulate domestic political activity in a manner that threatened to undermine the core processes of American democracy. As we have seen, that concern was the driving force behind the enactment of FISA. Against that background, FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse within our own political system. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact special restrictions on government surveillance of those persons who participate directly in its own system of self-governance. As an aside, we note that the very existence of these protections in the United States can help promote and preserve democratic accountability across the globe. In light of the global influence of the United States, any threat to effective democracy in the United States could have negative and far-reaching consequences in other nations as well. By helping to maintain an effective system of checks and balances within the United States, the special protections that FISA affords United States persons can therefore contribute to sustaining democratic ideals abroad.

Further, this hypocrisy has created the conditions that will accelerate the global rise of authoritarianism.

Chenoweth and Stephan 15 Erica Chenoweth, political scientist at the University of Denver.& Maria J. Stephan, Senior Policy Fellow at the U.S. Institute of Peace, Senior Fellow at the Atlantic Council. "How Can States and Non-State Actors Respond to Authoritarian Resurgence?" Political Violence @ a Glance. 7 July 2015. http://politicalviolenceataglance.org/2015/07/07/how-can-states-and-non-state-actors-respond-to-authoritarian-resurgence/. [Premier]

Chenoweth: Why is authoritarianism making a comeback? Stephan: There's obviously no single answer to this. But part of the answer is that democracy is losing its allure in parts of the world. When people don't see the economic and governance benefits of democratic transitions, they lose hope. Then there's the compelling "stability first" argument. Regimes around the world, including China and Russia, have readily cited the "chaos" of the Arab Spring to justify heavy-handed policies and consolidating their grip on power. The "color revolutions" that toppled autocratic regimes in Serbia, Georgia, and Ukraine inspired similar dictatorial retrenchment. There is nothing new about authoritarian regimes adapting to changing circumstances. Their resilience is reinforced by a combination of violent and non-coercive measures. But authoritarian paranoia seems to have grown more piqued over the past decade. Regimes have figured out that "people power" endangers their grip on power and they are cracking down. There's no better evidence of the effectiveness of civil resistance than the measures that governments take to suppress it—something you detail in your chapter from my new book. Finally, and importantly, democracy in this country and elsewhere has taken a hit lately. Authoritarian regimes mockingly cite images of torture, mass surveillance, and the catering to the radical fringes happening in the US political system to refute pressures to democratize themselves. The financial crisis here and in Europe did not inspire much confidence in democracy and we are seeing political extremism on the rise in places like Greece and Hungary. Here in the US we need to get our own house in order if we hope to inspire confidence in democracy abroad.

American surveillance is the primary driver behind this authoritarian acceleration. The plan is necessary to restore US credibility.

Jackson 15 Dean Jackson is an assistant program officer at the International Forum for Democratic Studies. "The Authoritarian Surge into Cyberspace." International Forum For Democratic Studies. 14 July 2015. http://www.resurgentdictatorship.org/the-authoritarian-surge-into-cyberspace/. [Premier]

This still leaves open the question of what is driving authoritarian innovation in cyberspace. Deibert identifies increased government emphasis on cybersecurity as one driver: cybercrime and terrorism are serious concerns, and governments have a legitimate interest in combatting them. Unfortunately, when democratic governments use mass surveillance and other tools to police cyberspace, it can have the effect of providing cover for authoritarian regimes to use similar techniques for repressive purposes—especially, as Deibert notes, since former NSA contractor Edward Snowden's disclosure of US mass surveillance programs. Second, Deibert observes that authoritarian demand for cybersecurity technology is often met by private firms based in the democratic world—a group that Reporters Without Borders (RSF) calls the "Corporate Enemies of the Internet." Hacking Team, an Italian firm mentioned in the RSF report, is just one example: The Guardian reports that leaked internal documents suggest Hacking Team's clients include the governments of "Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia, and the United Arab Emirates." Deibert writes that "in a world where 'Big Brother' and 'Big Data' share so many of the same needs, the political economy of cybersecurity must be singled out as a major driver of resurgent authoritarianism in cyberspace." Given these powerful forces, it will be difficult to reverse the authoritarian surge in cyberspace. Deibert offers some possible solutions: for starters, he writes that the "political economy of cybersecurity" can be altered through stronger export controls, "smart sanctions," and a monitoring system to detect abuses. Further, he recommends that cybersecurity trade fairs open their doors to civil society watchdogs who can help hold governments and the private sector accountable. Similarly, Deibert suggests that opening regional cybersecurity initiatives to civil society participation could mitigate violations of user rights. This might seem unlikely to occur within some authoritarian-led intergovernmental organizations, but setting a normative expectation of civil society participation might help discredit the efforts of bad actors. Deibert concludes with a final recommendation that society develop "models of cyberspace security that can show us how to prevent disruptions or threats to life and property without sacrificing liberties and rights." This might restore democratic states to the moral high ground and remove oppressive regimes' rhetorical cover, but developing such models will require confronting powerful vested interests and seriously examining the tradeoff

between cybersecurity and Internet freedom. Doing so would be worth it: the Internet is far too important to cede to authoritarian control.

Link – Autonomy

The loss of autonomy due to surveillance enables "turnkey totalitarianism" which threatens democracy.

Haggerty 15 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. December 2014. https://www.cambridge.org/core/books/world-without-privacy/1D4B6F436CB09B6EFD498E418C86F7E7. [Premier]

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.

Blocks

AT: Terrorism

Empirically false – 215 program once temporarily ended and it didn't create risks.

Globe and Mail 15 Globe editorial. "The end of US 'bulk telephony collection,' and the lessons for Canada." The Globe and Mail. 14 June 2015. http://www.theglobeandmail.com/globe-debate/editorials/the-end-of-us-bulk-telephony-collection-and-the-lessons-for-canada/article24948261/. [Premier]

For a few days, there was a happily yawning gap in the U.S. **N**ational **S**ecurity **A**gency**'s** ability to surveil American citizens. Congress could not agree on how – or whether – to renew the section of the foolishly named Patriot Act that had allowed the government to scoop up and hold all the metadata (identifying both callers and addressees) of all cellphone calls in the U.S. The Foreign Intelligence Surveillance Court would then grant or, at least sometimes, not grant, access to the actual contents of the conversations – in other words, a search warrant. The upshot – under the new U.S.A. Freedom Act (officially, the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015") – is that phone companies, not the NSA and the FBI, will record and store all the metadata for all phone calls. Those agencies will no longer be able to get at that kind of data at will, indiscriminately. The security agencies will have to apply to the FISC court for metadata, too. That's progress, though FISC may be a bit of a rubber stamp. **There is,** by the way, **no sign that terrorists attacked the United States in the unsurveilled interval between the Patriot Act section and the Freedom Act.**

US losing the war on terror.

Miller 15 Greg Miller, quoting Director of National Intelligence James R. Clapper Jr.,Intelligence reporter for the Washington Post; former national security correspondent for the Los Angeles Times and co-author of The Interrogators: Inside the Secret War against al Qaeda. "In campaign against terrorism, U.S. enters period of pessimism and gloom." Washington Post. 7 March 2015. http://www.washingtonpost.com/world/national-security/in-campaign-against-terrorism-us-enters-period-of-pessimism-and-gloom/2015/03/07/ca980380-c1bc-11e4-ad5c-3b8ce89f1b89_story.html. [Premier]

In congressional testimony recently, Director of National Intelligence James R. Clapper Jr. went beyond the usual litany of threats to say that terrorism **trend lines were worse "than at any other point in history."** Maj. Gen. Michael Nagata, commander of U.S. Special Operations forces in the Middle East, told participants on a counter-terrorism strategy call that he regarded the Islamic State as a greater menace than al-Qaeda ever was. Speaking at a New York police terrorism conference, Michael Morell, former deputy director of the CIA, said he had come to doubt that he would live to see the end of al-Qaeda and its spawn. "This is long term," he said. "My children's generation and my grandchildren's generation will still be fighting this fight." The assessments reflect a pessimism that has descended on the U.S. counterterrorism community over the past year amid a series of discouraging developments. Among them are the growth of the Islamic State, the ongoing influx of foreign fighters into Syria, the collapse of the U.S.-backed government in Yemen and the downward spiral of Libya's security situation. The latest complication came Saturday, when the terrorist group Boko Haram in Nigeria carried out a series of suicide bombings and reportedly declared its allegiance to the Islamic State. Unlike the waves of anxiety that accompanied the emergence of new terrorist plots over the past decade, the latest shift in mood seems more deep-seated. U.S. officials depict a bewildering landscape in which al-Qaeda and the brand of Islamist militancy it inspired have not only survived 14 years of intense counterterrorism operations but have also spread. Officials emphasize that their campaign has accomplished critical goals. In particular, most officials and experts now see the risk of a Sept. 11-scale attack as infinitesimal, beyond the reach of al-Qaeda and its scattered affiliates. Still, the adjusted outlook contrasts sharply with the surge of optimism that followed the killing of Osama bin Laden in 2011 and the dawn of the Arab Spring, which was initially seen as a political awakening across the Middle East that might render al-Qaeda and its archaic ideology irrelevant. Within months of bin Laden's death, then-Defense Secretary Leon E. Panetta said he was convinced "that we're within reach of strategically defeating al-Qaeda." President Obama echoed that view in subsequent years by saying that al-Qaeda was on "a path to defeat" and, more recently, that the then-nascent Islamic State was analogous to a junior varsity sports team. Such **upbeat characterizations have all but evaporated.**

No link – targeted warrants, which plan allows, solve the terror disad just as well.

Wyden et al. 14 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." 9 September 2014. https://www.eff.org/document/wyden-udall-heinrich-smith-amicus. [Premier]

As members of the Senate Select Committee on Intelligence, amici Senators Wyden and Udall have for years participated in the oversight of government surveillance conducted under the Patriot Act that they knew would astonish most Americans. They sought to warn the public about those activities as best they could without disclosing classified information. They also co-sponsored an amendment to the Patriot Act's reauthorization that sought to address the problem of government officials "secretly reinterpret[ing] public laws and statutes" and "describ[ing] the execution of these laws in a way that misinforms or misleads the public." See 157 Cong. Rec. S3360 (daily ed. May 25, 2011) (introducing SA 384 to S. 990, 112th Cong. § 3 (2011)); see also 157 Cong. Rec. S3386 (daily ed. May 26, 2011) (statement of Sen. Wyden) ("The fact is anyone can read the plain text of the PATRIOT Act. Yet many Members of Congress have no idea how the law is being secretly interpreted by the executive branch."); 157 Cong. Rec. S3258 (daily ed. May 24, 2011) (statement of Sen. Udall) ("Congress is granting powers to the executive branch that lead to abuse, and, frankly, shield the executive branch from accountability"). Now that the government's bulk call-records program has been documented and exposed, the executive branch has retreated from frequently repeated claims about its necessity and expressed an intent to end government bulk collection under section 215. Press Release, FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m ("White House Press Release"). While Senators Udall, Heinrich and Wyden broadly support a policy aimed at ending the government's indiscriminate collection of telephony metadata, they share a concern that there is no plan to suspend the bulk collection of Americans' phone records in the absence of new legislation, which is not necessarily imminent. Meanwhile, the government continues to defend its bulk call-record collection program vigorously against statutory and constitutional challenges in the courts. Amici submit this brief to respond to the government's argument that its collection of bulk call records is necessary to defend the nation against terrorist attacks. Amici make one central point: as members of the committee charged with overseeing the National Security Agency's surveillance, amici have reviewed this surveillance extensively and **have seen no evidence** that the bulk collection of Americans' phone records has provided **any intelligence of value that could not have been gathered through means that caused far less harm to** the **privacy interests** of millions of Americans. The government has at its disposal a number of authorities that allow it to obtain the call records of suspected terrorists and those in contact with suspected terrorists. It appears to amici that these more targeted authorities could have been used to obtain the information that the government has publicly claimed was crucial in a few important counterterrorism cases.

NSA doesn't solve terrorism—their statistics are overblown

Cahall et al. 14 Bailey, David Sterman, Emily Schneider, Peter Bergen, Cahall is a Policy Analyst at New America Foundation. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America. 13 January 2014. https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/. [Premier]

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.

Cooperation garnered by soft power is more important than intelligence capabilities.

Donahoe 14 Eileen, Stanford University's Freeman Spogli Institute for International Studies visiting scholar. "Why the NSA undermines national security." Rueters. 6 March 2014. http://blogs.reuters.com/great-debate/2014/03/06/why-nsa-surveillance-undermines-national-security/. [Premier]

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.

AT: Terrorism – Recruitment

NSA is losing talent because of low pay and bureaucracy.

Doctorow 18 Cory Doctorow, Canadian-British blogger, journalist, and science fiction author who served as co-editor of the blog Boing Boing. "The NSA can't recruit or retain hackers because the pay sucks and the Agency is a bureaucratic mess BoingBoing. 3 January 2018. https://boingboing.net/2018/01/03/same-job-better-pay.html. [Premier]

The Washington Post reports that the NSA "is losing its top talent at a worrisome rate as highly skilled personnel" because of a mix of low-pay, uninspiring leaders, and a bureaucratic re-org that everyone hates.

There's a post-Snowden angle to all this, with people of good will walking away from the Agency, but the real story is that the NSA, like all US spy agencies, buys in billions of dollars worth of private service from outside contractors (both Snowden and Reality Winner were working for these contractors when they leaked internal documents in order to blow the whistle on illegal/immoral activity).

Anyone who doesn't like the NSA's hidebound rules, bumbling leaders and government pay-scales can go to work for a myriad of contractors, or set up shop on their own, and end up doing basically the same job they did for the NSA, for an order of magnitude more pay, and without any of those strictures.

What's more, those contractors aren't limited to working for the NSA, so if you're morally flexible enough, you get to do the same job for a different government, too, ensuring lots of glamorous travel and an bottomless fountain of cash.

Barnes also noted the allure of Silicon Valley and other cities that tech start-ups call home. The U.S. private sector is struggling to fill more than 270,000 jobs in cybersecurity, according to Burning Glass Technologies, a labor analytics firm. Total compensation for those jobs can reach $200,000 or more, meaning even relatively junior cyber professionals in the industry can make more than top officials at the NSA.

Some senior officials say that the outflow in part reflects a cultural shift in which millennials are not inclined to stay in one workplace for an entire career. And it also stems from a disproportionate number of retirements of people who entered the agency in the 1980s during a hiring boom.

Morale crashing *because* of rule-breaking.

Friedersdorf 13 Conor Friedersdorf is a staff writer at The Atlantic, where he focuses on politics and national affairs. "Do You Trust The Washington Post's Sources on Morale at the NSA?" The Atlantic. 10 December 2013. http://www.theatlantic.com/politics/archive/2013/12/do-you-trust-em-the-washington-post-em-s-sources-on-morale-at-the-nsa/282184/. [Premier]

After reading what these former officials had to say, Marcy Wheeler points out that NSA employees have a reason for low morale that has nothing to do with Obama's support:¶ Most of the NSA's employees have not been read into many of these programs ... That raises the distinct possibility that NSA morale is low not because the President hasn't given them a pep talk, but because they're

uncomfortable working for an Agency that violates its own claimed rules so often. Most of the men and women at NSA have been led to believe they don't spy on their fellow citizens. Those claims are crumbling, now matter how often the NSA repeats the word "target."

AT: Terrorism – Cooperation Turn

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. "Racial Profiling Reported in NSA, FBI Surveillance." U.S. News & World Report. 9 July 2014. http://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance. [Premier]

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.

Surveillance creates support for terrorism and undermines investigations — it stigmatizes Muslim communities and undermines global credibility.

El-Said 15 Hamid El-Said, Professor of International Relations at Manchester Metropolitan University, Advisor to the UN Counter-Terrorism Task Force, Ph.D. in Political Economy from the University of Jordan, BSc in Business and Demographic Studies from the University of Jordan, M.A. in Middle Eastern Studies from the University of London, M.A. in Development Studies from the University of Manchester. "In Defence of Soft Power: Why a "War" on Terror Will Never Win," *The New Statesman.* 4 February 2015, accessible online at http://www.newstatesman.com/politics/2015/02/defence-soft-power-why-war-terror-will-never-win. [Premier]

Although the EU and UN's "soft" approaches, which called for "addressing the conditions conducive to the spread of terrorism" in the first place, held great potential, they were watered down by the continued prevalence of hard military approach worldwide. The United States, for instance, has never bought into the "soft" approach and continued to follow a military strategy, despite noticeable change

in terminology. As a report by the Bipartisan Policy Center's National Security Preparedness Group concluded in 2001, the US government has shown little interest in "soft" counter radicalisation and de-radicalisation policies.

This is despite the fact that home-grown terrorism has become more prominent in America. The American government has also ironically been active in promoting "soft" de-radicalisation programmes abroad (such as in Afghanistan and Iraq), as well as the establishment of several regional centres and forums allegedly aimed at countering the global rise in violent extremism through "soft" power. This contradiction has undermined the **credibility** of the US as a **genuine leader** of, and believer in, the role of "soft" power in **countering violent extremism**, including the **upholding of the rule of law**, **freedom of expression**, and **respect for human rights.**

Even globally, the "soft" power approach remains the exception, not the rule. A report by the United Nations Counter Terrorism Implementation Task Force in late 2009 showed that no more than 30 out of 192 UN Member States injected some form of "soft" powers into their counter terrorism strategies. The rest continue to rely on a kinetic approach that is only capable of creating more hostilities and antagonism. Many of those countries are close allies of the US in its so-called war on terror.

Neither in Europe nor in North America did de-radicalisation (an extensive form of rehabilitation of violent extremist detainees) receive sufficient attention. The practice has been either to "deport" the "terrorists" or to detain them "forever" in individual cells. The value of rehabilitating the detainees to prepare them for peaceful reintegration into their societies with a minimum risk was lost. Many academics and observers, including the author, have repeatedly warned that the benefits of effective de-radicalisation policies go beyond prison bars to affect the whole community from whence the detainees came. No heed was paid. The upshot has been the kind of attacks that we recently experienced in Paris and Copenhagen, both of which were accomplished by former un-rehabilitated convicts.

Europe and America however showed more interest in counter radicalisation policies that seek to stem the rise of violent extremism at a societal level. Such policies included, among others, community engagement and community policing. Rather than "winning hearts and minds" by solving problems and showing interest, these were **intelligence-led**, causing them to be perceived by most Muslims as no more than **spying-tools targeting their communities.** This **undermined trust between Muslim communities and the police**, a prerequisite for successful collaboration and effective community engagement in **countering radicalisation** in society.

As a report by the Equality and Human Rights Commission Research concluded, counter radicalisation measures have turned "Muslims [into] . . . the new **suspect community**." This, the report added, has **stigmatised whole Muslim communities**, **fuelled resentment** and even **bolstered "support for terrorist movements."**

It is against this background that the recent rise in Islamophobia in Europe and North America should be understood. Islamophobia is reflected in an alarming increase in anti-Islamism in Western societies and rise in fatal attacks against Muslims, which hardly receive the attention they deserve from the Western media, and state officials, especially when compared to incidents when the victims are Westerners and the perpetrators are "Muslims".

Some Western countries have recently ramped up security measures in response to some terrorist acts. This will neither make us safer nor answer the important, still unanswered question of what led some individuals to choose a nihilistic view of life in Western societies. Arresting somebody or cancelling his or her passports will also not prevent new attacks, nor will it explain why such attacks were attempted in the first place. As Rep. Tulsi Gabbard (D.-Hawaii), and an Iraq combat veteran, stated: "This war cannot be won, this enemy and threat cannot be defeated unless we understand what's driving them, what is their ideology." That we have not done.

In sum, despite the much talked about role of "soft" counter de-radicalisation policies in countering violent extremism, such policies have never been given a genuine opportunity to succeed. It is not surprising therefore that the main aim of the current White House summit, which is taking place in Washington DC between 18-20 March, is to combat violent extremism through the "search for strategies that go beyond only military action for countering terrorists". Let's hope that the summit will provide an opportunity to reverse our misguided military approach to countering the phenomenon of "terrorism". Although it is doubtful.

Muslim reporting is key to stopping terrorism — they provide critical intel for counter-terrorism.

Esman 11 Abagail Esman, contributor to Forbes with 20 years' experience writing for national and international magazines including Salon.com, Vogue, Esquire, and more. "Should New York Muslims Cooperate With the Police - Or With The Terrorists?" *Forbes*. 21 November 2011. http://www.forbes.com/sites/abigailesman/2011/11/21/should-new-york-muslims-cooperate-with-the-police-or-with-the-terrorists/2/. [Premier]

There is a lot behind terrorism cases that police cannot disclose for fear of revealing investigative techniques or intelligence sources.

The truth is, much of what counterterrorism officials have learned over the years has been gleaned from members of the Muslim community who have spoken out to expose radicalism in their midst. (According to the Chattanooga Times Press, "A recent study by North Carolina's Triangle Center on Terrorism and Homeland Security credited tips from Muslim Americans with thwarting **48 of 120 terrorism cases** allegedly involving Muslim Americans over the past 10 years.") **Without their assistance, our safety is far less certain.**

But that is exactly what Muslim activists now urge fellow Muslims to do: resist cooperation with law enforcement, **putting national security greatly at risk.** According to the AP, at a "Know your Rights" session for Muslims based on the recent allegations, Ramzi Kassem, a professor of law (of all things!) at the City University of New York, advised, "Most of the time it's a fishing expedition, so the safest thing you can do for yourself, your family, and for your community, is not to answer."

Not to answer? If you see something, keep your mouth shut? It is safer, if you know that there is a good chance someone in your community plans to set off a bomb in Times Square, or near your own place of business, or your child's school, or your father's office in Manhattan, to say nothing? Is he kidding?

Apparently not. And this is what he and CAIR and others are entreating their fellow Muslims to do. Stand by the ummah, the Muslim community. Defend even the terrorists. Know where your loyalty stands.

Frightening stuff.

Certainly these are tender issues. But the fact is, we face, now, quandaries and threats our founding fathers couldn't possibly have imagined. It's been only ten years since the World Trade Center attacks, which, in the grand scheme of history, isn't very long. **We are clearly still stumbling here**, and likely will be for a while yet, with reconciling balances between security and freedom, and ten years simply is not enough time for us to resolve the conflicts that exist between them.

AT: Terrorism – Turns Case

No rollback — no increase in fear and the public doesn't trust the government. Boston bombing proves.

Hayes 13 Danny Hayes, associate professor of political science at George Washington University, focusing on political communication and political behavior. "Why the Boston Marathon bombing won't erode civil liberties." The Washington Post, 28 April 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/04/28/why-the-boston-maraton-bombing-wont-erode-civil-liberties/. [Premier]

From the moment that Boston bombing suspect Dzhokhar Tsarnaev was pulled out of a boat in Watertown, Mass., the debate over civil liberties and domestic anti-terrorism policies, largely dormant in recent years, was reignited.

Noting that "the homeland is the battlefield," Sen. Lindsey Graham (R-S.C.) urged the Obama administration to designate Tsarnaev, an American citizen, as an enemy combatant. Civil liberties groups then objected when authorities decided not to read Miranda rights to the Boston Marathon bombing suspect, invoking a public safety exception. Speculation also arose that police might now find it easier to persuade the public to support the use of surveillance technology and domestic drones. "After Boston," Ryan Gallagher wrote this week in Slate, "the balance in the struggle between privacy and security may swing back in their favor."

But research conducted shortly after 9/11, combined with some recent polling data, suggests that Americans may be unlikely to trade civil liberties for a greater sense of security as a result of the bombing. That's because the attack **hasn't made the public significantly more fearful** of future domestic terrorism, and because **trust in government is low**.

After 9/11, concern over terrorism skyrocketed. In a Gallup survey fielded in the days before the attack, less than one-half of one percent of Americans said terrorism was the country's most important problem. But in October 2001, 46 percent did. These worries boosted support for legislation, such as the USA PATRIOT Act, that expanded law enforcement's power to investigate suspected terrorism, even as those measures were criticized for eroding civil liberties protections.

In a survey conducted between November 2001 and January 2002, political scientists Darren Davis and Brian Silver designed a series of questions to explore the tradeoffs between security and civil liberties. They began by asking people whether they agreed more with the statement that "in order to curb terrorism in this country, it will be necessary to give up some civil liberties" or that "we should preserve our freedoms above all, even if there remains some risk of terrorism." Forty-five percent of Americans chose the first option, indicating a willingness to give up some freedoms in exchange for greater security.

When respondents were asked about the tradeoffs involving specific measures, there was wide variation. Davis and Silver found that very few Americans – eight percent – believed that the government should have the power to investigate people who participate in nonviolent protests. And just 18 percent said they supported racial profiling. But when asked, for instance, whether they agreed

that “high school teachers have the right to criticize America’s policies toward terrorism” or that “high school teachers should defend America’s policies in order to promote loyalty to our country,” 60 percent said teachers should back the government.

Perhaps not surprisingly, the biggest influence on whether people were willing to offer pro-security over pro-civil liberties responses was their fear of a second attack. Respondents who believed another terrorist act was imminent were more likely to support tradeoffs in favor of security. Importantly, Davis and Silver found that the relationship was strongest among people who expressed high levels of political trust: People who believe the government typically does the right thing and who were fearful of another terrorist attack were the most willing to relinquish civil liberties protections.

Those findings are consistent with a series of studies by Stanley Feldman, Leonie Huddy and their colleagues at Stony Brook University. In one survey conducted between October 2001 and March 2002, the researchers found that 86 percent of Americans said they were “very” or “somewhat” concerned about another domestic terrorist act. The greater the concern, the more likely respondents were to support the use of government-issued ID cards and allowing authorities to monitor phone calls and e-mail.

But in contrast to 9/11, polling since the Boston Marathon suggests that the bombing has made Americans only slightly more fearful of future terrorist attacks than they were beforehand. Fifty-eight percent of respondents in a Pew poll conducted April 18-21 said they were “very” or “somewhat” worried about another attack on the United States. That was no higher, however, than when the same question was asked in November 2010. And it was significantly lower than the 71 percent who said they were worried in October 2001.

A slightly different question in a Washington Post poll taken April 17-18 found that 69 percent of Americans said that the possibility of a major terrorist attack worried them either “a great deal” or “somewhat.” That figure was only a few percentage points higher than when the same question was asked in 2007 and 2008.

In addition, political trust is lower today than it was in 2001, when public confidence in government rose sharply after the terrorist attacks. If Davis and Silver’s findings are correct, then greater skepticism of government – produced in part by the struggling economy – **should limit the public’s willingness to give law enforcement more latitude**.

Ultimately, the scope of the Boston tragedy was smaller than 9/11, which could help explain its limited effect on the public. It may also be that because Americans believe terrorist attacks are now a **fundamental part of life in the United States**, any single event will have a more **muted effect on public opinion**. And because the Tsarnaev brothers have not been connected to any known terrorist organizations, Americans may feel less under siege than they did when al-Qaeda and Osama bin Laden were identified as the perpetrators of the 2001 attacks.

Regardless of the reason, all of this suggests that policymakers are likely to face a more difficult task than they did after 9/11 in persuading the public to support additional security measures that infringe on Americans’ freedoms.

AT: Terrorism – No Impact

Terror isn't a war-level threat.

Diab 15 Robert Diab is an Assistant Professor in the Faculty of Law at Thompson Rivers University, and specializes in Canadian and US national security law, criminal, and constitutional law, author of The Harbinger Theory: How the Post-9/11 Emergency Became Permanent and the Case for Reform. "Has ISIS become the new pretext for curtailing our civil liberties?" Oxford University Press's Academic Insights for the Thinking World. 1 June 2015. http://blog.oup.com/2015/06/isis-new-pretext-curtailing-civil-liberties/. [Premier]

A series of measures put in place in the years following 9/11 have now become a fixture of Western government: mass warrantless surveillance, longer periods of detention without charge, and greater state secrecy without accountability. The United States finds itself at the vanguard of this movement with its embrace of executive authority to carry out targeted killing of its own citizens. Many of these measures arose in part as an over-reaction to the threat of al Qaeda. But they were also due in part to a plausible concern that terrorism had come to pose a threat of a much greater magnitude than was previously thought possible. For many, terrorism had become closer in nature to war than to crime, justifying a host of invasive measures. Almost 15 years later, the continuing argument for those measures rests on the belief that terrorism still poses a threat tantamount to war. In the wake of recent attacks in Paris, Ottawa, and Sydney, governments have sought to make this argument by linking the threat of domestic terrorism to ISIS. The link is necessary because ISIS is now the only entity capable of serving as a plausible basis for the claim that jihadist terrorism continues to be potentially war-like in scale. The need to see terrorism on this scale to justify extraordinary measures points to an earlier shift in perceptions of terror. Prior to 9/11, terror on domestic soil was seen as a criminal act, regardless of its scale. Conventional prosecutions followed the Oklahoma City and Air India bombings, and earlier events involving the IRA and other political groups. After 9/11, terrorism in much of the West came to be understood in terms of what can be called the harbinger theory. This was a belief that 9/11 was not an anomaly in the history of terrorism, but the harbinger of a new order of terror — one in which future attacks on the part of al Qaeda or an analogous group would soon occur in a major Western city on a similar or greater scale, possibly involving weapons of mass destruction. It now seemed plausible that terrorism could involve tens or hundreds of thousand of casualties, even millions, the threat was comparable to war. As a consequence, for Dershowitz, Posner, and others, the conventional limits on state power in constitutional and human rights were no longer tenable. In the United States, the harbinger theory still forms a crucial basis for national security policy. Following the Snowden revelations, for example, President Obama defended the continuing use of bulk metadata surveillance by asserting: "the men and women at the NSA know that if another 9/11 or massive cyberattack occurs, they will be asked by Congress and the media why they failed to connect the dots." A bill before Congress purporting to overhaul the Patriot Act has been lauded for ending bulk data collection by the NSA. But to appease concerns about "another 9/11," it will retain the practice of bulk data collection by shifting it to third parties. The evidence of domestic terrorism in Western nations in recent years runs directly contrary to the harbinger theory. As Mueller and Stewart and others have shown, the future of terrorism is likely to be more like the pre-9/11 past: lone-wolves or small, disparate groups with more limited capabilities. Recent attacks in Paris, Ottawa, and Sydney confirm this. One of the principals in the

Charlie Hebdo killings had received training from an al Qaeda affiliate in Yemen in 2011, but little more. The men involved in the Ottawa and Sydney events were known to police and acted alone. Security. CC0 via Pixabay. Security. CC0 via Pixabay. Yet, in keeping with the harbinger theory, governments have been quick to draw a connection between recent terror and ISIS, a large transnational entity with greater capacity. In the wake of the attack on Parliament, Canada's Prime Minister Stephen Harper asserted: "The international jihadist movement has declared war…" The epicenter of the threat is the "entire jihadist army that is now occupying large parts of Iraq and Syria." The US and French governments have also tied ISIS to the prospect of further domestic terror, ignoring ample evidence that ISIS is, as Ahmed Rashid put it, "not waging a war against the West." Despite the tenuousness of a link to ISIS, Canada, France, and Australia have sought to justify significant new measures in light of it. Canada's bill C-51 gives security intelligence service the unprecedented power to seek a warrant to breach any Charter right — not only those protecting against unreasonable search and seizure — if believed to be necessary to thwart a terror plot. France is debating a mass surveillance bill, while Australia will likely adopt a law that strips terror suspects of citizenship. In each case we have to ask: What will the new powers accomplish? Would they have prevented attacks in Sydney, Ottawa, or Paris? Looking back, it's hard to see how. Even with full surveillance, it would likely have been impossible to know how far along the path of radicalization certain individuals were prepared to go, until they got there. Yet by maintaining the perception of domestic terrorism as part of a larger war, questions of cause and effect become moot, and de facto emergency powers persist.

AT: Terrorism – No Nuclear Terror

No risk of nuclear terrorism

Mearsheimer 14 John Mearsheimer, IR Prof at UChicago. "America Unhinged." National Interest. 2 January 2014. http://nationalinterest.org/article/america-unhinged-9639?page=show. [Premier]

Am I overlooking the obvious threat that strikes fear into the hearts of so many Americans, which is terrorism? Not at all. Sure, the United States has a terrorism problem. But it **is a minor threat**. There is no question we fell victim to a spectacular attack on September 11, but it did not cripple the United States in any meaningful way and another attack of that magnitude **is highly unlikely in the foreseeable future**. Indeed, there has not been a single instance over the past twelve years of a terrorist organization exploding a primitive bomb on American soil, much less striking a major blow. Terrorism—most of it arising from domestic groups—was a much bigger problem in the United States during the 1970s than it has been since the Twin Towers were toppled.

What about the possibility that a terrorist group might obtain a nuclear weapon? Such an occurrence would be a game changer, but **the chances of that happening are virtually nil**. No nuclear-armed state is going to supply terrorists with a nuclear weapon because it would have no control over how the recipients might use that weapon. Political turmoil in a nuclear-armed state could in theory allow terrorists to grab a loose nuclear weapon, but the **U**nited **S**tates **already has detailed plans to deal with that highly unlikely contingency.**

Terrorists might also try to acquire fissile material and build their own bomb. But **that scenario is extremely unlikely as well**: there are **significant obstacles to getting enough material and even bigger obstacles to building a bomb and then delivering it**. More generally, virtually **every country has a profound interest in making sure no terrorist group acquires a nuclear weapon**, because they cannot be sure they will not be the target of a nuclear attack, either by the terrorists or another country the terrorists strike. **Nuclear terrorism**, in short, **is not a serious threat**. And to the extent that we should worry about it, the main remedy is to encourage and help other states to place nuclear materials in highly secure custody.

AT: Terrorism – No Bioterror

No risk of bioterror.

Keller 13 Rebecca, Analyst at Stratfor. "Bioterrorism and the Pandemic Potential." Stratfor. 7 March 2013. http://www.stratfor.com/weekly/bioterrorism-and-pandemic-potential. [Premier]

The risk of an accidental release of H5N1 is similar to that of other infectious pathogens currently being studied. Proper safety standards are key, of course, and experts in the field have had a year to determine the best way to proceed, balancing safety and research benefits. Previous work with the virus was conducted at biosafety level three out of four, which requires researchers wearing respirators and disposable gowns to work in pairs in a negative pressure environment. While many of these labs are part of universities, access is controlled either through keyed entry or even palm scanners. There are roughly 40 labs that submitted to the voluntary ban. Those wishing to resume work after the ban was lifted must comply with guidelines requiring strict national oversight and close communication and collaboration with national authorities. The risk of release either through accident or theft cannot be completely eliminated, but given the established parameters **the risk is minimal**. The use of the pathogen as a biological weapon requires an assessment of whether a non-state actor would have the capabilities to isolate the virulent strain, then weaponize and distribute it. Stratfor has long held the position that while terrorist organizations may have rudimentary capabilities regarding biological weapons, the **likelihood** of a **successful attack** is **very low**. Given that the laboratory version of H5N1 -- or any influenza virus, for that matter -- is a contagious pathogen, there would be two possible modes that a non-state actor would have to instigate an attack. The virus could be refined and then aerosolized and released into a populated area, or an individual could be infected with the virus and sent to freely circulate within a population. There are **severe constraints** that make **success** using either of these methods **unlikely**. The technology needed to refine and aerosolize a pathogen for a biological attack is **beyond the capability** of most non-state actors. Even if they were able to develop a weapon, other factors such as **wind patterns** and **humidity** can render an attack **ineffective**. Using a human carrier is a less expensive method, but it requires that the biological agent be a contagion. Additionally, in order to infect the large number of people necessary to start an outbreak, the infected carrier must be mobile while contagious, something that is **doubtful** with a **serious disease** like small pox. The carrier also cannot be visibly ill because that would limit the necessary human contact.

AT: Insider Threats

Bulk collection makes NSA systems more vulnerable to insider hacks—multiple structural weaknesses

Bellovin 8 Steven M. Bellovin, Columbia University, Matthew A. Blaze. University of Pennsylvania. "Risking Communications Security: Potential Hazards of the Protect America Act." IEEE Society. 1 January 2008. https://www.computer.org/csdl/magazine/sp/2008/01/msp2008010024/13rRUwhpBCk. [Premier]

The US has also experienced difficulties with communications surveillance systems. Under the Communications Assistance for Law Enforcement Act (P.L. 100-667), the US Federal Bureau of Investigation (FBI) was responsible for determining technical specifications for wiretapping built into switches of digital telephone networks. DCS 3000, an FBI suite of systems for collecting and managing data from wiretaps for criminal investigations, was designed to meet those requirements. Recently released FBI documents reveal serious problems in the system's implementation.22 Its auditing system was primitive, surprising for a system intended for evidence collection. The system has no unprivileged user IDs, relying on passwords rather than token-based or biometric authentication, and even uses an outdated hashing algorithm (MD5 appears in a 2007 "system security plan,"23 several years after Chinese researchers found serious problems with this already weak hashing algorithm). Most seriously, the system relied on a single shared login, rather than a login per authorized user. The system's ability to audit user behavior depended entirely on following proper processes, including using a manual log sheet to show who was using the system at a given time. **Remote access**—in an insecure fashion—is permitted from other DCS 3000 nodes, making the system vulnerable to insider attacks. These are a real risk: recall that the most damaging spy in FBI history, Robert Hanssen, abused his authorized access to internal FBI computer systems to steal information and track progress of the investigation aimed at him. The problems in the DCS 3000 implementation illustrate the risks in building a communications surveillance system. We do not know whether DCS 3000 was merely poorly implemented or whether it was poorly specified. What were the requirements on the FBI system? Did they include full auditing and full user identity? What were the project's goals? Were the designers required to meet all requirements or goals? These are questions that should have been asked of the DCS 3000 designers—and should be asked of any builder of a communications surveillance system. Although the NSA has extensive experience in building surveillance systems, that does not mean **things can**not **go wrong.** When you build a system to spy on yourself, you entail an awesome risk. In designing a system to satisfy the needs of the Protect America Act, the risk is made worse by four phenomena: cation carriers in all previous interception programs within the US communication system. This protective role was the result of the specificity required in wiretap warrants. placing the system properly within the US rather than at US borders; likelihood that the system will be built out of **pieces previously used abroad**, which runs the risk that opponents are already **familiar with the equipment** via intelligence-sharing agreements or capture of equipment; and use of CDRs, originally built for network development purposes, in an entirely new way involving "customers" outside the phone company. These architectural decisions facilitate three distinct types of problems: system capture to enable spying on US traffic; system defeat by using information learned from foreign examples to defeat selection and filtering strategies; and system spoofing by similar means. All of these can be used not only to make the surveillance system less

effective, but also to turn it into a tool for capturing communications that are not implicated in any illegal activity—endangering **both security and privacy**. We see several specific risks as a result. **Risk of exploitation by opponents**. A system that accesses domestic communications necessarily poses a greater direct risk to the communications of Americans than a surveillance system fielded overseas. To avoid foreign familiarity with its operation, communication security equipment is not often shared with allies. However, engineering economy reuses systems previously fielded abroad; thus, both allies and opponents are likely to be familiar with US surveillance equipment. Is there a risk that knowledge of the surveillance system acquired by studying equipment outside the US will be applied to defeating or subverting similar equipment deployed within the US? Is the NSA designing sufficiently robust mechanisms to assure complete control of the filtering and selection mechanisms? Even prior to the Protect America Act, US communications were vulnerable to surveillance, but building signals intelligence systems is expensive. The system designed as a result of the Protect America Act must not reduce foreign powers' difficulty in gaining access to US communications. Can the communications of US persons be tapped without increasing the risk that these communications will be exploited by others without authorization to do so?

We're already losing the spy war and it's too late to alter our status—even if we could, the timeframe is decades.

Schindler 15 John R., security consultant and a former National Security Agency counterintelligence officer. "China's Spies Hit the Blackmail Jackpot With Data on 4 Million Federal Workers." The Daily Beast. 11 June 2015. http://www.thedailybeast.com/articles/2015/06/11/china-s-spies-hit-the-blackmail-jackpot-with-every-data-on-federal-worker.html. [Premier]

With each passing day the U.S. government's big hacking scandal gets worse. Just what did hackers steal from the Office of Personnel Management? Having initially assured the public that the loss was not all that serious, OPM's data breach now looks very grave. The lack of database encryption appears foolhardy, while OPM ignoring repeated warnings about its cyber vulnerabilities implies severe dysfunction in Washington. To say nothing of the news that hackers were scouring OPM systems for over a year before they were detected. It's alarming that intruders got hold of information about every federal worker, particularly because OPM previously conceded that "only" 4 million employees, past and present, had been compromised, including 2.1 million current ones. Each day brings worse details about what stands as the biggest data compromise since Edward Snowden stole 1.7 million classified documents and fled to Russia. Then there's the worrisome matter of what OPM actually does. A somewhat obscure agency, it's the federal government's HR hub and, most important, it's responsible for conducting 90 percent of federal background investigations, adjudicating some 2 million security clearances every year. If you've ever held a clearance with Uncle Sam, there's a good chance you're in OPM files somewhere. Here's where things start to get scary. Whoever has OPM's records knows an astonishing amount about millions of federal workers, members of the military, and security clearance holders. They can now target those Americans for recruitment or influence. After all, they know their vices, every last one—the gambling habit, the inability to pay bills on time, the spats with former spouses, the taste for something sexual on the side—since all that is recorded in security clearance paperwork. (To get an idea of how detailed this gets, you can see the form, called an SF86, here.) Speaking as a former counterintelligence officer, it really doesn't get much worse than this. Do you have

friends in foreign countries, perhaps lovers past and present? The hackers know all about them. That embarrassing dispute with your neighbor over hedges that nearly got you arrested? They know about that, too. Your college drug habit? Yes, that too. Even what your friends and neighbors said about you to investigators, highly personal and revealing stuff, that's in the other side's possession now. Perhaps the most damaging aspect of this is not merely that millions of people are vulnerable to compromise, through no fault of their own, but that whoever has the documents now so dominates the information battlespace that they can halt actions against them. If they get word that an American counterintelligence officer, in some agency, is on the trail of one of their agents, they can pull out the stops and create mayhem for him or her: Run up debts falsely (they have all the relevant data), perhaps plant dirty money in bank accounts (they have all the financials, too), and thereby cause any curious officials to lose their security clearances. Since that is what would happen. This disaster was **decades in the making** and will take **decades to set right**. Then there's the troubling matter of who's behind this mega-hack. U.S. intelligence sources haven't been particularly shy about pointing the finger at China, particularly at hacker groups that serve as cut-outs for Chinese intelligence and who are the suspected culprits behind several major online data breaches of the U.S. economy, including the health-care industry. What they're particularly looking for is information about Chinese nationals who have ties to Americans working in sensitive positions. Why Beijing wants that information isn't difficult to determine. Armed with lists of Chinese citizens worldwide who are in "close and continuing contact" (to cite security clearance lingo) with American officials, Beijing can now seek to exploit those ties for espionage purposes. And it will. While many intelligence services exploit ethnic linkages to further their espionage against the United States—Russians, Cubans, Israelis, even the Greeks—none of the major counterintelligence threats to America exploit ethnic ties as consistently as Beijing does. The OPM compromise, however it came about, represents a genuine debacle for Washington, one that will take many years to repair. Our intelligence community already faces serious and long-standing problems with counterintelligence, the Beltway's perennial redheaded stepchild, and this setback promises to make things exponentially worse. This is a new kind of threat, the melding of ancient counterespionage techniques with 21st-century technology, and we're playing catchup. The OPM hack, which is unprecedented in its scope, offers our adversaries the opportunity to penetrate our government and use that information to deceive it at a strategic level. This is the essence of SpyWar, the secret struggle between the West and adversaries like China, Russia, and Iran, a clandestine battle that never ceases, yet which the public seldom gets wind of, except when something goes wrong. The extent of the damage here appears so vast that all the counterintelligence awareness in the world may not be able to offset the advantage in the SpyWar that Beijing has won with this data theft. If you are or have been employed with the federal government and have listed Chinese nationals on your SF86, it's time to be vigilant, while anybody who's worked for the feds since the mid-1980s ought to be watching their credit reports for anomalies. Then there's the matter of the lives possibly ruined by this. Simply put, there has long been a tacit agreement: You keep the U.S. government's secrets safe, it will do the same for yours. That important promise, the bedrock upon which the security clearance process is based, has been violated, with serious consequences for millions of Americans—and for Washington. Counterintelligence hands warned of the threat posed by putting all sorts of sensitive information in such databases, but they were ignored. **It's too late to undo the damage**, but we must finally get serious about preventing the next big compromise, while mitigating the pain of this loss. This disaster was decades in the making and will take decades to set right. There's no time for back-biting. Honest assessment is what's required. There's a SpyWar on that needs to be won.

Underreporting—97% chance that insiders bypass monitoring and surveillance checks

Bunn and Sagan 14 Matthew Bunn, American nuclear and energy policy analyst, currently a professor of practice at the Harvard Kennedy School at Harvard University, and Scott Sagan. "A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes." the American Academy of Arts and Sciences. 2014. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf . [Premier]

Nuclear managers may assume that their systems for detecting red flags are much better—that they would surely catch someone like Hasan. But the case of Sharif Mobley suggests that this may not always be the case. In March 2010, Mobley was arrested in Yemen for alleged involvement in al-Qaeda and for shooting a guard in an attempt to escape. Yet between 2002 and 2008, prior to traveling to Yemen, Mobley worked at five U.S. nuclear power plants (Salem-Hope Creek, Peach Bottom, Limerick, Calvert Cliffs, and Three Mile Island), where he was given unescorted access inside the plant (though not in the vital areas) to perform maintenance and carry supplies. According to a Nuclear Regulatory Commission (NRC) report, Mobley voiced his militant views during his work, referring to non-Muslim coworkers as "infidels" and remarking to some in his labor union: "We are brothers in the union, but if a holy war comes, look out."24 Though the rules in place at the time required individual workers to report any suspicious behavior on the part of coworkers, none of Mobley's fellow union members apparently reported these statements. The red flags were again invisible. Cases of ignoring red flags as extreme as Hasan's, or even Mobley's, do not happen often. But the issues raised—failing to report problems because of the headaches involved, passing troublesome employees off to someone else— arise in smaller ways in almost every organization. Indeed, research suggests that indicators of insider security problems are **systematically underreported**.25 One study of several cases of insider information-technology sabotage in critical infrastructure found that **97 percent** of the insiders involved in the cases "came to the attention of supervisors or coworkers for concerning behavior prior to the attack," but **the observed behavioral precursors were "ignored by the organization**."26 All managers of nuclear organizations should be asking themselves: how are the incentives for reporting such issues really aligned in my organization? How could I test how well such issues are reported? How could I improve my organization's ability to detect and act on a potential problem before it occurs?s

AT: Circumvention

Reform in one area snowballs with other areas.

Patel 15 Faiza, co-director of the Brennan Center's Liberty and National Security Program. "When will surveillance reform stop being just 'cool'?" Brennan Center. 25 June 2015. www.brennancenter.org/blog/when-will-surveillance-reform-stop-being-just-'cool'. [Premier]

Last week, former National Security Agency Director Michael Hayden declared that he was "cool" with the recently enacted USA Freedom Act, which reined in government bulk collection of Americans' phone records. His characterization of that program as "little" is no doubt accurate. Information from the archive of documents released by NSA whistleblower Edward Snowden has revealed many other programs that pose equal or greater risks to Americans' privacy. But Hayden is too quick to assume that the phone records program will be the only reform. The passage of the USA Freedom Act is the first **curtailment of intelligence authorities** since the 9/11 attacks and should mark the beginning — not the end — of reform. It's no surprise that Congress chose to tackle the phone record program first. It is relatively straightforward for people to understand, and its goal of amassing a vast database of information about Americans is patently difficult to square with our constitutional values. Two review boards found it to be of minimal counterterrorism value, and a federal appeals court declared it illegal. Even the intelligence community and the president were amenable to reform. But Congress is well aware that this reform is insufficient. Many of the votes against the act in the House and Senate came from lawmakers who believe it didn't go far enough.

Circumvention won't happen if surveillance is prohibited.

Ackerman 15 Spencer, American national security reporter and blogger, national security editor for the Guardian. "Fears NSA will seek to undermine surveillance reform; Privacy advocates are wary of covert legal acrobatics from the NSA similar to those deployed post-9/11 to circumvent congressional authority." The Guardian. 1 June 2015. https://www.theguardian.com/us-news/2015/jun/01/nsa-surveillance-patriot-act-congress-secret-law. [Premier]

Despite that recent history, veteran intelligence attorneys reacted with scorn to the idea that NSA lawyers will undermine surveillance reform. Robert Litt, the senior lawyer for director of national intelligence, James Clapper, said during a public appearance last month that creating a banned bulk surveillance program was " not going to happen ".

"The whole notion that NSA is just evilly determined to read the law in a fashion contrary to its intent is bullshit, of the sort that the Guardian and the left - but I repeat myself - have fallen in love with. The interpretation of 215 that supported the bulk collection program was creative but not beyond reason, and it was upheld by many judges," said the former NSA general counsel Stewart Baker, referring to Section 215 of the Patriot Act.

This is the section that permits US law enforcement and surveillance agencies to collect business records and expired at midnight, almost two years after the whistleblower Edward Snowden revealed to the Guardian that the Patriot Act was secretly being used to justify the collection of phone records from millions of Americans.

With one exception, the judges that upheld the interpretation sat on the non-adversarial Fisa court, a body that approves nearly all government surveillance requests and modifies about a quarter of them substantially. The exception was reversed by the second circuit court of appeals.

Baker, speaking before the Senate voted, predicted: "I don't think anyone at NSA is going to invest in looking for **ways to defy congressional** intent if USA Freedom is adopted."

AT: Disease

Tech isn't getting used.

Landman 6-29 Keren Landman, practicing physician, epidemiologist, and journalist who covers topics in medicine and public health. "Hey America, What Happened to Contact Tracing?." Elemental. 29 June 2020. https://elemental.medium.com/hey-america-what-happened-to-contact-tracing-47a2dbccc020. [Premier]

Because of the concern that air travel could be an important contributor to Covid-19 transmission, the White House and the Centers for Disease Control and Prevention (CDC) have for months supported a plan requiring airlines to assist with contact tracing efforts by gathering and sharing certain passenger data with the CDC. Although a representative of the industry association Airlines for America wrote in an email that U.S. airlines "fully comply with all requests made by CDC for contact information," recent reports indicate that as of yet, no airlines are systematically communicating contact information for all travelers to the CDC. An interagency group hopes to reach a solution by early September.

Despite the early promise of technological tools to improve the efficiency of contact tracing efforts — and their broad use in other countries — the **onslaught of new tools** without much **guidance** on how to choose, use, and adapt them has made the tech landscape **deeply confusing** to public health officials **at all levels**. "They don't really have a good way to read, like a Consumer Reports magazine" that would help each state choose the best tool to suit its needs, says Freeman. Nevertheless, many state health departments have invested in tools, often **without consulting, training, or informing** their local health departments, she says — and the resulting chaos has led some local health departments to **abandon those tools outright.**

Surveillance is ineffective for COVID.

Gallagher 20 Ryan Gallagher, Journalist at Bloomberg. "Surveillance Technology Will Only Get More Intense After Covid." Bloomberg. 2 June 2020. https://www.bloomberg.com/news/articles/2020-06-02/what-could-the-nsa-do-with-coronavirus-surveillance-technology. [Premier]

Even if you accept privacy risk as a price worth paying, questions remain about how effective surveillance can be as a tool in the fight against Covid-19. According to authorities in Israel, their phone tracking methods have so far helped identify more than 4,000 verified coronavirus cases in the country. But trials of similar technology elsewhere have provided **little evidence of success.**

"The lure of automating the painstaking process of contact tracing is apparent. But to date, no one has demonstrated that it's possible to do so reliably despite numerous concurrent attempts," concluded researchers at the Brookings Institution in April. "No clever technology—standing alone—is going to get us out of this unprecedented threat to health and economic stability."

Many of the approaches governments are taking have never been tried before. We are lab rats in a technological experiment, and it may take years before we learn the results. In some countries, forms of digital surveillance will undoubtedly provide some useful insights, helping epidemiologists to better understand the spread of the virus. In others, governments will use the moment to expand the reach of

invasive technology, with **little benefit to the pandemic recovery**. Both of these outcomes, like the virus itself, will leave a legacy felt by future generations.

It's not topical and the NSA isn't set up to conduct it.

Devine 20 Michael E. Devine, Analyst in Intelligence and National Security. "Intelligence Community Support to Pandemic Preparedness and Response." Congressional Research Service. 6 May 2020. https://crsreports.congress.gov/product/pdf/IF/IF11537/2. [Premier]

Yet in extenuating circumstances could IC capabilities, such as geospatial products and services, support domestic efforts to respond to a pandemic? The only explicit E.O. 12333 exception allowing the IC to conduct domestic collection of information not constituting foreign intelligence, which could conceivably involve support to a pandemic response, is the authority to conduct overhead (satellite or airborne) surveillance "no**t directed** at specific United States persons." The NGA, for example, has previously provided support to the Federal Emergency Management Agency (FEMA).

Therefore, while the IC has surveillance capabilities, it is **not currently well positioned** to provide added benefit to the capabilities of national, state and local public health authorities in a domestic context. Supplemental appropriations measures have included CDC funding for public health surveillance and disease detection both domestically and globally. **Public health surveillance is not an intelligence activity**, however. Rather, it applies to nonintelligence activities, such as health data collection, by national, state, and local health entities. Certain HHS biosurveillance programs such as CDC's Epidemic Intelligence Service, also do not directly involve the IC community.

Surveillance should be understood in the context of security, not public health.

Fuchs 11 Christian Fuchs, Chair in Media and Communication Studies Uppsala University, Department of Informatics and Media Studies. Sweden. "How Can Surveillance Be Defined?" Matrizes. 2011. http://www.matrizes.usp.br/index.php/matrizes/article/viewFile/203/347. [Prmeier]

In everyday language use, citizens tend to use the concept of surveillance in a negative way and to connection the Orwellian dystopia of totalitarianism with this notion. In academia, the notion of surveillance is besides in the social sciences especially employed in medicine. Surveillance data and surveillance systems in medicine are connected to the monitoring of diseases and health statuses. In the Social Sciences Citation Index (SSCI), the most frequently cited paper that contains the word surveillance in its title, is a medical work titled "Annual report to the nation on the status of cancer, 1975-2000, featuring the uses of surveillance data for cancer prevention and control" (SSCI search, April 30, 2010). This shows that there is a difference between the everyday usage and the predominant academic usage of the term surveillance. The first tends to be more political and normative, the latter more analytical. My argument is that the **social science usage of the term surveillance should not be guided by the understandings given to the term in medicine**, the natural sciences, or engineering because the specific characteristic of the social sciences is that it has a strong normative and critical tradition that should in my opinion not be dismissed. The question is if surveillance should be considered as a political concept or a general concept.

Tons of other IC groups solve.

Devine 20 Michael E. Devine, Analyst in Intelligence and National Security. "Intelligence Community Support to Pandemic Preparedness and Response." Congressional Research Service. 6 May 2020. https://crsreports.congress.gov/product/pdf/IF/IF11537/2. [Premier]

Of seventeen IC elements, the ones that may be most likely to support pandemic preparedness and response with medical foreign intelligence include the Office of the DNI (ODNI), the Central Intelligence Agency (CIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), the Defense Intelligence Agency's (DIA) National Center for Medical Intelligence (NCMI), and the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A).

The intelligence organization dedicated to providing the collection, analysis, and production of foreign medical intelligence is NCMI. Staffed by epidemiologists, virologists, veterinarians, toxicologists, and medical doctors, NCMI supports DOD with products and services that could include warnings of disease outbreaks with the potential to cause a pandemic or global health emergency, as well as foreign medical research and technology developments and the possible effect on U.S. or foreign military readiness.

The HHS CDC Global Disease Detection Operations Center (GDDOC) and the DHS National Biosurveillance Integration Center (NBIC) also compile information from the IC classified sources, international partnerships, domestic surveillance in the field, open-source internet research, and interagency coordination to provide early warning of and timely response to a pandemic or global health emergency.

AT: Disease – No Impact

Infectious diseases don't cause extinction

Cotton-Barratt et al. 17 Owen, PhD in Pure Mathematics, Oxford, Lecturer in Mathematics at Oxford, Research Associate at the Future of Humanity Institute. "Existential Risk: Diplomacy and Governance." 3 February 2017. https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf. [Premier]

For most of human history, natural pandemics have posed the greatest risk of mass global fatalities.37 However, there are some reasons to believe that natural pandemics are **very unlikely to cause human extinction.** Analysis of the International Union for Conservation of Nature (IUCN) red list database has shown that of the 833 recorded plant and animal species extinctions known to have occurred since 1500, **less than 4%** (31 species) were ascribed to infectious disease.38 None of the mammals and amphibians on this list were globally dispersed, and other factors aside from infectious disease also contributed to their extinction. It therefore seems that our own species, which is **very numerous**, **globally dispersed**, and capable of a **rational response to problems**, is very unlikely to be killed off by a natural pandemic.

One underlying explanation for this is that highly lethal pathogens can kill their hosts before they have a chance to spread, so there is a **selective pressure for pathogens not to be highly lethal**. Therefore, pathogens are likely to co-evolve with their hosts rather than kill all possible hosts.39

Resiliency, intervening actors, burnout check disease spread.

Adalja 16 Amesh, infectious-disease physician at the University of Pittsburgh. "Why Hasn't Disease Wiped out the Human Race?" *The Atlantic*. 17 June 2016. https://www.theatlantic.com/health/archive/2016/06/infectious-diseases-extinction/487514/. [Premier]

In Michael Crichton's The Andromeda Strain, the canonical book in the disease-outbreak genre, an alien microbe threatens the human race with extinction, and humanity's best minds are marshaled to combat the enemy organism. Fortunately, outside of fiction, there's **no reason** to expect alien pathogens to wage war on the human race any time soon, and my analysis suggests that any real-life domestic microbe reaching an extinction level of threat probably is just as **unlikely**.

When humans began to focus their minds on the problems posed by infectious disease, human life ceased being nasty, brutish, and short.

Any apocalyptic pathogen would need to possess a very special combination of two attributes. First, it would have to be **so unfamiliar** that no existing therapy or vaccine could be applied to it. Second, it would need to have a high and **surreptitious transmissibility** before symptoms occur. The first is essential because any microbe from a known class of pathogens would, by definition, have family members that could serve as **models for containment** and **countermeasures**. The second would allow the hypothetical disease to spread without being detected by even the most astute clinicians.

The three infectious diseases most likely to be considered extinction-level threats in the world today—**influenza**, **HIV**, and **Ebola**—**don't meet these two requirements**. Influenza, for instance, despite its well-established ability to kill on a large scale, its contagiousness, and its unrivaled ability to shift and drift away from our vaccines, is still what I would call a "**known unknown**." While there are many mysteries about how new flu strains emerge, from at least the time of Hippocrates, humans

have been attuned to its risk. And in the modern era, a **full-fledged industry** of influenza preparedness exists, with **effective vaccine strategies** and **antiviral therapies**.

HIV, which has killed 39 million people over several decades, is **similarly limited** due to several factors. Most importantly, HIV's dependency on blood and body fluid for transmission (similar to Ebola) requires intimate human-to-human contact, which **limits contagion**. **Highly potent antiviral therapy** allows most people to live normally with the disease, and a substantial group of the population has **genetic mutations** that render them impervious to infection in the first place. Lastly, simple prevention strategies such as **needle exchange** for injection drug users and **barrier contraceptives**—when available—can curtail transmission risk.

Ebola, for many of the same reasons as HIV as well as several others, also falls short of the mark. This is especially due to the fact that it spreads almost exclusively through people with **easily recognizable symptoms**, plus the taming of its once unfathomable 90 percent mortality rate by **simple supportive care**.

Beyond those three, **every other known disease falls short of what seems required to wipe out humans**—which is, of course, why we're still here. And it's not that diseases are ineffective. On the contrary, diseases' failure to knock us out is a testament to just how **resilient** humans are. Part of our evolutionary heritage is our immune system, one of the most complex on the planet, even without the benefit of vaccines or the helping hand of antimicrobial drugs. This system, when viewed at a species level, can adapt to almost any enemy imaginable. Coupled to genetic variations amongst humans—which open up the possibility for a range of advantages, from imperviousness to infection to a tendency for mild symptoms—this adaptability ensures that **almost any infectious disease** onslaught will **leave a large proportion of the population alive to rebuild**, in contrast to the fictional Hollywood versions.

While the immune system's role can never be understated, an even more powerful protector is the faculty of consciousness. Humans are not the most prolific, quickly evolving, or strongest organisms on the planet, but as Aristotle identified, humans are the **rational animals**—and it is this fundamental distinguishing characteristic that allows humans to form abstractions, think in principles, and plan long-range. These capacities, in turn, allow humans to modify, alter, and improve themselves and their environments. Consciousness equips us, at an individual and a species level, to make nature safe for the species through such technological marvels as **antibiotics**, **antivirals**, **vaccines**, and **sanitation**. When humans began to focus their minds on the problems posed by infectious disease, human life ceased being nasty, brutish, and short. In many ways, human consciousness became infectious diseases' worthiest adversary.

AT: Hegemony

NSA backlash hurts allied relationships.

Reichman 13 Deb, AP correspondent. “NSA Spying Threatens U.S. Foreign Policy Efforts.” Huffington Post. 26 October 2013. http://www.huffingtonpost.com/2013/10/26/nsa-spying-foreign-policy_n_4166076.html. [Premier]

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."**

NSA scandals let’s China strategically undermine US leadership.

O’Reilly 13 Brendan, freelance journalist. “China to reap harvest of NSA scandals.” Asia Times. 31 October 2013. http://www.atimes.com/atimes/China/CHIN-01-311013.html. [Premier]

A growing chorus of nations is decrying Washington's unrestrained cyber espionage. However, there is only one country with both the means and motivation for using mounting international resentment to challenge American hegemony**. The NSA surveillance of America's allies has opened up two vital fronts in which China can erode American global dominance.** Chinese Foreign Ministry spokeswoman Hua Chunying has claimed the rhetorical high ground, calling cyber security "a matter of sovereignty". She said Beijing is eager to address the issue through the framework of the United Nations, and to do so "China and Russia have submitted a draft plan, in an effort to help the world jointly tackle the problem." [1] This joint Sino-Russian proposal to combat the NSA's electronic surveillance coincides with a parallel initiative launched by two allies of the United States. Germany and Brazil are working together to create a UN resolution aimed at curtailing electronic spying. Both nations have been openly angry with Washington in the wake of revelations that the NSA has for years spied on the personal communications of both Brazilian President Dilma Rousseff and German Chancellor Merkel. Brazilian and German diplomats expect to finish the draft within a week, and then send the resolution to the UN Human Rights Committee. According to political scientist Gunther Maihold, "Brazil's main interest is that this should result in international regulation by the UN." [2] Such international regulation of electronic espionage would be anathema to large portions of the American political class, who believe unlimited NSA spying is justified by the perpetual threat of "terrorism", and are distrustful of the United Nations. Beijing may be supporting anti-cyber espionage efforts at the United Nations precisely because China's leaders expect such efforts will fail in the face of American political intransigence. **The fallout from Washington blocking anti-surveillance initiatives at the United Nations could disrupt American diplomacy for decades to come.** Chinese backing of UN efforts to curb the NSA's activities may undermine American hegemony by disrupting America's alliances. These alliances have cemented Washington's global dominance for the greater part of a century. Nevertheless, Beijing's opposition to American cyber espionage is to a large degree a defensive tactic. According to Der Spiegel, the NSA runs listening posts in Beijing, Shanghai, Chengdu, Hong Kong, and Taipei. Furthermore, this week Japanese media reported that in 2011 the NSA sought Tokyo's help to wiretap fiber-optic cables running through Japan. [3] This move was almost certainly aimed primary at gathering important political and economic data from China - terrorists of East Asian ancestry are not generally regarded as a major threat to the American homeland. The Japanese government declined the proposal because intercepting communications on such a large scale would be illegal under Japanese law. This story encapsulates some of the absurdities of the current situation. China, long accused by Washington of cooperation with lawless "rogue states", has been protected from American surveillance by the laws of Japan. Morality matters **The second front in which Beijing can make advances against Washington is in the sphere of international public opinion. American leaders have long espoused an image of America as a uniquely ethical nation, a "city upon a hill", an ideal moral power which lesser, more barbaric and grossly self-interested countries should emulate.** The practice of secretly monitoring tens of millions of phone calls of one's allies - including the communications of some of America's closest friends - has severely tarnished this image. China's official media is now capitalizing on this development. On Wednesday, the top story on the China Daily website was entitled "Spy scandal 'will weaken' US global credibility". Chinese-language media was even more vociferous. State-run CCTV Four featured Zhang Zhaozhong, a well-known military commentator, as saying: "Now the United States, if they wish to return to democratic freedom and human rights, should apologize to the entire world, saying: I am sorry, we designed some software like this, we have this type of back door, in the future we will manage it seriously..." [4] How times have changed. Only a few months ago, the US government was increasingly vocal in criticizing Chinese cyber espionage. Before President Barack Obama went to his first summit with President Xi Jinping, a White House official called on China to abide by international "rules of the road", and told reporters that "Governments are responsible for cyber attacks that take place from within their borders". [5] China is eager to remind domestic and international audiences of official American hypocrisy, now that such hypocrisy has been exposed on a global scale. **Morality - or rather, the perception of morality - plays a significant role in America's foreign policy objectives. The United States, for all its flaws, has garnered admirers and supporters all around the world for the open, democratic ideals it disseminates.** In contrast, Chinese foreign policy has had little relation to ideology for the past several decades. Beijing cements its relationships with foreign countries around mutual self-interest, usually of the economic kind. Beijing stands to benefit from emphasizing America's self-induced loss of moral standing. In the wake of Guantanamo Bay and the Iraq war, Washington cannot afford a further loss of integrity**. If the United States is increasingly perceived to an amoral and hypocritical power, then Chinese policies of practical economic benefits and political non-interference may be increasingly attractive.** It is worth pointing out that China is Brazil's largest trading partner, and bilateral trade between China and Germany is more valuable than trade between Germany and the US. As revelations of NSA electronic surveillance continue to mount, expect Beijing to continue highlighting Washington's moral duplicity. China will also support initiatives at the UN to curtail cyber espionage, potentially deepening divides between America and its allies. However, the damage is largely self-

wrought. The rocks that were once thrown at China have come back to shatter the glass-house of American integrity.

NSA overreach compromises it in a wide array of foreign policy areas.

Kehl 14 Danielle, Open Technology Institute senior policy analyst, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity", July, http://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf. [Premier]

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.**

AT: Hegemony – Heg Bad

Hegemony causes overextension and conflict spirals that trigger great power war

Forsyth and Mezzell 19 John, dean of Air Command and Staff College, Maxwell AFB, Alabama and Ann, Assistant Professor in the Department of International Security at Air Command and Staff College. "Through the Glass—Darker." Strategic Studies Quarterly, 13(4). Winter 2019. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-4/Forsyth.pdf. [Premier]

Finally, US forays into countering globalization's unforeseen effects are apt to generate security risks **similar to those Britain assumed before WWI**. US efforts to **shore up waning hegemony** by (re)building and exercising its vast power-projection capabilities, reminiscent of Britain's imperial overextension of the early 1900s, could **ultimately undermine stability**.54 The United States is still coming to grips with the need to curb China's aims in the Pacific. While the US Navy is "shrunken and overworked," the **PLA navy is now the largest** (in raw numbers of warships and submarines, though not in tonnage) and fastest growing in the world.55 **Xi** Jinping identifies the PLA's naval buildup and modernization as crucial to China's strength, prompting some to draw parallels between Xi and Kaiser Wilhelm.56 Though China's fleet is far less advanced, it has nonetheless allowed for the **expansion** of Chinese dominance in the South China, East China, and Yellow Seas. Indeed, the Pentagon's attempt to compensate for two decades of underinvestment during China's military modernization and A2/AD advancements may herald the next phase of a **spiral toward conflict**. The **Pentagon has reportedly assembled war plans** to account for a possible confrontation with China. It is also expanding and refurbishing the US fleet and fast-tracking weapons development and acquisition efforts (most notably, for longer-range missiles).57 Meanwhile, US partners and allies are prodding the United States to play a greater role in the Indo-Pacific region, offset Iran's ambitions in the Middle East, and deter Russian incursions into the Baltics . . . at the same time the US is trying to back away from its role as the global policeman.58 In other words, the need for US architectural planning—particularly with respect to China—may be **disrupted by calls for firefighting**. The push to fight fires rather than craft and execute measured plans is problematic; it not only derails the US ability to best prepare for great power competition but also generates the additional risk of **stumbling** ~~blindly~~ **into great power war**.

AT: Presidential Powers

War powers do not extend to domestic surveillance.

Barnett 15 Randy Barnett, Carmack Waterhouse Professor of Legal Theory, Georgetown University Law Center. Director, Georgetown Center for the Constitution. "Why the NSA Data Seizures Are Unconstitutional." Harvard Journal of Law and Public Policy. 2015. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2671&context=facpub. [Premier]

Constitutional protections against abuses of these powers vary. Consider that our military may kill enemy combatants in the field without any "due process of law" and may indefinitely incarcerate prisoners of war for the duration of hostilities. Neither of these measures can constitutionally be done to American citizens **domestically** in time of peace or war. Nor can they be done to foreign nationals in peacetime.

Those who would justify these programs under the war power are abandoning the domestic model. Therefore, any reliance on Katz's "reasonable expectation of privacy" doctrine, or Smith's "third-party doctrine," are make-weights and merely **confuse the issue**. You cannot defend the program using the "third-party" doctrine and then, when pressed on that argument, change the subject to the war power. Any war power argument must stand and fall on its own. Perhaps for this reason, in its recent brief in the ACLU's challenge to the NSA data seizures, the government did not assert the war power and never denied that the Fourth Amendment applied to this situation.

Although the government does rely on a "national security" theory of why the program is "reasonable" under the Fourth Amendment, even if it could be said to be reasonable to seize the phone records of every American in the interest of national security, this rationale cannot justify using the NSA data for **domestic** law enforcement purposes—as we are learning may well have occurred—or any other comparable data collection program that is used for domestic law enforcement purposes. That such mission creep has already occurred, albeit in secret, underscores the danger of allowing such bulk data seizures in the first place.

That defenders of this program will alternate between the domestic and war models of constitutional power signals that the conflict in which we are currently engaged does not fit neatly within either. The domestic model assumes that government is using its police powers to protect the rights of its citizens from others who are also members of the community. When citizens are accused of violating the rights of others that define the social compact, they deserve the benefit of the doubt before they are subjected to punishment. And we must be very careful to protect the civil liberties of the people from those in law enforcement who would abuse this police power to protect the public safety.

The war model assumes that government is using its military power to protect the rights of its citizens from threats posed by foreign powers, in particular the armies of foreign governments. Unlike persons who are accused of domestic crimes, the soldiers of a foreign power are not entitled to the protections of the Fourth and Fifth Amendments. But these war powers do not stretch into perpetuity and are typically limited to a geographically confined theater of combat. Wars between nations have both a beginning and end, and extraordinary war powers expire with the conflict that necessitated their use.

If the “cold war” between the United States and the USSR muddied the distinction between the domestic and war powers of the Congress and the President, what is sometimes called the “long war” against radical Islamic NGOs has threatened its collapse. If the battle ground is considered to include the territory of the United States, the enemy is hidden among the population, and such conflicts know no definitive end, adherence to the war power model threatens to completely subsume the protections of civil liberties afforded by the domestic model. In essence, the means of war are then turned against the People themselves to identify an enemy within.

Even if some blending of the models is warranted and that is what the original FISA and Patriot Acts were attempting to accomplish, it makes it all the more essential that the government **not exceed the limits** defined by these statutes. Construing Section 215 as broadly as the government now urges, and the FISA court has ruled in its secret opinions, threatens the very balance between the wartime and domestic models that Congress was presumably trying to strike. For this reason, the courts should avoid the constitutional issues by holding that Section 215 of the PATRIOT Act does not authorize the bulk seizure of the telephone and email communications records of all Americans.

No link – exigent circumstances allows emergency presidential action

Seamon 8 Richard, Professor, University of Idaho College of Law. “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. [Premier]

The hypothetical surveillance order described above, covering all cell phone calls to and from the doomed Flight 93, falls not only within the intrinsic limits of the President's powers under Article II but also within the extrinsic limits imposed by the Fourth Amendment. Ordinarily, the Fourth Amendment requires the government to get a warrant before electronically intercepting phone calls or reading their mail (presumably including their e-mail). 146 In addition, the Fourth Amendment ordinarily requires a particularized showing that the monitoring of each phone user is likely to reveal evidence of crime. 147 The traditional Fourth Amendment requirements of a warrant and an individualized showing of probable cause for a search do not, however, apply to our Flight 93 scenario. The exigent circumstances doctrine of Fourth Amendment law justifies immediate, warrantless surveillance of all cell phone users on board the flight.148 Moreover, although the exigent circumstances doctrine normally requires a particularized showing of probable cause of criminal activity, 149 that showing is unnecessary when "special needs, beyond the normal need for law enforcement," make the probable cause requirement impracticable. 50

The Flight 93 scenario thus illustrates the linkage between the President's congressionally irreducible, intrinsic power under Article II to respond to genuine national security emergencies and extrinsic limits on that power imposed by the Fourth Amendment. In a "genuine emergency," the President can take immediate action reasonably necessary to protect national security-**even if the action violates statutory restrictions**-and, if the President's action entails a search or seizure (as does Presidentially authorized electronic surveillance), exigent circumstances in the "special needs" context of national security will often excuse ordinary Fourth Amendment requirements. In short, the President's power reasonably to respond to a genuine national security emergency not only is irreducible by Congress but also satisfies

the Fourth Amendment-even if the response entails warrantless, suspicionless searches and seizures-as long as that response is reasonably justified by the emergency. 51

The perception of protection alone prevents a larger backlash against presidential power.

Small 8 Matthew, United States Air Force Academy. "His Eyes are Watching You: Domestic Surveillance, Civil Liberties and Executive Power during Times of National Crisis." http://cspc.nonprofitsoapbox.com/storage/documents/Fellows2008/Small.pdf. [Premier]

In fact, reasonable arguments can be made that there is no clearly formed public mandate demanding the consideration of an American citizen's right to privacy as important, if not more so, than national security. There exists only a concern of abridgement of their right, but this concern does not equate to motivating factor for government constraint. Studies show that from 1974 to 1983 Americans perceived little impact of privacy invasion, in its rare instances, on their lives (Katz and Tassone 1990, 125). Simultaneously, however, Americans did not, and still do not,17 favor wiretaps regardless of the presence of warrants (Katz and Tassone 1990, 130-131). Despite this, it appears that the public realizes the necessity of the power of the president to abridge certain rights in order to ensure national security. The public voices its concern but stops far short of forcing the government to restrain itself. Legislatures listen to the "broad climate of opinion" (Gandy Jr. 2003, 285) and that climate allows President Bush to act as he did.18 Like Abraham Lincoln, President Bush realized inadequacy within the government institutions tasked with keeping America safe through the collection of information on internal threats. In order to effectively combat terrorism, the NSA needed the ability to expand operations within the US. President Bush, in the manner of his Civil War predecessor, expanded his power to better equip the NSA to handle the threat. Court cases and legislation concerning wiretapping and intrusive domestic surveillance techniques only establish guidelines to give degrees of protection, but **more importantly the perception of protection**.19 This still leaves the president with the room to maneuver within these guidelines to maintain national security at the expense of complete civil liberty.

Justice Black's dissensions shed more light on this paradox that even though the courts deemed warrantless wiretaps an invasion of privacy, they still continue. There remains those of the persuasion that wiretapping is a viable information gathering tool and admissible in court with or without an accompanying warrant because the Forth Amendment is not a protection of privacy. In American history, domestic surveillance, later to include electronic surveillance, proved necessary to enforce those laws passed by Congress that quelled rebellion and silenced dissidents. Presently, the USA Patriot Act and other similar legislation requires an increase in domestic electronic surveillance in order to combat terrorism; so in the interest of adhering to the letter and the spirit of the law, President Bush must expand the use of domestic electronic surveillance.

President Bush took the precedent set by his predecessors and acted accordingly when the United States plummeted into turmoil. What is important now is for the president to realize when his power has reached its limit. The crux of the problem lies in justifying the remainder of a threat to American citizens. While the attacks of 9/11 still linger within the American psyche and legislation supports executive action, this task is less daunting. American citizens can stand some breaches in privacy but those breaches must not be permanent. Popular sentiment and legislation may currently favor

expanded presidential power but President Bush, or any subsequent president, would be remiss in assuming that it will remain as such for the duration of the struggle against international terrorism. The fickle nature of public and Congressional support in the domestic intelligence realm thus requires a great deal of prudence on the part of the president.

There are some indicators, albeit vague ones, of when domestic surveillance policy should yield to citizens' right to privacy. Following the progression witnessed during the Cold War it would be reasonable to expect that opposition to presidential power would first come in the form of Supreme Court rulings striking down certain powers as unconstitutional followed by public opinion more heavily favoring the right to privacy and finally, legislation codifying judicial rulings in accordance with public opinion. Court cases challenging the president's power under the USA Patriot Act have already surfaced. Both the American Civil Liberties Union (ACLU) and the Center for Constitutional Rights (CCR) have already filed formal complaints against the executive branch. The CCR, in particular, directly attacked the president's power to conduct electronic surveillance without a court order as criminal under the provisions of FISA. Similarly, the Electronic Frontier Foundation sued AT&T for violating free speech and the right to privacy by aiding the NSA. Although the president has fought these allegations, fighting most vehemently in the AT&T case, none of the cases reached the Supreme Court. The legal actions precipitated neither legislative response nor changes in executive policy. If, however, the populous feels so compelled as to bring the matter before the Supreme Court, the president risks losing the policy initiative as one or more unfavorable rulings may force Congress to act on behalf of the right to privacy. The president must take care to ensure that domestic surveillance policies are commensurate with the actual national security threat.

Although the war has no foreseeable end, the president's actions must have one. That end must be in concert with Congress and must demonstrate to the American people that the security of the US, and by default their own freedom, is better because of it. If not, the president risks losing all legitimacy and having his power constrained to the point where neither he nor the agencies below him can effectively protect the nation.

No spillover from surveillance to other areas.

Nzelibe 11 Jide Nzelibe, Professor of Law, Northwestern University Law School. "PARTISAN CONFLICTS OVER PRESIDENTIAL AUTHORITY." WILLIAM AND MARY LAW REVIEW, Vol. 53:389. 2011. [Premier]

This Essay argues that politicians may sometimes **strategically manipulate** the contours of the **President's** constitutional **authority** in order to achieve **partisan objectives**. At first glance, the notion that societal groups may ever stake out conflicting visions of presidential authority seems puzzling. After all, it is difficult to envision how any view of presidential authority can systematically confer one-sided benefits on any partisan or interest group, because presumably each group will sometimes lose and gain from any particular constraint on presidential authority. Thus, given the implicit veil of ignorance that underpins the separation of powers, one may think that the incentives of judges and elected officials to embrace visions of presidential authority that advance the specific objectives of any political party will be blunted. Unsurprisingly, much of the contemporary scholarship on presidential power has **ignored partisan factors** and has instead focused on how incentives **inherent** in the **institutional nature** of the various branches of government shape preferences for expansive presidential authority.2

This Essay suggests a **contrary view**: if certain conditions hold, partisan power holders can often calculate how an **expansive or narrow** view of presidential authority over **discrete issues** is likely to affect their electoral and ideological objectives. More specifically, staking out partisan positions on the allocation of presidential authority is likely to be rational when such authority can be **unbundled** on an **issue-by-issue basis**.3 Under these conditions, parties are likely to **favor** a vision of **presidential authority** that will **enable them** to **carry out** those **issues** in which **they have** an **electoral advantage** over the opposition, but that make it **more difficult** for the **opposition** to **carry out** its favored **issues**. For instance, when the presidential authority to negotiate human rights **treaties** can be effectively **unbundled** from the **war**-making **power**, Republicans may prefer more **constraints** on the President's treatymaking authority in human rights, but less on his **war**-making authority.4 By contrast, Democrats or left-leaning constituencies will likely adopt the opposite set of preferences regarding presidential authority on war and human rights. Similarly, Democratic administrations may be more willing to indulge a greater role for courts in adjudicating human rights controversies even at the expense of the President's interpretive discretion over international law, whereas Republican administrations are more likely to view such adjudications as interfering with the President's flexibility to conduct foreign affairs.5

Congress should have authority over war – it's key to balanced strategy.

Gallagher 11 Lieutenant Colonel Joseph V. Gallagher III, United States Marine Corps. "Unconstitutional War: Strategic Risk in the Age of Congressional Abdication." Parameters. Summer 2011. http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2011summer/gallagher.pdf. [Premier]

In other words, success at the tactical level of war first requires careful preparations at the political and strategic levels. The enabling institutions for success in war—**Congress**, the president, the cabinet, and other advisors—all need to be fully **engaged** in the development of feasible, suitable, and acceptable strategy.57 And this carefully crafted strategy needs to include legitimate justification for violence, rigorous calculation and valuation of political objectives, and commitment of resources sufficient to achieve strategic objectives.58

Since 1945, the **U**nited **S**tates has built the world's most capable **war-fighting** machine. So why, then, have most of the nation's large military **interventions** since World War II ended in **defeat** or, at best, **stalemate**? Political leaders should attend more to what Clausewitz calls the **political dimensions** of war—**national unity** and the **political value** of the objective—as **inseparable from** national and **military strategy**.

War theorists have long emphasized the importance of national unity and the political value of the war objective. Thousands of years ago, Sun Tzu identified the necessary pre-condition of national unity for successful war strategy.59 National unity enables political leaders to muster resources needed to win wars and to amass the human capital that makes an army. Clausewitz advised, "to discover how much of our resources must be mobilized for war, we must first examine our own political aim."60 National unity underwrites the commitment the nation needs to successfully prosecute war, provided the war has political value commensurate to the effort expended.61 The founders directed this nation to use a collaborative process to assess the political value of a war. So the Constitution requires Congress to deliberate on the decision to go to war and, when it so decides, to declare war. Therefore, the Constitution serves as the guarantor of ensuring national unity and a legitimate valuation of the war's political objective—provided through the mechanism of the war declaration. Consider the language of the 1941 war declaration against Japan. It captures the national unity, the political value of the objective, and the will and support of Congress to support the war.62 A Risk to Strategy

As the practice of declaring war has become passé, American strategy has likewise become disjointed and disconnected from national security objectives. Following World War II, an acquiescent Congress and an aggressive presidency have, for decades, fostered a **strategic climate** that **failed to maintain the links** between the political dimensions of the state and its strategy. The predominant "NSC-68 thinking," largely a product of executive national security panels that administrations have embraced and Congress has blithely followed, provided inadequate guidance on how objectives and capabilities should be joined to produce **coherent overall strategy**.63 This connection, Clausewitz observed, is **necessary for success** in war.

For example, US strategy following World War II ironically came to resemble the German strategy of the early 20th century, relying heavily on military ways and means that failed to address the political and economic components of warfare.64 Historians are quick to extol the superiority of the German military machine, but Germany lost two world wars. Similarly, the United States has pursued a strategy built on loosely linked operational and tactical successes. Unfortunately, without concretely defined end states specified in a coherent all-encompassing strategy, these successes have not achieved national strategic ends. In Vietnam, Afghanistan, and Iraq, our leaders failed to properly define the national strategic ends, so the attendant strategies have been **inchoate**. Leaders' attempts to match ways and means to fluctuating or poorly defined ends resulted in unacceptable levels of uncertainty and risk. These protracted and strategically uncertain conflicts are alien to America's strategic culture, which has little tolerance for long, risky, or uncertain conflicts.65

More recently, as the executive branch exercises greater authority in directing military interventions, the gap between risk and strategy becomes wider. **Theater commanders** charged with developing adequate or complete strategies with sound ends and feasible ways to achieve them **lack confidence in congressional support** to provide the means necessary to achieve these strategic objectives.66 As the world's only superpower, the **U**nited **S**tates can expect asymmetrical conflict as the norm. Future adversaries will increasingly focus on the **strategic target of the** American **people's collective will** in their efforts to subvert our national strategy.67

AT: Cyberattacks – No Impact

Cyberattacks impossible – empirics and defenses solve

Rid 12 Thomas Rid, reader in war studies at King's College London, is author of "Cyber War Will Not Take Place" and co-author of "Cyber-Weapons." "Think Again: Cyberwar." Foreign Policy. March/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full. [Premier]

"Cyberwar Is Already Upon Us." No way. "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. Since then, it seems to have arrived -- at least by the account of the U.S. military establishment, which is busy competing over who should get what share of the fight. Cyberspace is "a domain in which the Air Force flies and fights," Air Force Secretary Michael Wynne claimed in 2006. By 2012, William J. Lynn III, the deputy defense secretary at the time, was writing that cyberwar is "just as critical to military operations as land, sea, air, and space." In January, the Defense Department vowed to equip the U.S. armed forces for "conducting a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace." Meanwhile, growing piles of books and articles explore the threats of cyberwarfare, cyberterrorism, and how to survive them. **Time for a reality check: Cyberwar is still more hype than hazard**. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but **Reed's book is the only public mention of the incident and his account relied on a single document**. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. **The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack**. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus

Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. **The same is true for the vast majority of cyberattacks on record**. Indeed, **there is no known cyberattack that has caused the loss of human life**. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. "A Digital Pearl Harbor Is Only a Matter of Time." **Keep waiting**. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such **alarmist predictions have been ricocheting inside the Beltway for the past two decades**, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising, even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya **incident highlights how difficult a devastating attack would be to mount**. The plant's washout was an accident at the end of a complicated and unique chain of events. **Anticipating** such vulnerabilities in advance **is extraordinarily difficult** even for insiders; creating comparable coincidences from cyberspace would **be a daunting challenge at best for outsiders**. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath. "Cyberattacks Are Becoming Easier." **Just the opposite**. U.S. Director of National Intelligence James R. Clapper warned last year that the volume of malicious software on American networks had more than tripled since 2009 and that more than 60,000 pieces of malware are now discovered every day. The United States, he said, is undergoing "a phenomenon known as 'convergence,' which amplifies the opportunity for disruptive cyberattacks, including against physical infrastructures." ("Digital convergence" is a snazzy term for a simple thing: more and more devices able to talk to each other, and formerly separate industries and activities able to

work together.) Just because there's more malware, however, **doesn't mean that attacks are becoming easier**. In fact, potentially damaging or life-threatening cyberattacks should be more difficult to pull off. Why? **Sensitive systems generally have built-in redundancy and safety systems, meaning an attacker's likely objective will not be to shut down a system**, since merely forcing the shutdown of one control system, say a power plant, could trigger a backup and cause operators to start looking for the bug. To work as an effective weapon, malware would have to influence an active process -- but not bring it to a screeching halt. If the malicious activity extends over a lengthy period, it has to remain stealthy. That's a more difficult trick than hitting the virtual off-button. Take Stuxnet, the worm that sabotaged Iran's nuclear program in 2010. It didn't just crudely shut down the centrifuges at the Natanz nuclear facility; rather, the worm subtly manipulated the system. Stuxnet stealthily infiltrated the plant's networks, then hopped onto the protected control systems, intercepted input values from sensors, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, according to researchers who have studied the worm. Its objective was not just to fool operators in a control room, but also to circumvent digital safety and monitoring systems so it could secretly manipulate the actual processes. Building and deploying Stuxnet required **extremely detailed intelligence** about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, "convergence," standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused **defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex**, not less.

Negative

Terrorism

Link – Surveillance

Every form of data collection is useful because they give fragments to prevent attacks

.

Lewis 14 James Andrew, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies. "Underestimating Risk in the Surveillance Debate." CSIS. December 2014. http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf. [Premier]

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.

Zuckerman et al.13 Jessica, policy analyst at the Heritage Foundation, et al. "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism." Heritage Foundation. 22 July 2013. http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism. [Premier]

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.

Strong intelligence gathering is key to discourage initiation of weapons of mass destruction.

Pittenger 14 Robert Pittenger, chair of Congressional Task Force on Terrorism. "Bipartisan bill on NSA data collection protects both privacy and national security." Washington Examiner. 9 June 2014. 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. [Premier]

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.

Link – Recruitment

Calls for restraint tank NSA morale.

Reed 13 Brad Reed, news editor at BGR. "NSA morale reportedly hits rock bottom after Snowden revelations." BGR. 9 December 2013. https://bgr.com/2013/12/09/nsa-employees-snowden-leaks/. [Premier]

Employees at the National Security Agency aren't happy that we now know to look out for their trash-talking elves that they've created in World of Warcraft. The Washington Post reports that officials at the NSA are feeling depressed and demoralized by the constant stream of revelations being leaked by former contractor Edward Snowden and are also feeling hung out to dry by a White House that has spent most of its time trying to contain political damage caused by the Snowden leaks. Essentially, the Post's sources say that the NSA thinks that it's providing some of the most valuable intelligence in the United States' battle against terrorism and that it deserves recognition for its efforts instead of calls for more restraint.

That crushes recruitment and hurts national security.

Nakashima and Gregg 18 Ellen Nakashima and Aaron Gregg, reporters at WaPo. "NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization." Washington Post. 2 January 2018. https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html. [Premier]

The National Security Agency is **losing its top talent** at a worrisome rate as highly skilled personnel, some disillusioned with the spy service's leadership and an unpopular reorganization, take higher-paying, more flexible jobs in the private sector.

Since 2015, the NSA has lost several hundred hackers, engineers and data scientists, according to current and former U.S. officials with knowledge of the matter. **The potential impact on national security is significant**, they said.

Headquartered at Fort Meade in Maryland, the NSA employs a civilian workforce of about 21,000 there and is the largest producer of intelligence among the nation's 17 spy agencies. The people who have left were responsible for collecting and analyzing the intelligence that goes into the president's daily briefing. Their work also included monitoring a broad array of subjects including the Islamic State, Russian and North Korean hackers, and analyzing the intentions of foreign governments, and they were responsible for protecting the classified networks that carry such sensitive information.

"Some synonym of the word **'epidemic'** is the best way to describe it," said Ellison Anne Williams, a former senior researcher at the NSA who left in 2016 to start her own data-security firm, Enveil. More than 10 of her employees also came from the NSA, she said. "The agency is losing an amazing amount of its strongest technical talent, and to lose your best and brightest staff is a huge hit."

The NSA would not disclose how many job vacancies it has. Agency officials said there is a 5.6 percent attrition rate among personnel who specialize in science, technology and math. The attrition rate is closer to 8 or 9 percent among hackers and those who staff the agency's always-operating watch center monitoring for cyber attacks, a trend that has spanned the Obama and Trump administrations.

Although the departure rates are low, compared with attrition levels in the civilian technology industry, and although the agency is filling its vacancies, most new personnel **lack the experience** of those who have left, said one senior intelligence official, who like others spoke on the condition of anonymity to offer candid insights about the secretive organization. **That experience deficit can impede the NSA's core mission of collecting and analyzing the masses of data the agency lifts from foreign networks.**

It is a turbulent moment in the NSA's 65-year history. The agency continues to face public distrust after revelations, made by former contractor Edward Snowden in 2013, about the scope of its surveillance of American citizens. **Morale dipped** in the aftermath of those disclosures and has not fully recovered. More recently, the workforce was rattled by a series of breaches targeting the agency's highly sensitive hacking tools.

Link – Deterrence

Even if the data seems useless, its necessary to deter terrorists from planning an attack in the first place.

Kroneg and Pavel 12 Kroenig is an Assistant Professor of Government at Georgetown University and a Stanton Nuclear Security Fellow at the Council on Foreign Relations, Barry Pavel is Director of the Atlantic Council's International Security Program. "How to deter terrorism." CSIS. 19 March 2012. https://www.csis.org/analysis/twq-how-deter-terrorism-spring-2012. [Premier]

Given the value that terrorists place on operational success, states can deter terrorism by convincing terrorists that operations are likely to fail. For this reason, **simple homeland security measures can deter terrorist attacks.** Improving **domestic** intelligence and hardening key targets are strong deterrents to attack. Indeed, we know of many cases in which terrorists were deterred from carrying out an attack by the fear of failure. For example, an al-Qaeda affiliate planned to attack a U.S. military base in Turkey in late 2003, but the United States improved its defenses at the site during the planning stages, and the terrorists called off the attack.22 It is, of course, impossible to protect every conceivable target, and terrorists will often re-focus away from hardened targets toward softer ones. This fact can be an asset as well as a liability in the war on terror, however. It is, after all, the counterterrorists' choice about which targets should be defended and at what cost. Deploying effective **homeland security** measures may, for example, be targeted to specifically **help deter WMD terrorism**. In order to successfully conduct a WMD attack, terrorists would have to complete a number of difficult steps. Measures that the United States takes to reduce the probability that a WMD terror attack will succeed should have a deterrent effect. For example, as the United States improves its radiation detection capabilities at border crossings, the probability that a terrorist smuggling nuclear material across the border will be captured and the radioactive material confiscated increases. Given the value that terrorists might place on scarce and strategically important nuclear material, they may prefer not to even attempt to bring it into the United States, given a sufficiently high risk of losing it. A critic might counter that the United States is already improving homeland security and that this is being done for defensive, not deterrent purposes. This critique, however, glosses over one of the most important questions of U.S. counterterrorism policy: should homeland security measures be intended primarily as a deterrent or as a defense? We argue that homeland security policy should be designed primarily as a deterrent. **The objective of homeland security should not be to fend off an endless number and methods of terrorist attacks**. In fact, if it gets to the point that U.S. forces have to thwart an attack at the last moment, homeland security has failed. Rather, the United States should aim to deter terrorism. Washington should send the message that we are ready and that it is not in terrorists' best interests to attempt an attack. The point of building concrete barriers around the Washington Monument is not to haveterrorists smash explosive-laden trucks into the barricades day after day. Rather, the hope is that terrorists will see the defenses and decide not to attack in the first place. This insight has important implications for the way we structure homeland security. First, homeland security should not be designed primarily as a defense. We cannot hope to thwart every kind of conceivable attack. Rather the goal should be to raise the perceived probability that an operation will be thwarted to convince terrorists that they should not attempt an attack in the first place. For this goal, **a perfect defense is overkill** (and unachievable in any event). Homeland security can rely more heavily on measures such as randomized screening and

periodic surges in security levels at key sites. Such measures keep terrorists off guard, are less costly than a watertight defense, and if designed well, are sufficient for deterring terrorist attacks.

Link – Coop

Surveillance allows for international cooperation to combat terror.

Rotella 13 Sebastian Rotella, senior reporter at ProPublica. "How the NSA's High-Tech Surveillance Helped Europeans Catch Terrorists." ProPublica. 29 June 2013. http://www.propublica.org/article/how-the-nsas-high-tech-surveillance-helped-europeans-catch-terrorists. [Premier]

PARIS — In 2007, Belgian police were keeping close watch on Malika el-Aroud, a fierce al-Qaida ideologue whose dark eyes smoldered above her veil. The Moroccan-born Aroud had met Osama bin Laden while living in al-Qaida's stronghold in Afghanistan. She gained exalted status when her husband posed as a journalist to blow up the renowned Ahmed Shah Massoud, the chief of the anti-Taliban Northern Alliance, just two days before the Sept. 11 attacks. Aroud later returned to Europe, remarried and started an Islamist website that attracted a group of French and Belgian extremists. Led by her second husband, Moez Garsallaoui, half-a-dozen of them went to Waziristan, where they joined several thousand al-Qaida fighters, including a Latino convert from Long Island, learned to make bombs and plotted against the West with terrorist kingpins. The authorities — American, Belgian, French, Swiss, Italian, Turkish — were all over them. U.S. surveillance had tracked their radicalization, their emails from Pakistan, even calls made to their mothers before they trudged through snowy Iranian mountains. An intercepted photo that Garsallaoui sent his wife showed him holding a grenade launcher. He claimed to have killed U.S. soldiers in Afghanistan and described his escape from a missile strike: "I came close to dying." The militants took precautions, changing laptops and using Internet cafes. But they were no match for top-secret, real-time NSA intercepts. Some of the monitoring was approved by the Foreign Intelligence Surveillance Act. "We were inside their computers," a source said. As debate rages in the United States about the National Security Agency's sweeping data-mining programs, I've been on a reporting trip overseas, where I've been talking to sources about the controversy and how differing U.S. and European approaches to counterterrorism can complement each other. On Tuesday, NSA Director Gen. Keith Alexander, told a congressional committee that his agency's surveillance programs helped stop more than 50 terror plots in the U.S. and abroad. Five years ago, I was based in Europe covering terrorism, running from one attack or aborted plot to another. As the Brussels investigation shows, these cases frequently combined the high-tech reach of the U.S. counterterror apparatus with the street skills of foreign agencies. In November 2008, Pakistani and U.S. agents swooped into Kandahar and nabbed Bryant Neal Viñas, the convert from Long Island and al-Qaida militant. He cooperated with the FBI, admitting that he discussed an attack on the Long Island Rail Road with top al-Qaida figures. Days later, a drone strike killed Rashid Rauf, a Pakistani-British operative who helped plan the London transport bombings and the "liquid bomb" plot to blow up planes in 2006. Three Belgian and French militants returned home, where police arrested them after intercepts picked up menacing chatter. Viñas pleaded guilty. Aroud went to prison, and investigators believe her second husband Garsallaoui died in the land of jihad. Other cases benefited from close cooperation. In Germany in 2007, U.S. monitoring detected a suspect checking the draft file of an email box at an Internet cafe in Stuttgart. Armed with that lead, German security services deployed surveillance at numerous Internet cafes in the city. The investigation resulted in the dismantling of a Pakistan-trained group plotting to attack U.S. military targets in Germany. As several European sources told me, if an extremist in Marseilles was talking about nefarious activities with an extremist in Geneva over the Internet, chances were good that U.S. intelligence agencies would find out and inform the French and Swiss. Not because of sources on the ground, but because U.S. agencies could detect the communications through computer servers in the United States. The reaction here to the U.S. debate has been bemused. European terrorist hunters seem surprised that the revelation of the NSA data-monitoring programs is big news. The technological capacities of U.S. agencies have been an integral component of dramatically improved teamwork against terrorism during the past decade. "In the fight against terrorism, intelligence-sharing is essential," said Jean-Louis Bruguière, who served for more than two decades as a top French antiterror magistrate before retiring in 2007. (He declined to discuss the NSA's role in investigations.) "Cooperation with American services has always been trusting and excellent."

Impact – Turns Case

Another domestic terror attack would decimate the civil liberties that exist now which turns the case.

Friedman 13 Thomas L. Friedman became The New York Times foreign affairs Op-Ed columnist in 1995. "Blowing a Whistle." New York Times. 12 June 2013. http://www.nytimes.com/2013/06/12/opinion/friedman-blowing-a-whistle.html. [Premier]

I'm glad I live in a country with people who are vigilant in defending civil liberties. But as I listen to the debate about the disclosure of two government programs designed to track suspected phone and e-mail contacts of terrorists, I do wonder if some of those who unequivocally defend this disclosure are behaving as if 9/11 never happened – that the only thing we have to fear is government intrusion in our lives, not the intrusion of those who gather in secret cells in Yemen, Afghanistan and Pakistan and plot how to topple our tallest buildings or bring down U.S. airliners with bombs planted inside underwear, tennis shoes or computer printers. Yes, I worry about potential government abuse of privacy from a program designed to prevent another 9/11 — abuse that, so far, does not appear to have happened. But I worry even more about another 9/11. That is, I worry about something that's already happened once – that was staggeringly costly – and that terrorists aspire to repeat. I worry about that even more, not because I don't care about civil liberties, but because what I cherish most about America is our open society, and I believe that if there is one more 9/11 – or worse, an attack involving nuclear material – it could lead to the **end of the open society as we know it**. If there were another 9/11, I fear that 99 percent of Americans would tell their members of Congress: "Do whatever you need to do to, **privacy be damned, just make sure this does not happen again**." That is what I fear most. That is why I'll reluctantly, very reluctantly, trade off the government using data mining to look for suspicious patterns in phone numbers called and e-mail addresses – and then have to go to a judge to get a warrant to actually look at the content under guidelines set by Congress — to prevent a day where, out of fear, we give government a license to look at anyone, any e-mail, any phone call, anywhere, anytime. What we don't need is to give up our freedoms just to address levels of paranoia that are, frankly, infantile. So I don't believe that Edward Snowden, the leaker of all this secret material, is some heroic whistle-blower. No, I believe Snowden is someone who needed a whistle-blower. He needed someone to challenge him with the argument that we don't live in a world any longer where our government can protect its citizens from real, not imagined, threats without using big data — where we still have an edge — under constant judicial review. It's not ideal. But if one more 9/11-scale attack gets through, the cost to civil liberties will be so much greater. A hat tip to Andrew Sullivan for linking on his blog to an essay by David Simon, the creator of HBO's "The Wire." For me, it cuts right to the core of the issue. "You would think that the government was listening in to the secrets of 200 million Americans from the reaction and the hyperbole being tossed about," wrote Simon. "And you would think that rather than a legal court order, which is an inevitable consequence of legislation that we drafted and passed, something illegal had been discovered to the government's shame. Nope. … The only thing new here, from a legal standpoint, is the scale on which the F.B.I. and N.S.A. are apparently attempting to cull anti-terrorism leads from that data. … I know it's big and scary that the government wants a database of all phone calls. And it's scary that they're paying attention to the Internet. And it's scary that your cellphones have GPS installed. … The question is not should the resulting data exist. It does. … 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**." We do need to be constantly on guard for abuses. But the fact is, added Simon, that for at least the last two presidencies "this kind of data collection has been a baseline logic of an American anti-terrorism effort that is effectively asked to find the needles before they are planted into haystacks, to prevent even such modest, grass-rooted conspiracies as the Boston Marathon bombing before they occur." To be sure, secret programs, like the virtually unregulated drone attacks, can lead to real excesses that have to be checked. But here is what is also real, Simon concluded: "Those planes really did hit those buildings. And that bomb did indeed blow up at the finish line of the Boston Marathon. And we

really are in a continuing, low-intensity, high-risk conflict with a diffuse, committed and ideologically motivated enemy. And, for a moment, just imagine how much bloviating would be wafting across our political spectrum if, in the wake of an incident of domestic terrorism, an American president and his administration had failed to take full advantage of the existing telephonic data to do what is possible to find those needles in the haystacks." And, I'd add, not just bloviating. Imagine how many real restrictions to our beautiful open society we would tolerate if there were another attack on the scale of 9/11. Pardon me if I blow that whistle.

Alternatives to surveillance are more intrusive.

Lewis 14 James Andrew, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies. "Underestimating Risk in the Surveillance Debate." CSIS. December 2014. http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf. [Premier]

Broad surveillance of communications is the **least** intrusive method and **most effective** means for discovering terrorist activity. The alternatives to mass surveillance are straightforward. Countries can replace communications surveillance by increasing the number of security service personnel responsible for monitoring terrorism or they can decrease surveillance and accept some increase in the level of risk of a successful attack. The dilemma with choosing this course of action is that the number of agents required to replace communications surveillance is expensive and **overtly intrusive** in a way the communications surveillance is not. Hundreds of thousands of additional agents would be required to provide national coverage, may lack sufficient global reach to detect activity being planned or undertaken outside U.S. territory, and the creation of such a large force risks creating a much greater chilling effect on liberties.

Impact – Nuke Terror

Successful acquisition causes nuclear spoofing – extinction.

Barrett et al. 13 Anthony, PhD in Engineering and Public Policy from Carnegie Mellon University, Fellow in the RAND Stanton Nuclear Security Fellows Program, and Director of Research at Global Catastrophic Risk Institute, Seth Baum, PhD in Geography from Pennsylvania State University, Research Scientist at the Blue Marble Space Institute of Science, and Executive Director of Global Catastrophic Risk Institute, Kelly Hostetler, BS in Political Science from Columbia and Research Assistant at Global Catastrophic Risk Institute. "Analyzing and Reducing the Risks of Inadvertent Nuclear War Between the United States and Russia." Science & Global Security: The Technical Basis for Arms Control, Disarmament, and Nonproliferation Initiatives, Volume 21, Issue 2. 24 June 2013. https://www.tandfonline.com/doi/abs/10.1080/08929882.2013.798984. [Premier]

War involving significant fractions of the U.S. and Russian nuclear arsenals, which are by far the largest of any nations, could have **globally catastrophic effects** such as severely **reducing food production** for years, 1 potentially leading to **collapse of modern civilization** worldwide, and even the **extinction** of humanity. 2 Nuclear war between the United States and Russia could occur by various routes, including accidental or unauthorized launch; deliberate first attack by one nation; and inadvertent attack. In an accidental or unauthorized launch or detonation, system safeguards or procedures to maintain control over nuclear weapons fail in such a way that a nuclear weapon or missile launches or explodes without direction from leaders. In a deliberate first attack, the attacking nation decides to attack based on accurate information about the state of affairs. In an inadvertent attack, the attacking nation mistakenly concludes that it is under attack and launches nuclear weapons in what it believes is a counterattack. 3 (Brinkmanship strategies incorporate elements of all of the above, in that they involve intentional manipulation of risks from otherwise accidental or inadvertent launches. 4) Over the years, nuclear strategy was aimed primarily at minimizing risks of intentional attack through development of deterrence capabilities, and numerous measures also were taken to reduce probabilities of accidents, unauthorized attack, and inadvertent war. For purposes of deterrence, both U.S. and Soviet/Russian forces have maintained significant capabilities to have some forces survive a first attack by the other side and to launch a subsequent counter-attack. However, concerns about the extreme disruptions that a first attack would cause in the other side's forces and command-and-control capabilities led to both sides' development of capabilities to detect a first attack and launch a counter-attack before suffering damage from the first attack. 5 Many people believe that with the end of the Cold War and with improved relations between the United States and Russia, the risk of East-West nuclear war was significantly reduced. 6 However, it also has been argued that inadvertent nuclear war between the United States and Russia has continued to present a **substantial risk**. 7 While the United States and Russia are not actively threatening each other with war, they have **remained ready** to **launch nuclear missiles** in response to indications of attack. 8 False indicators of nuclear attack could be caused in several ways. First, a wide range of events have already been mistakenly interpreted as indicators of attack, including weather phenomena, a faulty computer chip, wild animal activity, and control-room training tapes loaded at the wrong time. 9 Second, **terrorist groups** or other actors might **cause attacks** on either the United States or Russia that **resemble** some kind of **nuclear attack by the other nation** by actions such as exploding a stolen or improvised nuclear bomb, 10 especially if such an event occurs during a crisis between the United States and Russia. 11 A variety of nuclear terrorism scenarios are **possible**. 12 Al Qaeda has sought to obtain or construct nuclear weapons and to use them against the United States. 13 Other methods could involve attempts to circumvent nuclear weapon launch control safeguards or exploit holes in their security. 14 It has long been argued that the probability of inadvertent nuclear war is significantly higher during U.S.–Russian crisis conditions, 15 with the Cuban Missile Crisis being a prime historical example. It is possible that U.S.–Russian relations will significantly deteriorate in the future, increasing nuclear tensions. There are a variety of ways for a third party to raise tensions between the United States and Russia, making one or both nations more likely to misinterpret events as attacks. 16

Impact – Bioterror

Bioterrorism is coming and outweighs nuke war.

Selk 17 Avi Selk, WaPo. "Bill Gates: Bioterrorism could kill more than nuclear war — but no one is ready to deal with it." Washington Post. 18 February 2017. https://www.washingtonpost.com/news/worldviews/wp/2017/02/18/bill-gates-bioterrorism-could-kill-more-than-nuclear-war-but-no-one-is-ready-to-deal-with-it/?utm_term=.2a3614882936. [Premier]

A genetically engineered virus is easier to make and could kill more people than nuclear weapons — and yet **no country on Earth is ready** for the threat, Bill Gates warned world leaders Saturday. No one on his panel at the Munich Security Conference argued with him. "The next epidemic has a good chance of originating on a computer screen," said Gates, who made a fortune at Microsoft, then spent much of it fighting disease through his global foundation. Whether "by the work of nature or the hands of a terrorist," Gates said, an outbreak could kill tens of millions in the near future unless governments begin "to prepare for these epidemics the same way we prepare for war." His co-panelists shared some of the same fears. "Disease and violence are killing fewer people than ever before, **but it's spreading more quickly**," said Erna Solberg, the prime minister of Norway. "**We have forgotten how catastrophic those epidemics have been."** She recalled the Black Death, which she said killed more than half her country's population and created a 200-year recession in Europe. "**It's not if, but when these events are going to occur again**," said Peter Salama, executive director of the World Health Organization. "**We need to ramp up** our **preparedness**." Gates, who founded the Bill & Melinda Gates Foundation with his wife in 2000, has been worrying about the world's ability to stop a deadly pandemic since Ebola killed thousands two years ago, while governments and militaries struggled to stop it from spreading through West Africa. "NATO countries participate in joint exercises in which they work out logistics such as how fuel and food will be provided, what language they will speak, and what radio frequencies will be used," Gates wrote in 2015 in the New England Journal of Medicine. "Few, if any, such measures are in place for response to an epidemic." He took the same message to Reddit a year later, when a commenter asked which technologies the world was better off without. '"I am concerned about biological tools that could be used by a bioterrorist," Gates wrote. "However the same tools can be used for good things as well." Before his panel on Saturday, Gates told the Telegraph: "**It would be** relatively **easy to engineer a new flu strain" by combining a version that spreads quickly with one that kills quickly. Unlike a nuclear war, such a disease would not stop killing once released.**

AT: "Data is Useless"

No such thing as useless data – it stops us from going after false leads.

Lewis 14 James Andrew, senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies. "Underestimating Risk in the Surveillance Debate." CSIS. December 2014. http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf. [Premier]

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.

Insider Threats

Link – Bulk Collection

New Freedom Act allows enough surveillance to check insider threats—the plan is too strict and prevents the data collection key to prevent another leak—status quo detection is key

Sternstein 15 Aliya Sternstein, covered technology for more than a decade at such publications as National Journal's Technology Daily, Federal Computer Week and Forbes, commentator on C-SPAN. "WATCHDOG SAYS PENTAGON NEEDS TO CRANK UP 'INSIDER THREAT' MONITORING. NextGov. 4 June 2015, http://www.nextgov.com/cybersecurity/2015/06/watchdog-says-dod-needs-crank-insider-threat-monitoring/114430/?oref=ng-relatedstories. [Premier]

Work to rein in some post-Sept. 11 domestic surveillance practices ended with passage of a bill that limits the National Security Agency's collection of U.S. call records. But regular Joes inside the Pentagon -- or at least those with access to sensitive or classified information -- should expect even greater scrutiny on their workplace digital activities. Just before the Senate cleared the USA Freedom Act, the Government Accountability Office released a report recommending the Defense Department take new steps to set up so-called "insider threat" programs, which aim to stop information leaks by disgruntled employees. The unclassified version of the report found only half of military components GAO reviewed have logged system and user behaviors to develop "a baseline of normal activity patterns." The purpose of tracing the activities of Pentagon personnel is to zero in on network "anomalies," computer usage that might be indicative of a leaker, the watchdogs said. NSA is part of the Defense Department. The employee insider threat program was borne out of various laws and White House policies issued since 2010 that require all departments to do a better job of fortressing classified information. That year, former soldier Chelsea Manning shared top secret files with the WikiLeaks website. The ability of ex-NSA contractor Edward Snowden to reveal classified intelligence in 2013 suggests anti-leak programs need more muscle, Patricia Larsen, co-director of the governmentwide National Insider Threat Task Force, said last December. This week, GAO agreed. A key element of the Pentagon's program has not consistently been incorporated Defensewide, the auditors said, noting "three of the six components [evaluated] have developed a baseline of normal activity" on Defense networks. They did not identify the organizations by name. "Anomalous activities are network activities that are inconsistent with the expected norms, the watchdogs added. "These activities, such as network activity outside of normal work hours or changes in typical data download patterns, could indicate the exploitation of cyber vulnerabilities, among other things." To detect anomalies, three of the components GAO examined plan to buy or upgrade analytic tools that allow them to monitor user behavior suggesting insider-threat activities. One entity that already has such technology said the enhanced model it expects to obtain will be able to watch a user's behavior across unclassified, secret and top-secret networks. A handful of policies published between 2000 and 2012 call for establishing a normal activity baseline. Auditors also pointed to a post-Snowden, nonpublic February 2014 directive on protecting national security systems from insider threats. The U.S. military's 2000 Final Report of the Insider Threat Integrated Process Team instructs organizations to come up with a specific list of employee behaviors that should be tracked online, because otherwise managers will suffer information overload. It will be impossible to baseline normal activity patterns "with the sheer volume of user characteristics data" unless supervisors establish an "inventory of **behavior attributes** and **patterns** grounded in **counterintelligence experience** and

stored to allow for **rapid automatic analysis** and monitoring," the authors of that Defense report wrote. Once a Pentagon organization has selected which employee and system activities to keep tabs on, those attributes should be studied for more than a couple of days. A December 2012 Carnegie Mellon Software Engineering Institute manual, Common Sense Guide to Mitigating Insider Threats, states "the longer the organization monitors the chosen data points, the more reliable the baseline will be." Recommended data points to observe include: Communications between devices: the devices a workstation communicates with and the devices a server communicates with; Bandwidth consumed, especially noting the differences between bandwidth use during and after business hours;. Virtual private network users: **times of access**, bandwidth consumed, **geolocation information**; Ports and protocols; Normal firewall and IDS alerts—Normal alerts may occur when business processes change (e.g., there is increased website traffic). The Carnegie Mellon researchers note, "Organizations may find it challenging to maintain employee privacy while collecting data to establish a baseline."

Link – Data Mining

Computerized data mining key to checking insider threats.

Braun 14 Stephen Braun, reporter at Associated Press. "U.S. intelligence officials to monitor federal employees with security clearances," PBS News. 10 March 2014. http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/. [Premier]

WASHINGTON — U.S. intelligence officials are planning a sweeping system of electronic monitoring that would tap into government, financial and other **databases** to **scan the behavior** of many of the 5 million federal employees with secret clearances, current and former officials told The Associated Press. The system is intended to identify rogue agents, corrupt officials and leakers, and draws on a Defense Department model under development for more than a decade, according to officials and documents reviewed by the AP. Intelligence officials have long wanted a computerized system that could continuously monitor employees, in part to **prevent cases similar to** former National Security Agency analyst Edward **Snowden**. His disclosures bared secretive U.S. surveillance operations. An administration review of the government's security clearance process due this month is expected to support continuous monitoring as part of a package of comprehensive changes. Privacy advocates and government employee union officials expressed concerns that continuous electronic monitoring could intrude into individuals' private lives, prompt flawed investigations and put sensitive personal data at greater risk. Supporters say the system would have safeguards. Workers with secret clearances are already required to undergo background checks of their finances and private lives before they are hired and again during periodic re-investigations. "What we need is a system of continuous evaluation where when someone is in the system and they're cleared initially, then we have a way of monitoring their behavior, both their electronic behavior on the job as well as off the job," Director of National Intelligence James Clapper told Congress last month. Clapper provided lawmakers with few details but said the proposed system would extend "**across the government**," drawing on "**six or seven data streams**." Monitoring of employees at some agencies could begin as early as September and be fully operational across the government by September 2016. The price tag, Clapper conceded, "is going to be costly." In separate comments last week, retiring NSA Director Keith Alexander said intelligence, Defense and Cyber Command officials are collaborating on "insider threat" planning. Recently declassified federal documents show that the NSA is already conducting electronic monitoring of agency staffers involved in surveillance operations. Budget documents released this week show the Pentagon requesting nearly $9 million next year for its insider threat-related research. Current and former officials familiar with the DNI's planning said the monitoring system will collect records from multiple sources of information about employees. They will use private credit agencies, law enforcement databases and threat lists, military and other government records, licenses, data services and public record repositories. During random spot checks, the system's software will sift through the data to spot unusual behavior patterns. The system could also link to outside databases to flag questionable behavior, said the officials, who spoke anonymously because they were not authorized to publicly discuss the plans. Investigators will analyze the information along with data separately collected from social media and, when necessary, polygraph tests, officials said. The proposed system would **mimic monitoring systems** already in use by the airline and banking industries, but it most closely draws from a

10-year-old Pentagon research project known as the Automated Continuous Evaluation System, officials said. The ACES program, designed by researchers from the Monterey, Calif.,-based Defense Personnel and Security Research Center and defense contractor Northrop Grumman, has passed several pilot tests but is not yet in full operation.

Link – Investigations

NSA surveillance key to address insider threats.

Gellman 13 Barton Gellman and Greg Miller. 'Black budget' summary details U.S. spy network's successes, failures and objectives." Washington Post. 29 August 2013. https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html. [Premier]

Counterintelligence The budget includes a lengthy section on funding for counterintelligence programs designed to protect against the danger posed by foreign intelligence services as well as betrayals from within the U.S. spy ranks. The document describes programs to "mitigate insider threats by trusted insiders who seek to **exploit their authorized access** to sensitive information to **harm U.S. interests**." The agencies had budgeted for a major counterintelligence initiative in fiscal 2012, but most of those resources were diverted to an all-hands emergency response to successive floods of classified data released by the anti-secrecy group WikiLeaks. For this year, the budget promised a renewed "focus . . . on safeguarding classified networks" and a strict "review of high-risk, high-gain applicants and contractors" — the young, nontraditional computer coders with the skills the NSA needed. Among them was Snowden, then a 29-year-old contract computer specialist whom the NSA trained to circumvent computer network security. He was copying thousands of highly classified documents at an NSA facility in Hawaii, and preparing to leak them, as the agency embarked on the new security sweep. "NSA will initiate a minimum of 4,000 periodic reinvestigations of **potential insider compromise** of sensitive information," according to the budget, scanning its systems for "**anomalies and alerts**."

Impact – Nukes

Insider threats risk exposing knowledge of nuclear weapons to terrorists

Kirkham 12 Lara Dawn Kirkham, American attorney with Jackson Walker L.L.P. The Insider Threat in the Digital Age: A Case for Electronic Monitoring in the Nuclear Weapons Complex." https://books.google.com/books/about/The_Insider_Threat_in_the_Digital_Age.html?id=qaFQmwEACAAJ. [Premier]

DoD defines the insider threat as, "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in personal injury or loss or degradation of resources or capabilities."6 In the context of this paper, an insider has authorized access, authority, and knowledge of DoD's nuclear weapons complex. The DoD nuclear weapons complex consists of the sites in the United States and abroad that maintain a modern arsenal of strategic nuclear warheads and special nuclear material.7 An insider becomes a threat once he is willing to exploit his position and knowledge of operations or security systems to further unauthorized activities.8 The insider threat to the nuclear weapons complex concerns an insider's potential to abuse his authorized level of system access to endanger the physical integrity of nuclear assets through theft, sabotage, or the deliberate unauthorized release of classified technical or command-and-control system information.9 Insider attacks against nuclear targets are likely to be attempted by anti-nuclear protest groups, mentally unstable individuals, criminals, terrorists, or foreign agents.10 Terrorists or foreign agents present the most serious threat since they are likely a more capable adversary and the nuclear material would be the most valuable to them for political uses.11 Insider adversaries acting in the following three ways are of particular concern to DoD: (1) active non-violent agents who may covertly assist external actors or directly participate in an attack, but will not use force or violence and will surrender if engaged; (2) active violent agents who will use physical force or violence to covertly assist external actors or to directly participate in an attack; or (3) passive agents who weaken the overall security of the system by failing to report unusual behavior or by inadvertently supplying information to external adversaries.12 In the context of the DoD nuclear weapons complex, the most plausible scenarios are a single active non-violent insider colluding with an outsider,13 an active non-violent insider acting alone,14 and a passive insider. Electronic monitoring inputs should initially focus on identifying these types of insiders.

Impact – Bioterror

Insider threats cause bioterror—pathogenic materials, equipment, and empirics prove.

Culp 13 Derrin Culp, research associate at the National Center for Disaster Preparedness, a unit of Columbia University/ "Lessons not learned: Insider threats in pathogen research." Bulletin of Atomic Scientists. 3 April 2013. https://thebulletin.org/2013/04/lessons-not-learned-insider-threats-in-pathogen-research/. [Premier]

Ivins repeatedly authorized the Army to obtain and review his medical and psychiatric treatment records. According to the panel, however, the Army neither examined Ivins' mental health records nor paid close attention to his daily behavior. The expert panel urged organizations to retain the **right to examine** such **records**, to keep that **access as broad as possible**, to use it even in the "absence of specific symptoms or diagnoses," and to withhold access to pathogens from scientists who don't renew privacy waivers. However, the national press and microbiology journals paid little attention to the audacious conclusions. The H5N1 controversy. During the winter of 2011 and 2012, Americans witnessed a prime-time discussion about research on the avian flu virus, known to scientists as H5N1. This organism kills millions of birds annually but, unlike the seasonal flu that makes so many people miserable every winter, H5N1 rarely infects humans. When it does, however, it is incredibly lethal; the World Health Organization estimates that 59 percent of all human cases end in death. The US National Institutes of Health funded two unclassified studies to better understand the likelihood that the H5N1 virus might naturally mutate in ways that would make it more transmissible among humans and, therefore, much more dangerous. When it appeared that at least one of the studies had created in the lab a strain of H5N1 that might be able to spread easily among humans, numerous commentators weighed in on whether publishing the studies would be tantamount to giving terrorists the blueprints for a biological weapon of mass destruction. Scientists and scholars not prone to hyperbole or histrionics indicated that, under certain conditions, the intentional release of a similarly modified virus could cause deaths in the tens or even hundreds of millions. The NSABB, which historically has been strongly opposed to publication restrictions, recommended unanimously that science journals limit what they published, arguing that "the deliberate release of a **transmissible highly pathogenic influenza** A/H5N1 virus would be an **unimaginable catastrophe**." The controversy was so intense that virus researchers around the world adopted an open-ended moratorium on similar research, which they maintained for a year. The risk from "terrorists" dominated the H5N1 discussion, and the potential for scientists to do harm barely lit up the radar -- as if that hadn't happened in a spectacular way just a decade earlier. One of the few people who thought it was germane to worry about researchers using their own findings in malevolent ways was Australian immunologist Ian Ramshaw: "I'm not so worried about bioterrorism. It's the disgruntled researcher who is dangerous." Rutgers microbiologist Richard Ebright, commenting at the time on the proposed Select Agent updates, wrote that failure to mandate video monitoring, a two-person rule, and psychological assessments for scientists working with the most dangerous pathogens "would represent a failure to learn lessons from the 2001 anthrax mailings [and] to address the 'insider threat' responsible for the 2001 anthrax mailings."

Competitiveness Module

The US is a target for espionage. An attack would hurt the economy, military, and economic competitiveness.

Poteat 14 Gene, president of the Association of Former Intelligence Officers. "COUNTERINTELLIGENCE, HOMELAND SECURITY AND DOMESTIC INTELLIGENCE." AFIO. 3 April 2014. http://www.afio.com/publications/Counterintelligence_(Poteat)_2014Apr03_DRAFT.pdf. [Premier]

In the present global economy, economic competition has been increasingly important in relation to military confrontations in world affairs. America's intellectual property, industrial and trade secrets are not only the basis of our strong economy and military, but also our economic competitiveness—and the loss of it through economic espionage to foreign governments poses a serious threat to the future of our nation. Economic espionage is a relatively low risk enterprise with extremely high pay off—with little consequences even when caught. The technologically-advanced strong U.S. economy is a priority target for our competitors and the present economic espionage feeding frenzy taking place is now being carried out by both friend and foe alike, for both economic and defense reasons. This economic espionage is an entirely new challenge for counterintelligence and led to the passing of the Economic Intelligence Act of 1996. There is, nonetheless, a widely held perception that the end of the Cold War means that other than a few scattered terrorism and drug problems we no longer face a truly serious foreign threat to our national security, and that these past threats have turned into nothing more than normal economic competition, or business as usual. The Economic Intelligence Act of 1996 thus far has failed to have much impact.5

Heg

Link – Power Projection

Intel-based hegemony allows the US to be present on a global scale—maintaining NSA flexibility is key to cost-saving security and global power projection—only way to prevent total collapse

McCoy 14 Alfred, J.R.W. Smail Prof of History @ Univ of Wisconsin-Madison. "Surveillance and Scandal: Time-Tested Weapons for US Global Power." The Nation. 21 January 2014. http://www.thenation.com/article/surveillance-and-scandal-time-tested-weapons-us-global-power/. [Premier]

Once upon a time, such surveillance was both expensive and labor intensive. Today, however, unlike the US Army's shoe-leather surveillance during World War I or the FBI's break-ins and phone bugs in the Cold War years, the NSA can monitor the entire world and its leaders with only 100-plus probes into the Internet's fiber optic cables. This new technology is both omniscient and omnipresent beyond anything those lacking top-secret clearance could have imagined before the Edward Snowden revelations began. Not only is it unimaginably pervasive, but **NSA surveillance is also a particularly cost-effective strategy compared to just about any other form of global power projection**. And better yet, it fulfills the greatest imperial dream of all: to be omniscient not just for a few islands, as in the Philippines a century ago, or a couple of countries, as in the Cold War era, but **on a truly global scale**. In a time of increasing imperial austerity and exceptional technological capability, everything about the NSA's surveillance told Washington to just "go for it." This cut-rate mechanism for both projecting force and preserving US global power surely looked like a no-brainer, a must-have bargain for any American president in the twenty-first century—before new NSA documents started hitting front pages weekly, thanks to Snowden, and the whole world began returning the favor. As the gap has grown between Washington's global reach and its shrinking mailed fist, as it struggles to maintain 40 percent of world armaments (the 2012 figure) with only 23 percent of global gross economic output, **the United States will need to find new ways to exercise its power far more economically.** As the Cold War took off, a heavy-metal US military—with 500 bases worldwide circa 1950—was sustainable because the country controlled some 50 percent of the global gross product. But as its share of world output falls—to an estimated 17 percent by 2016—and its social welfare costs climb relentlessly from 4 percent of gross domestic product in 2010 to a projected 18 percent by 2050, **cost-cutting becomes imperative if Washington is to survive as anything like the planet's "sole superpower."** Compared to the $3 trillion cost of the US invasion and occupation of Iraq, the NSA's 2012 budget of just $11 billion for **worldwide surveillance and cyberwarfare looks like cost saving the Pentagon can ill-afford to forego**.

Link – Perception

Mass surveillance is vital to maintaining US hegemony—the AFF creates a perception of global weakness that wrecks both domestic and foreign deterrence credibly.

Van Cleave 13 Michelle, MA and BA in International Relations @ USC, JD @ USC School of Law, former National Counterintelligence Executive under George W. Bush. "What It Takes: In Defense of the NSA." World Affairs. November/December 2013. http://www.worldaffairsjournal.org/article/what-it-takes-defense-nsa. [Premier]

Two inherent qualities make US intelligence unique among the world's intelligence services. The first is its accountability and unparalleled openness to public scrutiny and the rigorous oversight of the political process. The fact that we measure these things against civil liberties, and bring them under the careful checks and balances of our Constitution, is the bedrock of their strength. Even more fundamentally, US intelligence is part of the great experiment in governance that is our democratic republic. Beginning with George Washington's first State of the Union Address, in which he requested a secret fund for clandestine activities, intelligence has been an instrument to achieve the broad goals of the American people and the policies advanced by their duly elected representatives. That is why **any rupture between public confidence and the US intelligence enterprise is so destructive.** It is also why America's adversaries have long sought to provoke one.¶ During the Cold War, the KGB expended a great deal of energy and treasure in undermining the credibility and effectiveness of US intelligence in general and the CIA in particular. Soviet disinformation campaigns included some breathtaking lies, deceptions, and fantastic tales (e.g., forged documents, planted news reports, and grotesque accusations that the CIA was responsible for trafficking in baby parts, assassinating President Kennedy, and inventing AIDS).¶ It took decades for the CIA to recover from the Church Committee investigations of the 1970s—years that the Soviets used to advantage in undermining pro-Western governments, supporting insurgencies, and implanting spies. And here we go again.¶ Whatever Snowden may have had in mind when he decided to break his oath, the secrets he disclosed have been used to discredit US intelligence among the very democratic populations that depend most on the American defense umbrella. Across Europe, there have been lawsuits to stop NSA operations. Round two of Snowden's leaks included purported US collection activities directed against members of the European Union, so the EU, the French, the Germans, and others lodged diplomatic complaints and suspended trade and other talks and loudly proclaimed their indignation. (This is more than a little hypocritical, given their own intelligence activities against one another—not to mention the value they derive from ours.)¶ To make matters worse, a whole series of damaging leaks in recent years, ranging from WikiLeaks to include some from the highest levels of the US government, have called into question America's reliability as an intelligence partner. For friendly intelligence services, trusting the Americans to keep secrets secret has become a far riskier proposition. In fact, our stock as an intelligence partner has never been lower, which is exceedingly worrisome in an era when we rely so heavily on liaison services for essential intelligence about terrorist targets.¶ For American intelligence personnel, doing their jobs has become that much more difficult and that much more thankless. You can be sure that the **Russians, the Chinese, and others**, knowing about the demoralizing effects of the Snowden leaks, **are** working overtime **pursuing** new **recruitment** prospects within US intelligence ranks. They know from long experience that **low morale is a key factor in persuading** Americans to their own country.¶ Today, there are more Russian intelligence personnel operating in the United States than there were at the height of the Cold War, and they are far from alone. By some counts, China is here in even greater numbers, and even more active against us through cyber means. Add to that the Cubans, the Iranians, and most of the rest of the world's governments—plus some thirty-five suspected terrorist organizations—all here, taking advantage of the freedom of movement, access, and anonymity afforded by American society.¶ And then there is the phenomenon of the hacker culture and virtual anarchists like "Anonymous," which is hard at work to set the conditions for what it calls a "global secrets meltdown." Their ostensible plan is to recruit individuals to infiltrate governments to steal classified information or enable Anonymous hackers to steal it. Then, when the message "do it now" goes out, they will simultaneously reveal all of the world's secrets (but of course mostly concentrated in the West because that's where the access is). It may sound ridiculous until you realize just how many disaffected, cynical youth like Snowden are drawn to

these circles to find some sense of belonging and self-importance.¶ ¶ The United States has built a global intelligence apparatus because it has global interests and global responsibilities. We have taken seriously the duties of leader of the free world, as two world wars, Korea, Vietnam, Afghanistan, Iraq, and freedom fighters in many parts of the world can attest.¶ **None of these duties** in the last sixty years **could have been met without the** exceptional resources **of NSA.** Successive presidents and Congresses, entrusted with preserving and defending our freedom, have judged **these investments to be vital to our nation's security.** They have protected the core secrets that enable collection programs to succeed, as have those in US business and industry who have been integral to their success. **The unquestioned qualitative edge of US intelligence has been as essential to defending this country and preserving our freedom** as have the forces we have built to arm and equip our military.¶ But time has not stood still. **China is attacking computer systems throughout the world**, stealing information and implanting features to enable future control. China's prominence in IT commercial markets means that they are in the supply chain, and their market share is growing as part of a purposeful, state-run program for strategic position. **A long roll call of spies** from Russia, China, Cuba, and other nations **have targeted** the **essential secrets** of US intelligence capabilities in order to be able to defeat them. And now they have the Snowdens and the WikiLeakers of the world helping them out.¶ **Interconnected global networks** of digital data **have become the single most important source of intelligence warning** of threats, enabling our defense at home and the advancement of freedom abroad. **To say "hands off,"** as some shortsighted privacy advocates have been doing, **will not preserve our liberties, it will endanger them.** It should be possible for an enlightened citizenry to empower government action in that sphere without forfeiting the very rights that our government exists to secure. That challenge is, at the very least, a part of the continuing experiment that is our democracy.

Impact – Turns Case

Receding American military power greenlights autocratic revisionism and collapses democracy – causes the mass authoritarianism they say is bad.

Joshi 18 Shashank Joshi, senior research fellow at the Royal United Services Institute (RUSI). He has been a research associate at the Changing Character of War Programme at the University of Oxford, regularly lectured at the Defence Academy of the United Kingdom,. "Authoritarian Challenges to the Liberal Order." Institute for Global Change. 21 June 2018. https://institute.global/insight/renewing-centre/authoritarian-challenges-liberal-order. [Premier]

What does this mean for democracies? Autocracies present a **series** of **individual challenges** to their local rivals: **Russia** to the **Baltic states**, **China** to **Taiwan** and **North Korea** to **South Korea**, for instance. But the problem they pose to **world order** is **larger than the sum of these issues**. It is, rather, an **ideological** and **systemic challenge** that will **reshape the norms** of international relations. Will these norms reflect liberal principles such as openness, rule following and individual rights or competing authoritarian ones such as secrecy, arbitrariness and state power?

This competition over norms will influence not only Western liberal democracies but also the **wider multipolar order** that is emerging. In regions with weak political institutions or nascent democracies—parts of Africa, South and Southeast Asia, and East and Southeast Europe—the regional order is especially **malleable**. If authoritarian states can **shape these regions** in their **own image**, this **bolsters their global standing** and puts liberal democracy further on the **back foot**. This argument does not require an acceptance that democracies always act in liberal ways or adhere to a single and consistent set of norms. Authoritarian states also differ widely in levels of openness and repression, the balance between civilian and military authority, and civil versus political freedoms.11 Yet despite this variety, there remain systematic differences between democratic and authoritarian states in attitude, inclination and values—and this has important foreign policy implications.

TYPES OF AUTHORITARIAN CHALLENGE

The authoritarian challenge to liberal democracy can be broken down into six categories.

The Military Challenge

Authoritarian states represent the most serious military threat to the democracies of Europe and Asia. **Russia** has **dissolved existing norms** regarding the use of force, conducting in Europe the first **annexation of territory** and the first use of **chemical weapons** since the Second World War.12 Russia's use of **hybrid warfare**, which prioritises **secrecy, deception** and **political warfare**, presents a **particular danger** to **rule-bound open societies**.13 China, though more cautious, has also demonstrated **increasingly assertive behaviour** in the South China Sea, including the **militarisation of reclaimed islands**, the **rejection of arbitration efforts** and an **escalation** of the country's border dispute with India.14

The military challenge posed by authoritarian states is not a quirk of the past few years. Russian and Chinese behaviour is **rooted** in their **resentment of the Western order**, **ambition for great power status** and **fear of Western power**.15 **All three of these drivers are shaped by these countries' authoritarian political systems**. The **best available scholarship** continues to show that democracies enjoy **more peaceful relations** with other democracies than with **autocracies**, suggesting that authoritarian states are **intrinsically more likely** to be **threatening**.16 Among states that ratify treaties governing the laws of war, democracies are also more likely to comply with these rules than autocracies are.17

Impact – War

Primacy prevents great-power conflict — multipolar revisionism fragments the global order and causes nuclear war.

Brands & Edel 19 Hal Brands; PhD, Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies, Charles Edel; PhD, Senior Fellow and Visiting Scholar at the United States Studies Centre at the University of Sydney. "The Lessons of Tragedy: Statecraft and World Order." Ch. 6: Darkening Horizon. Yale University Press. 2019. [Premier]

Each of these geopolitical challenges is different, and each reflects the distinctive interests, ambitions, and history of the country undertaking it. Yet there is **growing cooperation** between the countries that are **challenging** the **regional pillars of the U.S.-led order. Russia** and **China** have **collaborated** on issues such as energy, sales and development of **military technology**, opposition to additional U.S. military deployments on the Korean peninsula, and naval exercises from the South China Sea to the Baltic. In Syria, Iran provided the **shock troops** that helped keep Russia's ally, Bashar al-Assad, in power, as Moscow provided the air power and the diplomatic cover. "Our **cooperation** can **isolate America**," supreme leader Ali Khamenei told Putin in 2017. More broadly, what links these challenges together is their **opposition** to the constellation of **power, norms, and relationships** that the U.S.-led order entails, and in their propensity to use **violence**, coercion, and intimidation as means of making that opposition **effective**. Taken collectively, these challenges constitute a **geopolitical sea change** from the post-Cold War era.

The revival of **great-power competition** entails higher international tensions than the world has known for decades, and the revival of **arms races, security dilemmas**, and **other artifacts** of a more **dangerous past**. It entails **sharper conflicts** over the international rules of the road on issues ranging from freedom of navigation to the illegitimacy of altering borders by force, and **intensifying competitions** over states that reside at the intersection of rival powers' **areas of interest**. It requires confronting the prospect that **rival powers** could **overturn** the **favorable regional balances** that have **underpinned** the U.S.-led order for decades, and that they might construct **rival spheres of influence** from which America and the liberal ideas it has long promoted would be excluded. Finally, it necessitates recognizing that great-power rivalry could lead to **great-power war**, a prospect that seemed to have followed the Soviet empire onto the ash heap of history.

Both **Beijing** and **Moscow** are, after all, **optimizing their forces** and **exercising aggressively** in preparation for potential **conflicts** with the United States and its allies; Russian doctrine explicitly emphasizes the limited use of **nuclear weapons** to achieve escalation dominance in a war with Washington. In Syria, U.S. and Russian forces even came into **deadly contact** in early 2018. American airpower decimated a contingent of government-sponsored Russian mercenaries that was attacking a base at which U.S. troops were present, an incident demonstrating the increasing boldness of Russian operations and the corresponding potential for escalation. The world has not yet returned to the epic clashes for global dominance that characterized the twentieth century, but it has returned to the **historical norm** of **great-power struggle**, with all the associated dangers.

Those dangers may be even greater than most observers appreciate, because if today's great-power competitions are still most intense at the regional level, who is to say where these competitions will end? By all appearances, Russia **does not simply want to be** a "**regional power**" (as Obama cuttingly described it) that dominates South Ossetia and Crimea.37 It **aspires** to the **deep European** and **extra-regional impact** that **previous incarnations** of the Russian state enjoyed. Why else would Putin boast about how far his troops can drive into Eastern Europe? **Why else** would Moscow be **deploy**ing military power

into the **Middle East?** **Why else** would it be continuing to cultivate intelligence and **military relationships** in regions as remote as **Latin America?**

Likewise, China is **today** focused primarily on securing its own **geopolitical neighborhood**, but its ambitions for **tomorrow** are **clearly much bolder.** Beijing probably does not envision itself fully overthrowing the international order, simply because it has profited far too much from the U.S.-anchored global economy. Yet China has nonetheless positioned itself for a **global challenge** to **U.S. influence**. Chinese military forces are deploying **ever farther** from China's immediate periphery; Beijing has **projected power** into the **Arctic** and **established bases** and **logistical points** in the **Indian Ocean** and **Horn of Africa**. Popular Chinese movies depict Beijing replacing Washington as the dominant actor in sub-Saharan Africa—a fictional representation of a real-life effort long under way. The **Belt and Road Initiative** bespeaks an aspiration to **link** China to countries throughout **Central Asia, the Middle East, and Europe**; BRI, AIIB, and RCEP look like the beginning of an alternative institutional architecture to rival Washington's. In 2017, Xi Jinping told the Nineteenth National Congress of the Chinese Communist Party that Beijing could now "**take center stage in the world**" and act as an **alternative** to **U.S. leadership**.38

These ambitions may or may not be realistic. But they demonstrate just how significantly the world's leading authoritarian powers desire to shift the global environment over time. The **revisionism** we are seeing today may therefore be **only the beginning**. As China's power **continues to grow,** or if it is successful in **dominating the Western Pacific**, it will **surely move on** to **grander endeavors**. If Russia reconsolidates control over the former Soviet space, it may seek to bring parts of the former Warsaw Pact to heel. Historically, this has been a recurring pattern of **great-power behavior**—interests **expand with power**, the appetite **grows** with the eating, **risk-taking** increases as **early gambles** are seen to **pay off**.39 This pattern is precisely why the revival of great-power competition is so concerning—because **geopolitical revisionism** by **unsatisfied major powers** has so often presaged **intensifying international conflict**, confrontation, and even **war**. The great-power behavior occurring today represents the warning light flashing on the dashboard. It tells us there may be still-greater traumas to come.

The threats today are compelling and urgent, and there may someday come a time when the balance of power has shifted so markedly that the postwar international system cannot be sustained. Yet that moment of failure has not yet arrived, and so the goal of U.S. strategy should be not to hasten it by giving up prematurely, but to push it off as far into the future as possible. Rather than simply **acquiescing** in the **decline** of a world it spent generations building, America should **aggressively bolster its defenses**, with an eye to **preserving** and perhaps even selectively **advancing** its remarkable achievements.

Circumvention

Link – Other Programs

Redundant capabilities from other agencies circumvent

Schneier 15 Bruce Schneier, 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. "Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World." 2015. https://books.google.com/books/about/Data_and_Goliath.html?id=_grPBgAAQBAJ. [Premier]

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.

A litany of other programs will just substitute for the NSA.

Cohn and Crocker 15 Cindy & Andrew, researchers at the Electronic Frontier Foundation. "Don't Worry, The Government Still Has Plenty Of Surveillance Power Despite Section 215 Sunset." 2 June 2015. www.defendingdissent.org/now/dont-worry-the-government-still-has-plenty-of-surveillance-power-despite-section-215-sunset/. [Premier]

The story being spun by the defenders of Section 215 of the Patriot Act and the Obama Administration is that if the law sunsets entirely, the government will lose critical surveillance capabilities. The fearmongering includes President Obama, who said: "heaven forbid we've got a problem where we could've prevented a terrorist attack or could've apprehended someone who was engaged in dangerous activity but we didn't do so." So how real is this concern? Not very. Section 215 is only one of a number of largely overlapping surveillance authorities, and the loss of the current version of the law will leave the government with a range of tools that is still incredibly powerful. First, there's the most famous use of Section 215—the bulk collection of telephone records by the NSA. Of course, no matter what law the government relies on, bulk surveillance is unconstitutional. But equally importantly, it doesn't work. Every assessment about the bulk collection of telephone records, including two by hand-picked administration panels, have concluded that "collecting it all" hasn't materially aided any terrorism investigation. The same goes for other still-secret bulk surveillance programs under Section 215, the latest evidence of which came in a recently released oversight report by the Justice Department's Office of the Inspector General (OIG). And then there's the matter of targeted investigations. The ACLU's Jameel Jaffer has explainedthat this too is scaremongering, because "the sunset of Section 215 wouldn't affect the government's ability to conduct targeted investigations of terrorist threats." That's because even without Section 215, the government still has broad powers to collect

information during its national security investigations. EFF believes that many of these laws can be scaled back and made more transparent as well, but given the current situation, these are the tools in the national security investigators' toolbox: **Pen Registers:** These allow the government to collect "dialing, routing, addressing, or signaling information" including telephone numbers dialed and Internet metadata such as IP addresses and email headers. There are two pen register statutes, one for foreign intelligence surveillance and one for law enforcement. Both rely require only that the pen register be likely to obtain information relevant to a national security or criminal investigation respectively. Until the end of 2011, the NSA used the Foreign Intelligence Surveillance Act (FISA) pen register statute to conduct mass surveillance of Internet metadata, much as it still uses Section 215 for mass collection of telephone records. **The Pre-Patriot Act Business Records Provision**: Before the passage of the Patriot Act in 2001, FISA contained a provision allowing the government to obtain business records from transportation carriers and storage facilities. Harley Geiger of the Center for Democracy and Technology has pointed out that under a June 1 sunset, FISA would simply revert to this provision**. An ECPA "D Order":** Under Section 2703(d) of the Electronic Communications Privacy Act (ECPA), the government can get a court order for information from ISPs or other communications providers about their customers, including the sorts of metadata the government gets with Section 215. To get a D Order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." **Grand Jury Subpoenas**: Given that Section 215 explicitly says that the FISA Court (FISC) "may only require the production of a tangible thing if such thing can be obtained" with a grand jury subpoena, it's apparent that a grand jury subpoena is a reasonable substitute, at least where a grand jury can be convened. **National Security Letters** (NSLs): Similar to subpoenas, NSLs allow intelligence agencies to collect records from a range of entities including telecommunications providers, financial institutions, credit reporting bureaus, travel agencies and others. Nearly all NSLs include self-certified gag orders, which EFF has successfully challenged as unconstitutional. Nevertheless, the FBI and other agencies can use NSLs to collect much the same information as Section 215, although the government has also misused NSLs to obtain communication records not authorized by the NSL statute. Administrative Subpoenas: Many federal agencies have the authority to issue **subpoenas for customer records** in their normal course of business. These authorities are extremely widespread, comprising 335 different statutes by one count. FISA Warrants: Under FISA, the government can get warrants from the FISC forelectronic surveillance and physical searches in the context of national security investigations. Although these require a higher showing—probable cause—statistics compiled by EPIC show the FISC routinely issues them, and has done so since FISA was passed in 1978.

Link – Foreign

Domestic constraints will just cause the NSA to shift attention abroad.

Chandler and Le 15 Anupam, 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 Uyen, Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law. "Data Nationalism." Emory Law Journal, 64(3). https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/. [Premier]

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.

Link – Other Countries

Other countries like China will spy on the U.S. instead.

Wittes 15 Benjamin, editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution. "Turns out privacy groups are outraged about the OPM Hack-At me." Lawfare. 18 June 2015. https://www.lawfareblog.com/turns-out-privacy-groups-are-outraged-about-opm-hack%E2%80%94-me. [Premier]

The other day, I wrote a little piece about the silence among our self-appointed privacy guardians at the monstrous breach of privacy perpetrated by the Chinese in the OPM hack. The piece made the (I think) modest observation that privacy groups—who have denounced NSA collection obsessively though it takes place under the rule of law and with strict restrictions—have had remarkably little to say about the mass collection of the most sensitive sorts of data, and I spectulated about the reason for that silence: the privacy community is virtually silent. Look on the websites of the major privacy groups and you'll see almost nothing about this program. Don't look for breathless coverage of it on the The Intercept either. The reason? This giant surveillance program isn't being run by the United States government. It's being run against the U.S. government—by the Chinese government. And for some reason, even the grossest of privacy violations—in this case the pilfering of millions of background investigations and personnel records—just doesn't seem so bad when someone other than the United States is doing it. I didn't expect this piece to make me many friends, but I have been amused and a bit surprised by the harsh reactions from a number of privacy groups on Twitter. In particular, Harley Geiger of CDT and Chris Soghoian of the ACLU seemed to take particular umbrage---both issuing lengthy streams of tweets denouncing the piece. Neither made points that seem to me to warrant response. In the flurry of invective, however, there was one point that seemed to me substantial and worth addressing. That was made by the Cato Institute's Julian Sanchez, somewhat crudely, on Twitter, as well as by a correspondent by email: I didn't expect this piece to make me many friends, but I have been amused and a bit surprised by the harsh reactions from a number of privacy groups on Twitter. In particular, Harley Geiger of CDT and Chris Soghoian of the ACLU seemed to take particular umbrage---both issuing lengthy streams of tweets denouncing the piece. Neither made points that seem to me to warrant response. In the flurry of invective, however, there was one point that seemed to me substantial and worth addressing. That was made by the Cato Institute's Julian Sanchez, somewhat crudely, on Twitter, as well as by a correspondent by email: Is Sanchez right here? Should we understand the silence of privacy groups on this score as just reflecting the fact that there's no controversy, that everyone agrees the conduct is terrible? Sanchez goes on to point out that most advocacy work is directed at one's own government. So maybe the privacy groups are making a tactical judgment that it's better to focus on their own government and its policies than that a foreign authoritarian sovereign over which one has no influence. In this account, the issue is not so much a double standard as a hard-headed assessment of where one's energy is best spent. There are several reasons why I think this is not an adequate account of the behavior of the privacy groups in this instance, nd to the extent it does explain their behavior, why I think they are grossly misjudging the merits of the matter. For one thing, human rights groups comment all the time on the behavior of governments over which they have no influence. Glance at the front page of Human Rights Watch's home page and you won't see the implausibility of the group's influencing Russian or Angolan policy inhibiting HRW from talking about what governments are doing. Yes, it's true that democracies subject to human rights suasion tend to get more of it as a result of their responsiveness. But this does not explain the near-total silence on the part of the privacy groups about Chinese behavior on this score. Tilting at authoritarian windmills is part of what human rights advocacy is. Second and more importantly, privacy issues associated with giant international hacks are unlike other human rights issues in at least one fundamental sense. When China abuses due process or stifles free speech or tortures people, or harvests their organs, its victims are its own people. A U.S. advocacy group can reasonably take the position that, though terrible, this is not really that group's problem but a problem between the Chinese government and its people and civil society. Conversely, if you're a privacy group devoted to protecting the privacy of Americans, the OPM hack should be unthinkable to ignore. It is, after all, a far bigger threat to the interests you are pledged to protect than is any activity by your own government. You may have an argument for leaving Chinese domestic collection to Chinese civil libertarians to restrain, but to the extent you don't speak up against the bulk collection of the health records of kids of U.S. federal employees, you are tolerating an absurd double standard in which anyone can ride roughshod over Americans' privacy except the United States government.

Link – Companies

Tech companies will circumvent the plan on behalf of the government.

Greenwald 14 Glenn, constitutional lawyer. "CONGRESS IS IRRELEVANT ON MASS SURVEILLANCE. HERE'S WHAT MATTERS INSTEAD." First Look. 19 November 2014. https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance. [Premier]

1) Individuals refusing to use internet services that compromise their privacy. The FBI and other U.S. government agencies, as well as the U.K. Government, are apoplectic over new products from Google and Apple that are embedded with strong encryption, precisely because they know that such protections, while far from perfect, are serious impediments to their power of mass surveillance. To make this observation does not mean, as some deeply confused people try to suggest, that one believes that Silicon Valley companies care in the slightest about people's privacy rights and civil liberties. As much of the Snowden reporting has proven, **these companies don't care about any of that.** Just as the telecoms have been for years, U.S. tech companies were more than happy to eagerly cooperate with the NSA in violating their users' privacy en masse when they could do so in the dark. But it's precisely because they can't do it in the dark any more that things are changing, and significantly. That's not because these tech companies suddenly discovered their belief in the value of privacy. They haven't, and it doesn't take any special insight or brave radicalism to recognize that. That's obvious. Instead, these changes are taking place because these companies are petrified that the perception of their collaboration with the NSA will harm their future profits, by making them vulnerable to appeals from competing German, Korean, and Brazilian social media companies that people shouldn't use Facebook or Google because they will hand over that data to the NSA. That—fear of damage to future business prospects—is what is motivating these companies to at least try to convince users of their commitment to privacy. And the more users refuse to use the services of Silicon Valley companies that compromise their privacy—and, conversely, resolve to use only truly pro-privacy companies instead—the stronger that pressure will become. Those who like to claim that nothing has changed from the NSA revelations simply ignore the key facts, including the serious harm to the U.S. tech sector from these disclosures, driven by the newfound knowledge that U.S. companies are complicit in mass surveillance. Obviously, tech companies don't care at all about privacy, but they care a lot about that. Just yesterday, the messaging service WhatsApp announced that it "will start bringing end-to-end encryption to its 600 million users," which "would be the largest implementation of end-to-end encryption ever." None of this is a silver bullet: the NSA will work hard to circumvent this technology and tech companies are hardly trustworthy, being notoriously close to the U.S. government and often co-opted themselves. But as more individuals demand more privacy protection, the incentives are strong. As The Verge notes about WhatsApp's new encryption scheme, "'end-to-end' means that, unlike messages encrypted by Gmail or Facebook Chat, WhatsApp won't be able to decrypt the messages itself, even if the company is compelled by law enforcement."

Link – Lawyering

Creative lawyering guarantees circumvention.

Redmond 14 Valerie, J.D. Candidate, Fordham University School of Law. "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. 2014. https://ir.lawnet.fordham.edu/ilj/vol37/iss3/3/. [Premier]

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

Impact – Confidence

Circumvention hurts public confidence even more.

Seamon 8 Richard, Professor, University of Idaho College of Law. "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. [Premier]

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

Impact – Econ

Private-sector surveillance tanks consumer confidence in the economy

Michaels 8 Jon D. , Acting Professor, UCLA School of Law. "ARTICLE: All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror." California Law Review, 96 Calif. L. Rev. 901. August 2008. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1279867. [Premier]

Even if a given informal partnership is not aimed at defying governing legal requirements, a range of harms may still follow from the ostensibly lawful decision to proceed by handshake. For instance, left to their own devices, both corporations and intelligence agencies may systematically undervalue the social costs associated with the commodity being traded (i.e., private information) - and thus traffic in an inordinately high amount of citizens' personal information. n161 As in the case of industrial regulation of pollution, the possibility of exposing or misusing individuals' personal data is not fully internalized by the parties to the given transaction. Therefore, irrespective of what value society as a whole would assign to the personal information in question, n162 the parties to the transaction peg it comparatively lower. n163 In other words, without the government having to resort to legal process (e.g., by obtaining ex ante authorization and compelling corporate cooperation, n164), the [*938] "informal market" may transfer more information with fewer safeguards than is socially optimal, or even necessary. n165 If, on the other hand, the Executive and the corporations were required to internalize these social costs (say, if a robust oversight regime existed or if private rights of action were readily enforceable), n166 it is likely that the parties would have a greater incentive to reduce instances of over-trafficking in the information and thus better abide by whatever agreed-upon privacy protections were in place. This result would be similar to how corporations respond when forced by outside interests to come to terms with an environmental externality. n167¶ Second, under any of the possible arrangements agreed to voluntarily or via legal compulsion, if word gets out that such partnerships exist for the purpose of domestic-intelligence gathering, there could be a **chilling effect**. Some individuals would be less candid on the telephone and over email (especially when voicing political dissent), and expressive activities would [*939] suffer. n168 Certainly, if such a chilling effect occurred, it would set in **no matter what type** of private-public intelligence-gathering partnership was reported by the press; but, if the arrangement were described as having been regulated pursuant to the dictates of the law, individuals could take some solace in the fact that the partnership's activities were accountable and being monitored for a requisite showing of cause. n169 They might also find some comfort in the fact that the firms were evidently protective of their customers, giving out information only upon pains of legal compulsion.¶ By contrast, when a legally informal relationship is exposed by the media, a consumer could reasonably fear that **intelligence-gathering intrusions lack meaningful limits**. Consider a counterfactual about New York's Container Inspection Program, which involves police officers conducting random searches of subway passengers in an effort to locate or deter concealed explosives. n170 While many passengers may find the random search itself to be bothersome and intrusive, they at least know that as a matter of unambiguous law the agents are forbidden from looking through reading materials or collecting personally identifying information about those searched. n171 If suddenly, however, it came to light that the police had mini-hand scanners and, notwithstanding the clear limitations on their discretion, were secretly cataloging personal information and triangulating it with time/location of people's travel and reading habits, it may well be the case that, on the margins, people may choose to take the bus (at least when they are carrying particularly personal materials). Thus, informality, and the corresponding uncertainty that [*940] attaches, may excessively chill expression or limit freedoms. n172¶ Third, and building on the previous point, evidence that any private-public surveillance program operated without complying with the relevant regulatory requirements is likely to engender **distrust of private industry writ large**. Individuals confronted with the realities of legally informal relationships have no reason to believe that journalists or government watchdogs have smoked out all of the possible collaborations of that kind. Instead, people have cause for suspecting that if such partnerships exist in realms A and B, the government might just as likely be doing something improper in realms C and D, too. n173 These worries are only **compounded** when revelation of such partnerships, including the infamous NSA warrantless eavesdropping program, prompts an unrepentant President to insist that Congress grant retroactive legal immunity to the private parties involved. n174

Disease

Link – Public Health

Rigid health privacy protections collapses public health – expansive surveillance key

Fiarchild et al. 7 Amy Fairchild. associate professor in the Department of Sociomedical Sciences and assistant director for scholarly and academic affairs at the Center for the History and Ethics of Public Health at the Joseph L. Mailman School of Public Health, Columbia University in New York City, Ronald Bayer, professor of public health and codirector of the Center for the History and Ethics of Public Health at the Joseph L. Mailman School of Public Health, Columbia University in New York City, and James Colgrove, assistant professor in the Department of Sociomedical Sciences at the Joseph L. Mailman School of Public Health, Columbia University in New York City. "Privacy and Public Health Surveillance: The Enduring Tension." December 2007. Journal of Ethics. http://journalofethics.ama-assn.org/2007/12/mhst1-0712.html. [Premier]

The discovery that cases of paralytic polio in 1955 were caused by a single manufacturer of Salk vaccine, the linkage of toxic shock syndrome to tampons in 1979, the identification of the sentinel cases of AIDS on the East and West coasts in the early 1980s, the recognition of West Nile, SARS, and avian flu at the turn of the twenty-first century—were all the result of surveillance systems, through which alert and troubled physicians could communicate with public health officials, thus enabling emerging patterns to be identified. In each instance, such vigilance made it possible to initiate measures that could limit the human toll. Surveillance serves as the eyes of public health. Name-based reporting of cases has provided the foundation for planning, intervention, and prevention and has been critical for epidemiological research into patterns of morbidity and mortality for a wide variety of diseases and conditions. Registries have been essential for tracking individuals and their conditions over time. Surveillance has also served to trigger the imposition of public health control measures, such as contact tracing, mandatory treatment, and quarantine. The threat of such intervention and long-term monitoring has provoked alarm and rendered surveillance suspect for those concerned about the unwarranted exercise of state authority in the name of public health. Thus the history of surveillance has been bounded by a promise and a specter. Over the course of the 20th century, public health officials reiterated the importance of surveillance, arguing that without the name and location of diseased individuals they worked "in the darkness of ignorance" and might "as well hunt birds by shooting into every green bush" [1]. It was the prospect of what surveillance might offer that raised hopes—for the delivery of services, for lifesaving knowledge, and for protection of individuals and communities. Hermann Biggs, a titanic figure in the history of public health, who was perhaps the most important late 19th- and early 20th-century architect and philosopher of U.S. public health surveillance, made it clear that names of the diseased were never collected "in order to keep clerks or adding machines busy" [2]. Toward the end of the 20th century, Surgeon General David Satcher would state the value of surveillance as plainly as had Biggs: "In public health, we can't do anything without surveillance. that's where public health begins" [3]. When surveillance opened the doors to vital services and knowledge, its subjects could well become among its most ardent advocates, thus underscoring a politics that goes beyond the politics of privacy. In the late 19th and early 20th centuries, as public health was extending the ambit of surveillance, the medical community reacted with hostility, particularly when it came to tuberculosis surveillance and seemingly threatened to intrude on the sanctity of the clinical relationship, over which the physician was guardian. Medical Record editor George Shrady thus complained of TB surveillance, The compulsory

step taken is a mistaken, untimely, irrational, and unwise one.... The real obnoxiousness of this amendment to the sanitary code is its offensively dictatorial and defiantly compulsory character. It places the Board [of Health] in the rather equivocal position of dictating to the profession and of creating a suspicion of an extra bid for public applause [4]. "Already," he continued, "the profession as a whole has watched with jealous eye the encroachments of the Board upon many of the previously well-recognized privileges of the medical attendant" [4]. Over time, disease reporting was extended to chronic, noncontagious conditions such as cancer, birth defects, and occupational illnesses. Not only physicians but laboratories were often required to report cases to local health authorities. The surveillance of chronic diseases, of course, differs because these conditions do not represent a direct threat to the health of others. And, indeed, when state and local health departments first began tracking conditions like congenital malformations and cancers in the first half of the 20th century, these initiatives typically served epidemiological or research purposes only. These reporting efforts, critically, also became linked to the assessment and improvement of clinical care. Tumor registries, for example, emphasized patient care improvement since the 1950s and, currently, data from the National Cancer Institute's SEER program (Surveillance, Epidemiology, and End Results Program) are routinely used for quality improvement initiatives. It was not until the AIDS epidemic that activists challenged the long-standing tradition of name-based reporting. Even so, as AIDS has become a more treatable disease, resistance to reporting has all but vanished. In the 1990s, the promulgation of national standards to safeguard the privacy of medical records, as dictated by HIPAA (the Health Insurance Portability and Accountability Act), provoked intense public debate. But there was virtually no opposition to carving out an exception in the guidelines for the reporting of diseases to public health agencies. While there was initial uncertainty among physicians and researchers about whether hospitals could continue to provide cancer data to state registries, the Department of Health and Human Services made clear that HIPAA did not serve as an obstacle to reporting. In the early 20th century it was physicians who spearheaded opposition to surveillance; since the 1970s, patients have often been at the forefront of challenges to reporting diseases. Parents of children with disabilities, for example, successfully changed the terms of birth defects surveillance in Minnesota, requiring the state to allow unwilling parents to opt out of reporting. Patient advocates within the American Diabetes Association forced New York City health officials to place limits on an initiative to track cases of diabetes. But just as often, patients with serious illnesses have pushed for better tracking of their conditions. Breast cancer survivors have emerged as the most ardent defenders of universal name-based cancer reporting, recognizing how important surveillance and the research it makes possible is to their own well-being. Similarly, communities concerned about "cancer clusters" and environmental threats have demanded access to the data that only cancer registries can accumulate. Patients expect their privacy to be protected, of course, but also maintain that a rigid commitment to privacy could hobble the usefulness of registries. In these instances, public health officials, committed to the paramount importance of surveillance, have been extremely wary about disclosing any data that could potentially compromise individual privacy.

Link – Databases

The NSA collaborates with health agencies to surveil health non-profits – they use that data to study disease and prepare for bioweapons.

McLaughlin 16 Jenna McLaughlin is a reporter and blogger covering surveillance and national security. "How the U.S. Spires on Medical Nonprofits and Health Defenses Worldwide." The Intercept. 10 August 2016. https://theintercept.com/2016/08/10/how-the-u-s-spies-on-medical-nonprofits-and-health-defenses-worldwide/. [Premier]

AS PART OF an ongoing effort to "exploit medical intelligence," the National Security Agency teamed up with the military-focused Defense Intelligence Agency to extract "**medical SIGINT**" from the intercepted communications of nonprofit groups starting in the early 2000s, a top-secret document shows.

Medical intelligence can include information about **disease outbreaks; the** ability of a foreign regime to respond to chemical, biological, and nuclear attacks; the capabilities of overseas **drugs companies**; advances in **medical technology**; medical research, and the medical response capabilities of various governments, according to the document and others like it, provided by NSA whistleblower Edward Snowden. The documents show that such intelligence is used in efforts to protect U.S. forces, assess the readiness of foreign armies, create opportunities for U.S. diplomats to build goodwill, uncover chemical weapons programs, identify specific bio-weapons facilities, and study how diseases spread.

The existence and broad contours of U.S. medical intelligence collection have been previously disclosed (as has one of its more nefarious uses, in which the flow of medical supplies would be used to hunt down a targeted individual). But a top-secret, previously-unreleased article published in November 2003 in the NSA's internal newsletter, SIDtoday, details the birth of a collaboration between the agency and the DIA's National Center for Medical Intelligence, then known as the Armed Forces Medical Intelligence Center. (The article is being published along with 262 others by The Intercept today; here are some other highlights.)

Work began when the NSA brought in a DIA expert on infectious diseases to help its hamstrung International Organizations Branch — tasked with spying on non-governmental organizations, or NGOs — **exploit medical intelligence** it collected from the nonprofit groups' reports on outbreaks. The DIA staffer became an NSA "integree" and was granted access to signals intelligence, or SIGINT, that was considered "raw," meaning it had not been edited or stripped of personal information. Topics of interest included "SARS in China, cholera in Liberia, and dysentery, polio, and cholera in Iraq," according the article, which was written by the NSA's "account manager for DIA."

"The timing of the integree's arrival, as it coincided with a worldwide SARS epidemic, could not have been better," the article stated. SARS, a respiratory virus, infected over 8,000 people worldwide, with an epicenter in China, before it was contained.

During that time, the NSA and its partners researched "the effect of the epidemic on the state security apparatus," media coverage of the disease, the political and economic impacts of its spread, as well as the "impact" of SARS on China's People's Liberation Army "readiness" — according to NSA documents about a SARS conference published by The Intercept in May.

But SARS wasn't the only purpose of the coupling, according to the SIDtoday article.

"Efforts to develop related topics will inform and facilitate future endeavors to exploit medical intelligence in the International Organizations Branch," they continued — though it's not clear how else the information might be exploited.

The collaboration joined NSA communication intercepts with NCMI's longstanding expertise on medical issues. Within NCMI, military and civilian experts, mostly medical doctors and researchers working at a facility now based in Fort Detrick in Maryland, study information on diseases and other topics clustering around health, medicine, pharmaceuticals, and biological weapons, with one of the goals being to protect U.S. forces widely deployed abroad.

The joint effort to mine "medical SIGINT" is particularly noteworthy 13 years later, as medical devices and body monitors are increasingly connected to the internet, opening up new possibilities to expand intelligence gathering beyond epidemics and bioweapons and into more focused forms of surveillance. The NSA's deputy director, Richard Ledgett, said in June that the spy agency was "looking … theoretically" at exploiting biomedical devices like pacemakers in order to surveil targets, even as he admitted that there are often easier ways to spy.

The NSA did not comment on the collaboration. Speaking on behalf of DIA, the Office of the Director of National Intelligence did not answer specific questions about the partnership, instead writing, via a spokesperson, that "from forecasting and tracking infectious disease outbreaks to assessing foreign health threats, medical intelligence is key to protecting our deployed forces from a wide range of threats across the globe."

The Evolution of Medical Intelligence Gathering

One of the more prominent examples of focused medical spying came in 2010, when the agency crafted a plan to stow tracking devices with medical supplies bound for an ill Osama bin Laden in order to locate the terrorist leader, as detailed in Snowden documents published by The Intercept last year. It's unclear if the plan was ever carried out.

But the military has been gathering intelligence on medicine, health, and scientific developments in biology since early World War II, according to Dr. Jonathan D. Clemente, a North Carolina physician and researcher who wrote a 2013 report on medical intelligence for The Intelligencer, a journal published by the Association of Former Intelligence Officers. During the war, the Army surgeon general began disseminating public health information about various countries to field commanders and military surgeons prior to combat.

By the later stages of the war, the Allies began seizing foreign medical technology and drugs to improve its own stock — and spying on Germany for any plans it had to unleash a biological weapon.

Medical intelligence programs dissipated and were reborn under the CIA around 1947 — playing an important role in intelligence on the Communist Bloc, and during the Korean War.

After several leadership and name changes, the medical intelligence unit was permanently transferred to the Defense Intelligence Agency in 1992, tasked with "prepar[ing] intelligence assessments and forecasts on foreign military and civilian medical systems, infectious disease and environmental health risks, and biomedical research," according to Clemente.

Concerns about drug-resistant infectious diseases were only heightened after the September 11 attacks, strengthening the need for medical intelligence analysts to monitor aggressors' attempts to weaponize biological tools like anthrax.

Other known partners of agency, now called the National Center for Medical Intelligence, include the National Geospatial Intelligence Agency and the Department of Agriculture.

A former director of the DIA's medical intelligence unit, now a biology professor, Anthony Rizzo, described his mission as "protecting this country from threats that people will never even know we faced."

John Schindler, a writer, former NSA intelligence analyst, and former professor of national security affairs at the U.S. Naval War College described the medical intelligence capabilities in the U.S. government in a blog post as "decidedly unique," claiming the NCMI is "the **only full-fledged medical intelligence outfit on earth."**

Link – EMRs

Privacy regulations impose costs on hospitals that prevent them from adopting EMR systems

Miller and Tucker 9 Amalia R. Miller, Associate Professor of Economics at the University of Virginia, holds a Ph.D. in Economics from Stanford University and an S.B. in Economics from Massachusetts Institute of Technology, and Catherine Tucker, Professor of Marketing at MIT Sloan, Chair of the MIT Sloan PhD Program, received an NSF CAREER Award for her work on digital privacy, the Erin Anderson Award for Emerging Marketing Scholar and Mentor, the Paul E. Green Award for contributions to the practice of Marketing Research and a Garfield Award for her work on electronic medical records, holds a PhD in economics from Stanford University, and a BA from the University of Oxford. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Management Science, 55(7). July 2009. https://pubsonline.informs.org/doi/10.1287/mnsc.1090.1014. [Premier]

At the same time, **privacy laws may impose additional network costs on** hospitals who wish to transfer information electronically, for example, by demanding more of a paper trail, or by requiring more robust software. The design of networked EMR systems with strong security and confidentiality protections involves well-known challenges. Individual consent requirements that can be limited to particular types of information and provider destinations demand a flexibility that is costly to implement (Win and Fulcher 2007). It is more expensive to design a system that has the additional flexibility to limit the flow of information by the type of detail in a patient medical record and by the type of external destination, irrespective of how many patients refuse to have their records shared. **Confidentiality protection** that demands prior patient consent, which can be revoked at any time, also **increases the costs of information exchange.** McCarthy et al. (1999) give details of how privacy legislation that requires subjects to give their consent for each study used in research led to lower response rates. When individual consent was required by state law, it was granted by 19% of individuals, as opposed to 93% of patient records made available directly by providers in states without this privacy protection. Finally, in addition to the fixed costs that are added to the complexity of designing the EMR system, the laws require additional documentation, and that burden increases with the flow of information between providers. Theoretically, therefore, **privacy regulation can affect the fixed or the variable costs of EMR adoption,** and without detailed breakdowns of the costs involved, we cannot distinguish between the two.

Privacy protection inhibits EMR diffusion not by creating a different legal requirement for different record types, but by raising compliance costs. **Complying with privacy laws increases the costs of electronic record systems and**, in particular, **the costs of sharing information.** This is particularly important if one of the key benefits of EMRs is the reduced costs of sharing information as compared with paper records. In this sense, **the laws may pose an institutional barrier to information flow**, which in turn reduces the potential benefits to hospitals from the adoption of EMRs, a technology that would otherwise reduce the physical barriers to information exchange. Although it would be desirable to estimate the effects of privacy regulation on network costs and benefits separately, we observe neither of these outcomes. Using data on adoption decisions, we can identify only the net effect of privacy law on network benefits.

Privately collected data is the backbone of effective health care systems — reduces costs and mortality rates.

Goldfarb and Tucker 12 Avi Goldfarb, Professor of Marketing in the Rotman School of Management at University of Toronto, has published over 50 articles in a variety of outlets in economics, marketing, statistics, computing, and law, holds a PhD from Northwestern, MA from Northwestern, and BAH from Queens University, with Catherine Tucker, Professor of Marketing at MIT Sloan, Chair of the MIT Sloan PhD Program, received an NSF CAREER Award for her work on digital privacy, the Erin Anderson Award for Emerging Marketing Scholar and Mentor, the Paul E. Green Award for contributions to the practice of Marketing Research and a Garfield Award for her work on electronic medical records, holds a PhD in economics from Stanford University, and a BA from the University of Oxford. "Privacy and Innovation." Innovation Policy and the Economy, Chicago Journals, The National Bureau of Economic Research, 12(1). January, 2011. https://www.jstor.org/stable/10.1086/663156. [Premier]

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act, devoted $19.2 billion to increase the use of electronic medical records (EMRs) by health care providers. Underlying this substantial public subsidy is a belief that creating an electronic rather than a paper interface between patient information and health care providers can improve health care quality, facilitate the adoption of new technologies, and also save money.

EMRs are the backbone software system that allows health care providers to store and exchange patient health information electronically. As EMRs diffuse to more medical practices, they are expected to reduce medical costs and improve patient care. For example, they may reduce medical costs by reducing clerical duplication; however, there are no universally accepted estimates concerning how much money EMRs will save. Hillestad et al. (2005) suggest that EMRs could reduce America's annual health care bill by $34 billion through higher efficiency and safety, assuming a 15-year period and 90% EMR adoption.

In contrast, the clinical benefits from EMR systems have been demonstrated in recent empirical work (Miller and Tucker 2011a).1 This research examines effects of the digitization of health care on neonatal outcomes over a 12-year period. Neonatal outcome is a measure commonly used to assess the quality of a nation's health care system and is important in its own right. As we discuss in depth later, Miller and Tucker (2011a) is also directly relevant to the current chapter, as it measures the relationships among health care outcomes, hospitals' adoption of information technology, and state-level privacy regulation.

Miller and Tucker (2011a) find that **a 10% increase in basic EMR adoption would reduce neonatal mortality rates by** 16 deaths per 100,000 live births, **roughly 3% of the annual mean** (521) across counties. Furthermore, they find that a 10% increase in hospitals that adopt both EMRs and obstetric-specific computing technology reduces neonatal mortality by 40 deaths per 100,000 live births. This finding suggests **there are increasing gains from the digitization of health care.** The paper shows that the reduction in deaths is driven by a decrease in deaths from conditions that can be treated with **careful monitoring** and **data about patient histories**. There is no such decrease for conditions where prior patient data are not helpful from a diagnostic standpoint.

Overall, Miller and Tucker (2011a) document that the use of patient data by hospitals helps to improve monitoring and the accuracy of patient medical histories. More broadly, even basic EMR systems can improve the quality of data repositories and ease access to relevant patient information. Adoption of technologies that facilitate data collection and analysis can help hospitals to improve outcomes and perhaps to reduce costs.

Link – Prediction

Digital surveillance predicts outbreak.

Science 2.0 14 Science 2.0. Staff. "Upside to NSA Spying: It May Predict Disease Outbreak." Scientific Blogging. 17 January 2014. https://www.science20.com/news_articles/upside_nsa_spying_it_may_predict_disease_outbreak-127983. [Premier]

U.S. President Barack Obama has been explaining the value of spying on the American public throughout history, as a way of deflecting concern about his administration and government overreach. Critics will dismiss his claims along the lines of 'why it was wrong when Bush did what I do but it is right for me to do it now' rationalization, so he should instead leverage the value spying has in **public health.**

Traditional surveillance methods for detecting infectious diseases such Dengue Fever and Influenza take weeks because it relies on doctors reporting cases. Today, people tend to Google for an online diagnosis before visiting a GP and a paper in Lancet Infectious Diseases says Internet-based surveillance can be a big help.

Take that, people who don't believe the NSA should be hijacking your webcams. Analyzing Google searches isn't even illegal.

Senior author Dr. Wenbiao Hu of Queensland University of Technology says spikes in searches for information about infectious diseases could accurately predict outbreaks of that disease.

"This is because traditional surveillance relies on the patient recognizing the symptoms and seeking treatment before diagnosis, along with the time taken for health professionals to alert authorities through their health networks," Hu said. "In contrast, digital surveillance can provide **real-time detection** of epidemics."

Using digital surveillance through search engine algorithms such as Google Trends and Google Insights, detecting the 2005-06 avian influenza outbreak "Bird Flu" would have been possible between one and two weeks earlier than official surveillance reports.

"In another example, a digital data collection network was found to be able to detect the SARS outbreak more than two months before the first publications by the World Health Organisation (WHO)," Hu said.

"Early detection means early warning and that can help reduce or contain an epidemic, as well alert public health authorities to ensure risk management strategies such as the provision of adequate medication are implemented."

Social media and micoblogs including Twitter and Facebook could also be effective in detecting disease outbreaks

"There is the potential for digital technology to revolutionise emerging infectious disease surveillance," Hu said. "While this study has looked at the effectiveness of digital surveillance systems retrospectively, Australia is well-placed to take the lead in developing a real-time infectious disease warning surveillance system.

"The next step would be to combine the approaches currently available such as social media, aggregator websites and search engines, along with other factors such as climate and temperature, and develop a real-time infectious disease predictor."

He said it was also important for future research to explore ways to apply Internet-based surveillance systems on a global scale.

"The international nature of emerging infectious diseases combined with the globalization of travel and trade, have increased the interconnectedness of all countries and means detecting, monitoring and controlling these diseases is a global concern."

NSA mass surveillance prevents outbreaks.

Mientka 14 Mientka, Matthew. "The NSA's Controversial Mass Surveillance Could Help Thwart Disease Outbreaks." Medical Daily. 19 January 2014. https://www.medicaldaily.com/nsas-controversial-mass-surveillance-could-help-thwart-disease-outbreaks-267456. [Premier]

For many, the massive digital surveillance of American society by the U.S. National Security Agency evinces deep-seated fears of authoritarian dystopia, even as former contractor Edward Snowden gains a mixed status as both traitor and hero, an idealogue who betrayed his oath of secrecy to pursue his own brand of justice. The complexity of balancing individual liberties with the promise of security notwithstanding, the Obama administration might try to soften the government's image by touting another collective benefit of such intelligence gathering — **early warning for infectious disease outbreaks.**

Whereas traditional disease surveillance may take weeks to identify an outbreak, the collection of signals intelligence, as well as something much less sinister — totally legal analysis of Google searches — allows the government to potentially predict future epidemics. Rather than analyzing doctor reports over time, public health authorities might glean real-time information about disease outbreaks, offering the ability to forecast such events like the weather.

Dr. Wenbiao Hu, an investigator from Queensland University of Technology in Australia, told reporters last week that spikes in online searches for infectious diseases might predict outbreaks of disease, an idea long touted by academics in the United States and elsewhere. "This is because traditional surveillance relies on the patient recognizing the symptoms and seeking treatment before diagnosis, along with the time taken for health professionals to alert authorities through their health networks," Hu said, according to Business Standard. "In contrast, digital surveillance can provide real-time detection of epidemics."

By analyzing online searches, scientists might have predicted the 2005-2006 avian influenza epidemic a week or two ahead of official reports that used traditional means. "In another example, a digital data collection network was found to be able to detect the SARS outbreak more than two months before the first publication by the World Health Organization," Hu said. "Early detection means early warning and that can help reduce or contain an epidemic, as well as alert public health authorities to ensure risk management strategies, such as the provision of adequate medication, are implemented."

Investigators next want to incorporate more forms of digital media into the analysis, including social media platforms such as Twitter. “There is the potential for digital technology to revolutionize emerging infectious disease surveillance,” Hu said. “While this study has looked at the effectiveness of digital surveillance systems retrospectively, Australia is well-placed to take the lead in developing a real-time infectious disease warning surveillance system.”

Hu and his colleagues published a paper in November in The Lancet Diseases describing how **increasing numbers** of emerging diseases might be countered with the new growth of **mass digital surveillance**. “The increase in emerging infectious diseases has led to calls for new technologies and approaches for detection, tracking, reporting, and response. Internet-based surveillance systems offer a novel and developing means of monitoring conditions of public health concern, including emerging infectious diseases,” Hu and his team wrote. Although many Americans remain leery of mass surveillance, government health officials expect to make increasingly greater use of mass data.

Link – Pandemic Response

Tracking disease is key to stop COVID and future pandemics – manual contact tracing isn't enough.

Fussell 20 Sidney Fussell is a senior staff writer at WIRED covering surveillance, ad tech, and Silicon Valley's social and political impact. "How Surveillance Could Save Lives Amid a Public Health Crisis." WIRED. 21 March 2020. https://www.wired.com/story/surveillance-save-lives-amid-public-health-crisis/. [Premier]

FOR EACH NEW transmission of coronavirus, imagine the "tick tick tick" of a stopwatch. At least 2 million adults in the US could require hospitalization over the course of the pandemic, the Centers for Disease Control and Prevention estimates; that's more than double the nation's supply of hospital beds. Curfews and social distancing will hopefully help mete out the number of infections slowly—because 2 million patients over 18 months will be more manageable than 2 million over six months. Yet all such predictions are essentially guesswork at this point.

Leaders are looking for guidance on when to close schools or order residents to shelter in place, and whether the measures they've already taken are working. Early research on coronavirus suggests that isolating people soon after they become symptomatic plays the "largest role in determining whether an outbreak [is] controllable."

Officials have **a powerful potential surveillance tool** unavailable in past epidemics: smartphones.

Government officials are anxious to tap the information from phones to help monitor and blunt the pandemic. White House officials are asking tech companies for more insight into our social networks and travel patterns. Facebook created a disease mapping tool that tracks the spread of disease by aggregating user travel patterns.

Such efforts clash with people's expectations of privacy. Now, there's a compelling reason to collect and share the data; surveillance may save lives. But it will be difficult to draw boundaries around what data is collected, who gets to use it, and how long the collection will continue.

One concern: Data collected for one purpose can later be used for another. Privacy experts say transparency is crucial if typically private information is harnessed for public health. Data used to fight Covid-19 could be reused for something else down the road.

"What's really important is for the government to be really clear in articulating what specific public health goals it's seeking to accomplish," said Kelsey Finch, senior counsel at the Future of Privacy Forum, an industry-backed group focused on tech policy. "And how it's limiting the collection of personal data to what's necessary to achieve those very specific goals, and then making sure that there are appropriate privacy safeguards put in place before data starts to change hands."

Even anonymized, aggregate data can inform health efforts. Consider a scenario where city officials close bars and restaurants for a weekend, hoping to reduce the number of new coronavirus infections. But instead, infections increase. Some may be the result of exposures days earlier, but tracking where people went over the weekend could reveal new transmission hot spots.

Some lawyers and academics have suggested that public health officials tap the geofencing capability of phones, to learn who may have been near people infected with the virus. Police have relied on geofencing in investigations, using broad warrants to request information on every smartphone near a crime scene.

Last May, police requested location data from every “Google account that is associated with a device” within 150 meters of a bank robbery. In theory, Google could notify users whose phones were recently near an infected person. Google didn’t respond to a request for comment.

There’s already legal debate over whether such actions would overstep the Fourth Amendment’s restrictions on the government’s ability to search private property. Evan Selinger, a privacy expert and philosophy professor at the Rochester Institute of Technology, says partnerships between tech companies and government agencies could create a "Covid-19 response infrastructure" that incentivizes companies to "find creative ways to benefit from mission creep.”

Some privacy scholars question whether enhanced surveillance in the name of fighting disease can be dialed back once the danger has passed.

“I'm not sure that we should be making longer-term judgments, in an emergency situation, about what the right balance is right now,” said Jennifer Daskal, faculty director of the Tech, Law, and Security program at American University and a former national security official in the Department of Justice. “That often doesn't work out so well.”

Pointing back to 9/11, when Congress granted immense surveillance powers to the federal government, Daskal said decisions made during emergency situations tend to lead to overreach. Another thing to remember: There were no iPhones on 9/11. Technology has progressed rapidly since then, and in some cases, has outpaced the laws meant to govern it. “One of the lessons I hope we learned from 9/11 is that new powers in an emergency situation” should come with preset expirations, she added.

The rapid spread of the disease has prompted even some traditional defenders of personal privacy to acknowledge the potential benefits of digital tracking. “Public policy must reflect a balance between collective good and civil liberties in order to protect the health and safety of our society from communicable disease outbreaks,” the Electronic Frontier Foundation wrote in a blog post earlier this month. But, the group continued, any data collection “must be scientifically justified and … proportionate to the need.”

Balancing privacy and the need to quickly isolate patients is only becoming more complex as companies which individually target and identify individuals are also volunteering their technology. The controversial facial recognition startup Clearview AI says it is in talks with public officials to use its software to identify anyone in contact with people who are infected. The weapons detection company Athena Security claims its AI-enabled cameras can detect the coronavirus by spotting fevers.

One potentially powerful tool for public health officials is contact tracing—identifying the people that an infected person has been around. This reveals potential outbreak hot spots, offers some idea of where the virus may spread next, and importantly, warns officials who to contact next and potentially isolate if they become symptomatic. Earlier this month, the CDC issued a temporary rule requiring airlines to share data on passengers traveling from overseas on request, including addresses, phone numbers, and email.

“Contact tracing is giving you an idea about how many people are being infected, along with a control strategy to stop those people that you've tracked from infecting” others, said Cameron Browne, a mathematical biologist at the University of Louisiana studying the virus’s spread in China. “You need to know where these clusters of cases are coming from and how strong the transmission is going forward. So it is both a control and a surveillance.”

In epidemiology, a “control” is a means of intervention used to stop the spread of a disease. It also, necessarily, involves controlling people. Investigators in China and Singapore, for example, interviewed patients, then reviewed their credit card receipts, personal diaries, and calendars to trace where they'd traveled and with whom they had contact.

In the US, however, that prospect unsettles some. “I'd love to give the federal government all the latitude that they deserve, but the reality is that [we've seen] abuse after abuse after abuse,” said Jake Williams, a cybersecurity expert and former member of the NSA’s hacking unit. “When you start adding in identifiers and email addresses, [physical] addresses, [and] other flights you’ve been on, you start to see patterns of behavior. Now, suddenly we're in a little bit different territory.”

Police databases generally include only those suspected or convicted of a crime. But a disease surveillance database could include lots of people who did nothing other than sit next to an infected person on a flight. It’s deeply troubling, but could become a necessity in urgent times.

“The problem is, I don't actually believe that that’s where the use of the data ends,” Williams said. “I would challenge you to find any government surveillance program, for that matter, that hasn't suffered a large number of abuses.”

At a certain point, however, contact tracing becomes unviable. There can be too many contacts to follow and the path from one infected person to another becomes too muddled. More than 18,000 people in the US have tested positive. Officials in Los Angeles instructed doctors on Friday not to test symptomatic patients if the results wouldn’t change the treatment.

Impact – Disease

Pandemics cause extinction—best models confirm global interconnection and mutation outpace burnout. Ebola proves the potential for extinction, not die off.

Bar-Yam 16 Yaneer Bay-Yam, Complex systems scientist studying social and economic systems, president of the New England Complex Systems Institute. "Transition to Extinction: Pandemics in a connected world." 3 July 2016. http://necsi.edu/research/social/pandemics/transition. [Premier]

The video (Figure 1) shows a simple model of hosts and pathogens we have used to study evolutionary dynamics. In the animation, the green are hosts and red are pathogens. As pathogens infect hosts, they spread across the system. If you look closely, you will see that the red changes tint from time to time — that is the natural mutation of pathogens to become more or less aggressive. Watch as one of the more aggressive—brighter red — strains rapidly expands. After a time it goes extinct leaving a black region. Why does it go extinct? The answer is that it spreads so rapidly that it kills the hosts around it. Without new hosts to infect it then dies out itself. That the rapidly spreading pathogens die out has important implications for evolutionary research which we have talked about elsewhere [1–7]. In the research I want to discuss here, what we were interested in is the effect of **adding long range transportation** [8]. This includes natural means of dispersal as well as unintentional dispersal by humans, like adding airplane routes, which is being done by real world airlines (Figure 2). **When we introduce long range transportation into the model, the success of more aggressive strains changes. They can use the long range transportation to find new hosts and escape local extinction**. Figure 3 shows that the more transportation routes introduced into the model, the more higher aggressive pathogens are able to survive and spread. As we add more long range transportation, there is a critical point at which pathogens become so aggressive that the entire host population dies. The pathogens die at the same time, but that is not exactly a consolation to the hosts. We call this the phase **transition to extinction** (Figure 4). **With increasing levels of global transportation, human civilization may be approaching such a critical threshold.** In the paper we wrote in 2006 about the dangers of global transportation for pathogen evolution and pandemics [8], we mentioned the risk from Ebola. Ebola is a horrendous disease that was present only in isolated villages in Africa. It was far away from the rest of the world only because of that isolation. Since Africa was developing, it was only a matter of time before it reached population centers and airports. While the model is about evolution, it is really about which pathogens will be found in a system that is highly connected, and Ebola can spread in a highly connected world. The traditional approach to public health uses historical evidence analyzed statistically to assess the potential impacts of a disease. As a result, many were surprised by the spread of Ebola through West Africa in 2014. As the connectivity of the world increases, past experience is not a good guide to future events. **A key point about the phase transition to extinction is its suddenness. Even a system that seems stable, can be destabilized by a few more long-range connections, and connectivity is continuing to increase**. So how close are we to the tipping point? We don't know but it would be good to find out before it happens. While Ebola ravaged three countries in West Africa, it only resulted in a handful of cases outside that region. One possible reason is that many of the airlines that fly to west Africa stopped or reduced flights during the epidemic [9]. In the absence of a clear connection, public health authorities who downplayed the dangers of the epidemic spreading to the West might seem to be vindicated. As with the choice of airlines to stop flying to west Africa, our analysis didn't take into

consideration how people respond to epidemics. It does tell us what the outcome will be unless we respond fast enough and well enough to stop the spread of future diseases, which may not be the same as the ones we saw in the past. As the world becomes more connected, the dangers increase. Are people in western countries safe because of higher quality health systems? Countries like the U.S. have highly skewed networks of social interactions with some very highly connected individuals that can be "superspreaders." The chances of such an individual becoming infected may be low but events like a mass outbreak pose a much greater risk if they do happen. **If a sick food service worker in an airport infects 100 passengers, or a contagion event happens in mass transportation, an outbreak could very well prove unstoppable.** Watch this mock video of a pathogen spreading globally through land and air transportation. Long range transportation will continue to pose a threat of pandemic if its impacts cannot be contained.

Impact – Bioweapons

NSA surveillance specifically stops bioweapons.

McLaughlin 16 Jenna McLaughlin is a reporter and blogger covering surveillance and national security. "How the U.S. Spires on Medical Nonprofits and Health Defenses Worldwide." The Intercept. 10 August 2016. https://theintercept.com/2016/08/10/how-the-u-s-spies-on-medical-nonprofits-and-health-defenses-worldwide/. [Premier]

Additional SIDtoday articles further elucidate the NSA's focus on medical intelligence in 2003 — including its strategies to combat possible weapons of mass destruction and coordinate with the new Department of Homeland Security.

One article from August 2003 identifies an NSA project to keep an eye on the evolution of biotechnology in various countries. "Can we … determine the specific features that would distinguish a Bio Warfare Program from a benign civilian pharmaceutical production effort?" the author wrote, identifying a "suspect Iranian [biological warfare] facility" as a target for inspection.

A separate slideshow from April 2013, called "Special Source Operations Weekly" briefs analysts on an intelligence gathering mission into two Iranian universities that the NSA suspected might be involved in state chemical and biological warfare programs.

Their research, involving human trials on patients exposed to chemicals in pesticides, "could also be used in the event of … nerve agent exposure," the slideshow reads. "This type of information enabled [intelligence community] customers, such as NCMI (National Center for Medical Intelligence) … to assess the types of medical countermeasures being developed by Iran, as well as Iran's ability to respond to and protect against [chemical and biological warfare] threats," reads a footnote at the bottom of the slide.

Medical intelligence gathering has continued since then, according to the so-called "black budget" proposed for the 2013 fiscal year, published in February 2012.

The document specifies a request for the NMCI to "expand its warning capability for health and biological events that have strategic implications by fielding more sophisticated analytic tools to forecast, detect, prepare, and respond to foreign health threats, emphasizing models for infectious disease spread and toxic and radiological contaminant dispersion."

Further information from the 2013 budget request identifies other goals of the National Center for Medical Intelligence: tracking "foreign pharmaceutical industry capabilities," "health-related opportunities for US diplomatic/goodwill efforts," "foreign military and civilian health care and response capabilities and trends," and "foreign medical advances for defense against **chemical, biological, radiological, and nuclear warfare."**

And the budget request specifically targeted research in Afghanistan and Pakistan, to gather information about "military and civilian medical capabilities" as well as funds to allow analysts to "support joint targeting and no-strike list selection for medical facilities."

COVID primed the pump for a bioweapon attack – it revealed American vulnerability and overstretched health infrastructure necessary for rapid response.

Lippman & Bertrand **3/19** Natasha Bertrand is POLITICO's national security correspondent, Daniel Lippman is a reporter covering the White House and Washington for POLITICO. "'It is not science fiction anymore': Coronavirus exposes U.S. vulnerability to biowarfare." Politico. 19 March 2020. https://www.politico.com/news/2020/03/19/coronavirus-biowarfare-terror-136194. [Premier]

America's struggle to deal with the spread of the highly infectious new virus **Covid**-19 is bad enough, with the number of confirmed cases surging, hospitals begging for help and entire cities going on lockdown. But it's also exposed just how unprepared the U.S. is for a threat many would-be Cassandras have been warning about for years: a **targeted biological attack**. "When one thinks about what a bioterror attack would look like—it is crystal clear we are not even close to being ready," said former Department of Homeland Security official Daniel Gerstein, now a senior policy researcher at the Rand Corporation. Today's mantra of "flattening the curve" — or lessening the spike in illnesses, thereby slowing the infection rate to reduce the burdens on the health care system — would not apply to a bioterror attack. "The people in that cloud would be infected **all at once**, so you would see a very large **spike** of very sick patients," Gerstein said. As the response to the outbreak from governments at all levels has shown, the U.S. was completely unprepared for a slowly creeping pandemic — let alone a **biological attack** that would **overwhelm it all at once.** Potential biological weapons include anthrax, which, the Centers for Disease Control and Prevention says, "makes a good weapon because it can be released quietly and without anyone knowing"; smallpox, frozen stocks of which are still maintained by the U.S. and Russia; tularemia, also known as rabbit fever, which attacks the skin, eyes, lymph nodes and lungs and was stockpiled by the U.S. military and the former Soviet Union after World War II; and botulism, which is caused by exposure to toxins made by C. botulinum — the most toxic substances known to humankind, which attack the body's nerves and can lead to respiratory failure. More than six weeks into the Trump administration's response effort — which began Jan. 29 with the announcement of a coronavirus task force and, two days later, the declaration of a public health emergency — ramped-up testing for the virus has only just begun, hospital systems say they don't have enough beds and medical supplies to handle the onslaught of anticipated patients, and there is a shortage of respirators, ventilators and other protective equipment for nurses and doctors on the front lines. President Donald Trump, meanwhile, only recently shifted his tone: On Sunday, he called the virus "something we have tremendous control of." By Monday, he was urging people to stay home and beginning to hurl the full might of thefederal government at what he described as "an invisible enemy." But with confirmed cases soaring past 7,000 and now reaching into 50 states, officials are warning privately that it may be as long as 18 months before the pandemic is brought to heel. To biodefense experts, the Trump administration's sluggish response revealed a **dangerous failure** of imagination throughout the system, and showed how unprepared the government still is to handle a **catastrophic** biological **event**.

Presidential Powers

Link – Regulation

NSA surveillance is part of presidential authority, sole commander and chief power is critical to flexibility.

US DOJ 6 Department of Justice. "LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT." Department of Justice Briefing. 19 January 2006. http://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf. [Premier]

As the President has explained, since shortly after the attacks of September 11, 2001, he has authorized the National Security Agency ("NSA") to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. This paper addresses, in an unclassified form, the legal basis for the NSA activities described by the President ("NSA activities"). SUMMARY On September 11, 2001, the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history. Al Qaeda's leadership repeatedly has pledged to attack the United States again at a time of its choosing, and these terrorist organizations continue to pose a grave threat to the United States. In response to the September 11th attacks and the continuing threat, the President, with broad congressional approval, has acted to protect the Nation from another terrorist attack. In the immediate aftermath of September 11th, the President promised that "[w]e will direct every resource at our command—every means of diplomacy, every tool of intelligence, every tool of law enforcement, every financial influence, and every weapon of war—to the destruction of and to the defeat of the global terrorist network." President Bush Address to a Joint Session of Congress (Sept. 20, 2001). The NSA activities are an **indispensable aspect** of this defense of the Nation. By targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda, these activities provide the United States with an early warning system to help avert the next attack. For the following reasons, the NSA activities are lawful and consistent with civil liberties. The NSA activities are supported by the President's well-recognized **inherent constitutional authority as Commander in Chief** and **sole organ** for the Nation in foreign affairs to conduct **warrantless surveillance** of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility. The President has made clear that he will exercise all authority available to him, consistent with the Constitution, to protect the people of the United States.

Curtailing domestic surveillance undermines the sole organ doctrine – which underpins every facet of presidential power

Wood and Webb 11 Dan, Department of Political Science at Texas A&M University, presented to the faculty at Vanderbilt University, Clayton Webb. "EXPLAINING PRESIDENTIAL SABER RATTLING." 17 October 2011. http://www.vanderbilt.edu/csdi/events/Wood_Presidential_Saber_Rattling_112111.pdf. [Premier]

The courts affirmed early on that as sovereign leaders, presidents are the nation's **chief foreign policy representative**. Future Supreme Court Justice John Marshall stated in 1800 when he served in the U.S. House of Representatives —The President is the **sole organ** of the nation in its external relations, and its sole representative with foreign nations.‖ (10 Annals of Congress 613) Relying on Marshall's —sole organ‖ doctrine, Supreme Court Justice George Sutherland wrote in 1937 (United States vs. Curtiss-Wright Export Corp , 299 U.S. 319) —In this vast external realm [foreign policy], with its important, complicated, delicate and manifold

problems, the President alone has the power to speak or listen as a representative of the nation.‖ While the plenary nature of executive authority in foreign relations is not universally accepted (e.g., see the persuasive arguments by **Fisher** 2006, 2007a, 2007b, 2007c, 2007d, 2007e, 2008a, 2008b), ***FOOTNOTE BEGINS*** . 2007d. "Statement by Louis Fisher appearing before the House Committee on the Judiciary, "Constitutional **Limitations on Domestic Surveillance**"." ed. L. L. o. Congress.***FOOTNOTE ENDS*** the modern chief executive relies extensively on the —sole organ‖ doctrine to **define presidential power broadly**, and it is now commonly assumed that presidents are the sole representatives of the nation to the outside world.

Link – Emergencies

A limited emergency exception to the plan is vital to presidential powers.

Seamon 8 Richard, Professor, University of Idaho College of Law. "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. [Premier]

Of course, the President's "genuine emergency" power has limits. The Japanese attack on Pearl Harbor created a "genuine emergency," but that emergency did not last for the entire war.'34 Nor did the attack on Pearl Harbor necessarily justify every measure that the President deemed reasonable, including the mass internment of Japanese Americans.135 The existence of genuine emergency powers in the President-and the relaxation of Bill of Rights limits on those powers-must be limited in time and scope.136 **Otherwise, the separation of powers system cannot work effectively** and Bill of Rights freedoms become fair weather friends. I propose two limits on the President's "genuine emergency" powers.

First, the President's power depends on the legislative framework within which it is exercised. The President can defy an Act of Congress in a national security emergency **only if defiance of the legislation is necessary** to respond to the emergency. If the President can effectively respond to the emergency while obeying the statute, the President lacks power to defy it. 137 Thus, Congress can regulate the President's power to respond to national security emergencies by enacting legislation that gives the President adequate leeway in such emergencies. By the same token, it is the inadequacy of legislation that justifies presidential defiance of the legislation in cases of genuine emergency. 38

Second, the President's emergency powers are residual when Congress has enacted generally valid legislation in the same area. Congress and the President share power in many areas, including the waging of war.139 In matters of shared governance, the separation of powers doctrine gives Congress the power to make rules and the President power-**not to unmake Congress's rules-but to break them when reasonably necessary** in a genuine emergency. 40 For example, in late 2005 Congress enacted a law prohibiting members of the armed forces from torturing people detained in the war on terrorism. 14 1 Assume for the sake of argument that it is possible to conceive of a "genuine emergency" in which the President could reasonably decide it was necessary to defy this prohibition. 42 It is one thing to recognize presidential power to break Congress' rule in a particularly exigent situation, after making an individualized determination that it was necessary to violate the prohibition. It is quite a different matter to recognize presidential power to unmake Congress's rule by promulgating a "program" authorizing torture in broadly defined categories of situations.1 43 One way to express the difference is by saying that, in the second situation, the President is impermissibly exercising legislative power, whereas in the first situation he is exercising irreducible executive power.144 Another way to express the difference is to say that the executive power to act in "emergencies" is limited in scope and duration to that necessary when there is "no time for deliberation., 145 Those limits flow from our system of separated powers.

Impact – War

Surveillance is part of presidential powers to fight wars—any interference in surveillance disrupts this power—wide presidential discretion is key

US DOJ 6 Department of Justice. "LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT." Department of Justice Briefing. 19 January 2006. http://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf. [Premier]

The present circumstances that support recognition of the President's **inherent constitutional authority to conduct the NSA activities** are considerably stronger than were the circumstances at issue in the earlier courts of appeals cases that recognized this power. All of the cases described above addressed inherent executive authority under the foreign affairs power to conduct surveillance in a peacetime context. The courts in these cases therefore had no occasion even to consider the fundamental authority of the President, as Commander in Chief, to gather intelligence in the context of an ongoing armed conflict in which the United States already had suffered massive civilian casualties and in which the intelligence gathering efforts at issue were specifically designed to thwart further armed attacks. Indeed, **intelligence gathering is particularly important** in the current conflict, in which the enemy attacks largely through clandestine activities and which, as Congress recognized, "pose[s] an unusual and extraordinary threat," AUMF pmbl. Among the President's most basic constitutional duties is the duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. The courts thus have long acknowledged the President's inherent authority to take action to protect Americans abroad, see, e.g., Durand v. Hollins, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186), and to protect the Nation from attack, see, e.g., The Prize Cases, 67 U.S. at 668. See generally Ex parte Quirin, 317 U.S. 1, 28 (1942) (recognizing that the President has authority under the Constitution "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war," including "important incident[s] to the conduct of war," such as "the adoption of measures by the military command . . . to repel and defeat the enemy"). As the Supreme Court emphasized in the Prize Cases, if the Nation is invaded, the President is "bound to resist force by force"; "[h]e must determine what degree of force the crisis demands" and need not await congressional sanction to do so. The Prize Cases, 67 U.S. at 670; see also Campbell v. Clinton, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) ("[T]he Prize Cases . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected."); id. at 40 (Tatel, J., concurring) ("[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack **without obtaining prior congressional approval.").** Indeed, "in virtue of his rank as head of the forces, [the President] has certain powers and duties with which **Congress cannot interfere**." Training of British Flying Students in the United States, 40 Op. Att'y Gen. 58, 61 (1941) (Attorney General Robert H. Jackson) (internal quotation marks omitted). In exercising his constitutional powers**, the President has wide discretion**, consistent with the Constitution, **over the methods of gathering intelligence** about

Maintaining effective warfighting capabilities key to sustain global peace – prevents extinction

Barnett 11, Former Senior Strategic Researcher and Professor in the Warfare Analysis & Research Department, Center for Naval Warfare Studies, U.S. Naval War College

(Thomas P.M., The New Rules: Leadership Fatigue Puts U.S., and Globalization, at Crossroads, www.worldpoliticsreview.com/articles/8099/the-new-rules-leadership-fatigue-puts-u-s-and-globalization-at-crossroads)

Events in Libya are a further reminder for Americans that we stand at a crossroads in our continuing evolution as the world's **sole full-service superpower**. Unfortunately, we are increasingly seeking change without cost, and shirking from risk because we are tired of the responsibility. We don't know who we are anymore, and our president is a big part of that problem. Instead of leading us, he explains to us. Barack Obama would have us believe that he is practicing strategic patience. But many experts and ordinary citizens alike have concluded that he is actually beset by strategic incoherence -- in effect, a man overmatched by the job. It is worth first examining the larger picture: We live in a time of arguably the greatest structural change in the global order yet endured, with this historical moment's most amazing feature being its relative and absolute **lack of mass violence**. That is something to consider when Americans contemplate military intervention in Libya, because if we do take the step to prevent larger-scale killing by engaging in some killing of our own, we will not be adding to some fantastically imagined global death count stemming from the ongoing "megalomania" and "evil" of American "empire." We'll be engaging in the same sort of system-administering activity that has marked our stunningly successful stewardship of global order since World War II. Let me be more blunt: As the guardian of globalization, **the U.S. military has been the greatest force for peace the world has ever known**. Had America been removed from the global dynamics that governed the 20th century, the mass murder never would have ended. Indeed, it's entirely conceivable there would now be **no identifiable human civilization left,** once nuclear weapons entered the killing equation**.** But the world did not keep sliding down that path of **perpetual war.** Instead, America stepped up and changed everything by ushering in our now-perpetual **great-power peace**. We introduced the international liberal trade order known as globalization and played loyal Leviathan over its spread. What resulted was the collapse of empires, an explosion of democracy, the persistent spread of human rights, the liberation of women, the doubling of life expectancy, a roughly 10-fold increase in adjusted global GDP and a profound and persistent reduction in battle deaths from state-based conflicts. That is what American "hubris" actually delivered. Please remember that the next time some TV pundit sells you the image of "unbridled" American military power as the cause of global disorder instead of its cure. With self-deprecation bordering on self-loathing, we now imagine a post-American world that is anything but. Just watch who scatters and who steps up as the Facebook revolutions erupt across the Arab world. While we might imagine ourselves the status quo power, we remain the world's most vigorously revisionist force. As for the sheer "evil" that is our military-industrial complex, again, let's examine what the world looked like before that establishment reared its ugly head. The last great period of global structural change was the first half of the 20th century, a period that saw a death toll of about 100 million across two world wars. That comes to an average of 2 million deaths a year in a world of approximately 2 billion souls. Today, with far more comprehensive worldwide reporting, researchers report an average of less than 100,000 battle deaths annually in a world fast approaching 7 billion people. Though admittedly crude, these calculations suggest a 90 percent absolute drop and a 99 percent relative drop in deaths due to war. We are clearly headed for a world order characterized by multipolarity, something the American-birthed system was designed to both encourage and accommodate. But given how things turned out the last time we collectively faced such a fluid structure, we would do well to keep U.S. power, in all of its forms, deeply embedded in the geometry to come. To continue the historical survey, after salvaging Western Europe from its half-century of civil war, the U.S. emerged as the progenitor of a new, far more just form of globalization -- one based on actual free trade rather than colonialism. America then successfully replicated globalization further in East Asia over the second half of the 20th century, setting the stage for the Pacific Century now unfolding.

Executive authority is a conflict dampener.

Royal 11 John-Paul, Institute of World Politics. “War Powers and the Age of Terrorism.” http://www.thepresidency.org/storage/Fellows2011/Royal-_Final_Paper.pdf. [Premier]

The international system itself and national security challenges to the United States in particular, underwent rapid and significant change in the first decade of the twenty-first century. War can no longer be thought about strictly in the terms of the system and tradition created by the Treaty of Westphalia over three and a half centuries ago. Non-state actors now possess a level of destructiveness formerly enjoyed only by nation states. Global terrorism, coupled with the threat of weapons of mass destruction developed organically or obtained from rogue regimes, presents new challenges to U.S. national security and place innovative demands on the Constitution's system of making war. In the past, as summarized in the 9/11 Commission Report, threats emerged due to hostile actions taken by enemy states and their ability to muster large enough forces to wage war: "Threats emerged slowly, often visibly, as weapons were forged, armies conscripted, and units trained and moved into place. Because large states were more powerful, they also had more to lose. They could be deterred" (National Commission 2004, 362). This mindset assumed that peace was the default state for American national security. Today however, we know that threats can emerge quickly. Terrorist organizations half-way around the world are able to wield weapons of unparalleled destructive power. These attacks are more difficult to detect and deter due to their unconventional and asymmetrical nature. In light of these new asymmetric threats and the resultant changes to the international system, peace can no longer be considered the default state of American national security. Many have argued that the Constitution permits the president to use unilateral action only in response to an imminent direct attack on the United States. In the emerging security environment described above, pre-emptive action taken by the executive branch may be needed more often than when nation-states were the principal threat to American national interests. Here again, the 9/11 Commission Report is instructive as it considers the possibility of pre-emptive force utilized over large geographic areas due to the diffuse nature of terrorist networks: In this sense, 9/11 has taught us that terrorism against American interests "over there" should be regarded just as we regard terrorism against America "over here." In this sense, the American homeland is the planet (National Commission 2004, 362). Furthermore, the report explicitly describes the global nature of the threat and the global mission that must take place to address it. Its first strategic policy recommendation against terrorism states that the: U.S. government must identify and prioritize actual or potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and on the run, using all elements of national power (National Commission 2004, 367). Thus, fighting continues against terrorists in Afghanistan, Yemen, Iraq, Pakistan, the Philippines, and beyond, as we approach the tenth anniversary of the September 11, 2001 attacks. Proliferation of weapons of mass destruction (WMD), especially nuclear weapons, into the hands of these terrorists is the most dangerous threat to the United States. We know from the 9/11 Commission Report that Al Qaeda has attempted to make and obtain nuclear weapons for at least the past fifteen years. Al Qaeda considers the acquisition of weapons of mass destruction to be a religious obligation while "more than two dozen other terrorist groups are pursing CBRN [chemical, biological, radiological, and nuclear] materials" (National Commission 2004, 397). Considering these statements, rogue regimes that are openly hostile to the United States and have or seek to develop nuclear weapons capability such as North Korea and Iran, or extremely unstable nuclear countries such as Pakistan, pose a special threat to American national security interests. These nations were not necessarily a direct threat to the United States in the past. Now, however, due to proliferation of nuclear weapons and missile technology, they can inflict damage at considerably higher levels and magnitudes than in the past. In addition, these regimes may pursue proliferation of nuclear weapons and missile technology to other nations and to allied terrorist organizations. The United States must pursue condign punishment and appropriate, rapid action against hostile terrorist organizations, rogue nation states, and nuclear weapons proliferation threats in order to protect American interests both at home and abroad. Combating these threats are the "top national security priority for the United States…with the full support of Congress, both major political parties, the media, and the American people" (National Commission 2004, 361). Operations may take the form of pre-emptive and sustained action against those who have expressed hostility or declared war on the United States. Only the executive branch can effectively execute this mission, authorized by the 2001 AUMF. If the national consensus or the nature of the threat changes, Congress possesses the intrinsic power to rescind and limit these powers.

Sustaining military leadership is key to prevent multiple nuclear conflicts

Brooks, Ikenberry and Wohlforth 13 Stephen, Government Prof at Dartmouth, John, International Affairs Prof at Princeton, John, Government Prof at Dartmouth. "Lean Forward." Foreign Affairs. Jan/Feb 2013. https://www.foreignaffairs.com/articles/united-states/2012-11-30/lean-forward. [Premier]

Of course, even if it is true that the costs of deep engagement fall far below what advocates of retrenchment claim, they would not be worth bearing unless they yielded greater benefits. In fact, they do. The most obvious benefit of the current strategy is that it reduces the risk of a dangerous conflict. The United States' security commitments deter states with aspirations to regional hegemony from contemplating expansion and dissuade U.S. partners from trying to solve security problems on their own in ways that would end up threatening other states. Skeptics discount this benefit by arguing that U.S. security guarantees aren't necessary to prevent dangerous rivalries from erupting. They maintain that the high costs of territorial conquest and the many tools countries can use to signal their benign intentions are enough to prevent conflict. In other words, major powers could peacefully manage regional multipolarity without the American pacifier. But that outlook is too sanguine. If Washington got out of East Asia, Japan and South Korea would likely expand their military capabilities and go nuclear, which could provoke a destabilizing reaction from China. It's worth noting that during the Cold War, both South Korea and Taiwan tried to obtain nuclear weapons; the only thing that stopped them was the United States, which used its security commitments to restrain their nuclear temptations. Similarly, were the United States to leave the Middle East, the countries currently backed by Washington--notably, Israel, Egypt, and Saudi Arabia--might act in ways that would intensify the region's security dilemmas. There would even be reason to worry about Europe. Although it's hard to imagine the return of great-power military competition in a post-American Europe, it's not difficult to foresee governments there refusing to pay the budgetary costs of higher military outlays and the political costs of increasing EU defense cooperation. The result might be a continent incapable of securing itself from threats on its periphery, unable to join foreign interventions on which U.S. leaders might want European help, and vulnerable to the influence of outside rising powers. Given how easily a U.S. withdrawal from key regions could lead to **dangerous competition**, advocates of retrenchment tend to put forth another argument: that such rivalries wouldn't actually hurt the United States. To be sure, few doubt that the United States could survive the return of conflict among powers in Asia or the Middle East--but at what cost? Were states in one or both of these regions to start competing against one another, they would likely boost their military budgets, arm client states, and perhaps even start regional proxy wars, all of which should concern the United States, in part because its lead in military capabilities would narrow. Greater regional insecurity could also produce **cascades of nuclear proliferation** as powers such as Egypt, Saudi Arabia, Japan, South Korea, and Taiwan built nuclear forces of their own. Those countries' regional competitors might then also seek nuclear arsenals. Although nuclear deterrence can promote stability between two states with the kinds of nuclear forces that the Soviet Union and the United States possessed, things get shakier when there are multiple nuclear rivals with less robust arsenals. As the number of nuclear powers increases, the probability of illicit transfers, irrational decisions, accidents, and unforeseen crises goes up. The case for abandoning the United States' global role misses the underlying security logic of the current approach. By reassuring allies and actively managing regional relations, Washington dampens competition in the world s key areas, thereby preventing the emergence of a hothouse in which countries would grow new military capabilities. For proof that this strategy is working, one need look no further than the defense budgets of the current great powers: on average, since 1991 they have kept their military expenditures as A percentage of GDP to historic lows, and they have not attempted to match the United States' top-end military capabilities. Moreover, all of the world's most modern militaries are U.S. allies, and the United States' military lead over its potential rivals .is by many measures growing. On top of all this, the current grand strategy acts as a hedge against the emergence regional hegemons. Some supporters of retrenchment argue that the U.S. military should keep its forces over the horizon and pass the buck to local powers to do the dangerous work of counterbalancing rising regional powers. Washington, they contend, should deploy forces abroad only when a truly

credible contender for regional hegemony arises, as in the cases of Germany and Japan during World War II and the Soviet Union during the Cold War. Yet there is already a potential contender for regional hegemony--China--and to balance it, the United States will need to maintain its key alliances in Asia and the military capacity to intervene there. The implication is that the United States should get out of Afghanistan and Iraq, reduce its military presence in Europe, and pivot to Asia. Yet that is exactly what the Obama administration is doing. MILITARY DOMINANCE, ECONOMIC PREEMINENCE Preoccupied with security issues, critics of the current grand strategy miss one of its most important benefits: sustaining an open global economy and a favorable place for the United States within it. To be sure, the sheer size of its output would guarantee the United States a major role in the global economy whatever grand strategy it adopted. Yet the country's military dominance undergirds its economic leadership. In addition to protecting the world economy from instability, its military commitments and naval superiority help secure the sea-lanes and other shipping corridors that allow trade to flow freely and cheaply. Were the United States to pull back from the world, the task of securing the global commons would get much harder. Washington would have less leverage with which it could convince countries to cooperate on economic matters and less access to the military bases throughout the world needed to keep the seas open. A global role also lets the United States structure the world economy in ways that serve its particular economic interests. During the Cold War, Washington used its overseas security commitments to get allies to embrace the economic policies it preferred--convincing West Germany in the 1960s, for example, to take costly steps to support the U.S. dollar as a reserve currency. U.S. defense agreements work the same way today. For example, when negotiating the 2011 free-trade agreement with South Korea, U.S. officials took advantage of Seoul's desire to use the agreement as a means of tightening its security relations with Washington. As one diplomat explained to us privately, "We asked for changes in labor and environment clauses, in auto clauses, and the Koreans took it all." Why? Because they feared a failed agreement would be "a setback to the political and security relationship." More broadly, the United States wields its security leverage to shape the overall structure of the global economy. Much of what the United States wants from the economic order is more of the same: for instance, it likes the current structure of the World Trade Organization and the International Monetary Fund and prefers that free trade continue. Washington wins when U.S. allies favor this status quo, and one reason they are inclined to support the existing system is because they value their military alliances. Japan, to name one example, has shown interest in the Trans-Pacific Partnership, the Obama administration's most important free-trade initiative in the region, less because its economic interests compel it to do so than because Prime Minister Yoshihiko Noda believes that his support will strengthen Japan's security ties with the United States. The United States' geopolitical dominance also helps keep the U.S. dollar in place as the world's reserve currency, which confers enormous benefits on the country, such as a greater ability to borrow money. This is perhaps clearest with Europe: the EU'S dependence on the United States for its security precludes the EU from having the kind of political leverage to support the euro that the United States has with the dollar. As with other aspects of the global economy, the United States does not provide its leadership for free: it extracts disproportionate gains. Shirking that responsibility would place those benefits at risk. CREATING COOPERATION What goes for the global economy goes for other forms of international cooperation. Here, too, American leadership benefits many countries but disproportionately helps the United States. In order to counter transnational threats, such as terrorism, piracy, organized crime, climate change, and pandemics, states have to work together and take collective action. But cooperation does not come about effortlessly, especially when national interests diverge. The United States' military efforts to promote stability and its broader leadership make it easier for Washington to launch joint initiatives and shape them in ways that reflect U.S. interests. After all, cooperation is hard to come by in regions where chaos reigns, and it flourishes where leaders can anticipate lasting stability. U.S. alliances are about security first, but they also provide the political framework and channels of communication for cooperation on nonmilitary issues. NATO, for example, has spawned new institutions, such as the Atlantic Council, a think tank, that make it easier for Americans and Europeans to talk to one another and do business. Likewise, consultations with allies in East Asia spill over into other policy issues; for example, when American diplomats travel to Seoul to manage the military alliance, they also end up discussing the Trans-Pacific Partnership. Thanks to conduits such as this, the United States can use bargaining chips in one issue area to make progress in others. The benefits of these communication channels are especially pronounced when it comes to fighting the kinds of threats that require new forms of cooperation, such as terrorism and pandemics. With its alliance system in place, the United States is in a stronger position than it would otherwise be to advance cooperation and share burdens. For example, the intelligence-sharing network within

NATO, which was originally designed to gather information on the Soviet Union, has been adapted to deal with terrorism. Similarly, after a tsunami in the Indian Ocean devastated surrounding countries in 2004, Washington had a much easier time orchestrating a fast humanitarian response with Australia, India, and Japan, since their militaries were already comfortable working with one another. The operation did wonders for the United States' image in the region. The United States' global role also has the more direct effect of facilitating the bargains among governments that get cooperation going in the first place. As the scholar Joseph Nye has written, "The American military role in deterring threats to allies, or of assuring access to a crucial resource such as oil in the Persian Gulf, means that the provision of protective force can be used in bargaining situations. Sometimes the linkage may be direct; more often it is a factor not mentioned openly but present in the back of statesmen's minds." THE DEVIL WE KNOW Should America come home? For many prominent scholars of international relations, the answer is yes--a view that seems even wiser in the wake of the disaster in Iraq and the Great Recession. Yet their arguments simply don't hold up. There is little evidence that the United States would save much money switching to a smaller global posture. Nor is the current strategy self-defeating: it has not provoked the formation of counterbalancing coalitions or caused the country to spend itself into economic decline. Nor will it condemn the United States to foolhardy wars in the future. What the strategy does do is help prevent the outbreak of conflict in the world's most important regions, keep the global economy humming, and make international cooperation easier. Charting a different course would threaten all these benefits. This is not to say that the United States' current foreign policy can't be adapted to new circumstances and challenges. Washington does not need to retain every commitment at all costs, and there is nothing wrong with rejiggering its strategy in response to new opportunities or setbacks. That is what the Nixon administration did by winding down the Vietnam War and increasing the United States' reliance on regional partners to contain Soviet power, and it is what the Obama administration has been doing after the Iraq war by pivoting to Asia. These episodes of rebalancing belie the argument that a powerful and internationally engaged America cannot tailor its policies to a changing world. A grand strategy of actively managing global security and promoting the liberal economic order has served the United States exceptionally well for the past six decades, and there is no reason to give it up now. The country's globe-spanning posture is the devil we know, and a world with a disengaged America is the devil we don't know. Were American leaders to choose retrenchment, they would in essence be running a massive experiment to test how the world would work without an engaged and liberal leading power. The results could well be disastrous.

Cyberattacks

Link – Surveillance

Cyber security is a top priority now – new programs ensure safety from attack

Matias 15 Shavit, research fellow at the Hoover Institution and a member of the Jean Perkins Task Force on National Security and Law. "Combating Cyberattacks In The Age Of Globalization." Hoover Institution. 5 March 2015. http://www.hoover.org/research/combating-cyberattacks-age-globalization. [Premier]

Over the past decade, facing the alarming growth of cyberattacks on industry, media, banks, infrastructure and state institutions, there has been an increasing focus of industry and states on building tools to enhance capabilities to combat cybercrime, cyber espionage, cyberterrorism and cyberwarfare, and there is a major shift of funds, efforts, and focus to these areas. Many countries are creating cyber defense institutions within their national security establishments and enhancing their cyber capabilities, including through the creation of dedicated cyberwarfare units within their defense forces. Others are beginning to be aware of the necessity. According to Director of National Intelligence James R. Clapper in a January 29, 2014 Statement for the Record before the Senate Select Committee on Intelligence, the United States estimates that several of the cyber defense institutions created by states will likely be responsible for offensive cyber operations as well. The cyber arena is complex and continuously evolving. Recognizing the critical interlink between the various actors and the need for cooperation and innovation, states are increasingly trying to build cooperation between domestic state cyber institutions and industry and academia, and devise mechanisms for internal cooperation between different state units and agencies. While in the past states kept many of these efforts — including information on the formation of military cyber units — relatively secret, today they increasingly publicize their efforts both nationally and internationally. "Be an Army hacker: This top secret cyber unit wants you" shouts the headline of an April 6, 2013 article in the Military Times, explaining that the US Army is looking for computer-savvy American troops to "turn into crack cyberwarriors" for both offensive and defensive purposes. The United States Cyber Command has already announced that over the next few years it intends to recruit 6,000 cyber experts and create teams of soldiers and civilians to assist the Pentagon in defending US national infrastructure.

Strong NSA Surveillance necessary to stop cyberattacks

Goldsmith 13 Jack. "We Need an Invasive NSA." New Republic. 10 October 2013. http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks. [Premier]

Ever since stories about the National Security Agency's (NSA) electronic intelligence-gathering capabilities began tumbling out last June, The New York Times has published more than a dozen editorials excoriating the "national surveillance state." It wants the NSA to end the "mass warehousing of everyone's data" and the use of "back doors" to break encrypted communications. A major element of the Times' critique is that the NSA's domestic sweeps are not justified by the terrorist threat they aim to prevent.¶ At the end of August, in the midst of the Times' assault on the NSA, the newspaper suffered what it described as a "malicious external attack" on its domain name registrar at the hands of the Syrian Electronic Army, a group of hackers who support Syrian President Bashar Al Assad. The

paper's website was down for several hours and, for some people, much longer. "In terms of the sophistication of the attack, this is a big deal," said Marc Frons, the Times' chief information officer. Ten months earlier, hackers stole the corporate passwords for every employee at the Times, accessed the computers of 53 employees, and breached the e-mail accounts of two reporters who cover China. "We brought in the FBI, and the FBI said this had all the hallmarks of hacking by the Chinese military," Frons said at the time. He also acknowledged that the hackers were in the Times system on election night in 2012 and could have "wreaked havoc" on its coverage if they wanted.¶ Illustration by Harry Campbell¶ 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 Timesconcluded, "Americans will be justified in asking why their lawmakers ... failed to protect them."¶ When catastrophe strikes, the public will adjust its tolerance for intrusive government measures.¶ 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 Timesand 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.¶ Alexander's domestic cybersecurity plans look like pumped-up versions of the NSA's counterterrorism-related homeland surveillance that has sparked so much controversy in recent months. That is why so many people in Washington think that Alexander's vision has "virtually no chance of moving forward," as the Times recently reported. "Whatever trust was there is now gone," a senior intelligence official told Times.¶ 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 undoubted 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.

Link – Encryption

Snowden revelations is creating a commercial market for encryption and other security technologies.

Doctorow 14 Cory, technology columnist for the Guardian. "What happens with digital rights management in the real world?" The Guardian. 5 February 2014. http://www.theguardian.com/technology/blog/2014/feb/05/digital-rights-management. [Premier]

The revelations of the NSA whistleblower Edward Snowden have changed the global conversation about privacy and security. According to a Pew study from last autumn, most American Internet users are now attempting to take measures to make their computers more secure and keep their private information more private. It's hard to overstate how remarkable this is (I devoted an entire column to it in December). For the entire history of the technology industry, there was no appreciable consumer demand for security and privacy. There was no reason to believe that spending money making a product more secure would translate into enough new users to pay for the extra engineering work it entailed. With the shift in consciousness redounding from the Snowden files, we have, for the first time ever, the potential for commercial success based on claims of security. That's good news indeed – because computer security is never a matter of individual action. It doesn't matter how carefully you handle your email if the people you correspond with are sloppy with their copies of your messages. It's a bit like public health: it's important to make sure you have clean drinking water, but if your neighbours don't pay attention to their water and all get cholera, your own water supply's purity won't keep you safe.

Surveillance "reform" tricks the public into believing that their communications are now private-destroys consumer market for privacy and encryption technology.

Greenwald 14 Glenn, constitutional lawyer. "CONGRESS IS IRRELEVANT ON MASS SURVEILLANCE. HERE'S WHAT MATTERS INSTEAD." First Look. 19 November 2014. https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance. [Premier]

All of that illustrates what is, to me, the most important point from all of this: the last place one should look to impose limits on the powers of the U.S. government is . . . the U.S. government. Governments don't walk around trying to figure out how to limit their own power, and that's particularly true of empires. The entire system in D.C. is designed at its core to prevent real reform. This Congress is not going to enact anything resembling fundamental limits on the NSA's powers of mass surveillance. Even if it somehow did, this White House would never sign it. Even if all that miraculously happened, the fact that the U.S. intelligence community and National Security State operates with no limits and no oversight means they'd easily co-opt the entire reform process. That's what happened after the eavesdropping scandals of the mid-1970s led to the establishment of congressional intelligence committees and a special FISA "oversight" court—the committees were instantly captured by putting in charge supreme servants of the intelligence community like Senators Dianne Feinstein and Chambliss, and Congressmen Mike Rogers and "Dutch" Ruppersberger, while the court quickly became a rubber stamp with subservient judges who operate in total secrecy. Ever since the Snowden reporting began and public opinion (in both the U.S. and globally) began radically changing, the White House's strategy has been obvious. It's vintage Obama: Enact something that is called "reform"—so that he can give a pretty speech telling the world that he heard and responded to their concerns—but that in actuality changes almost nothing, thus strengthening the very system he can pretend he "changed." That's the same tactic as Silicon Valley, which also supported this bill:

Be able to point to something called "reform" so they can trick hundreds of millions of current and future users around the world into believing that their communications are now safe if they use Facebook, Google, Skype and the rest. In pretty much every interview I've done over the last year, I've been asked why there haven't been significant changes from all the disclosures. I vehemently disagree with the premise of the question, which equates "U.S. legislative changes" with "meaningful changes." But it has been clear from the start that U.S. legislation is not going to impose meaningful limitations on the NSA's powers of mass surveillance, at least not fundamentally. Those limitations are going to come from—are now coming from —very different places

Encryption and other defensive strategies are necessary to combat cyberattacks- current infrastructure is all offense no defense.

Doctorow 15 (Cory, citing Bruce Schneider-acclaimed security expert. "Schneier: China and Russia probably did get the Snowden leaks — by hacking the NSA." Boing Boing. 20 June 2015, http://boingboing.net/2015/06/20/schneier-china-and-russia-pro.html. [Premier]

Schneier argues that China and Russia's spy agencies are full of infowar ninjas who've been hacking away at the NSA's repositories for years, and that there is likely a steady flow of secrets that are exfiltrated by the agencies. He says that he thinks successful hack-attacks against the NSA are much more likely than Chinese and Russian spooks coming up with some kind of magic crypto-cracking ability (especially as Snowden didn't even bring the docs with him to Russia). There is a lot of evidence for this belief. We know from other top-secret NSA documents that as far back as 2008, the agency's Tailored Access Operations group has extraordinary capabilities to hack into and "exfiltrate" data from specific computers, even if those computers are highly secured and not connected to the Internet. These NSA capabilities are not unique, and it's reasonable to assume both that other countries had similar capabilities in 2008 and that everyone has improved their attack techniques in the seven years since then. Last week, we learned that Israel had successfully hacked a wide variety of networks, including that of a major computer antivirus company. We also learned that China successfully hacked US government personnel databases. And earlier this year, Russia successfully hacked the White House's network. These sorts of stories are now routine. Which brings me to the second potential source of these documents to foreign intelligence agencies: the US and UK governments themselves. I believe that both China and Russia had access to all the files that Snowden took well before Snowden took them because they've penetrated the NSA networks where those files reside. After all, the NSA has been a prime target for decades. Those government hacking examples above were against unclassified networks, but the nation-state techniques we're seeing work against classified and unconnected networks as well. In general, it's far easier to attack a network than it is to defend the same network. This isn't a statement about willpower or budget; it's how computer and network security work today. A former NSA deputy director recently said that if we were to score cyber the way we score soccer, the tally would be 462–456 twenty minutes into the game. In other words, it's all offense and no defense.

Impact – War

Cyberattacks on nuclear arsenals escalate to war.

Fritz 09 Jason Fritz, Bond University IR Masters. "Hacking Nuclear Command and Control." July 2009. http://www.icnnd.org/latest/research/Jason_Fritz_Hacking_NC2.pdf. [Premier]

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 – Grid

Cyber attack on the grid shuts down the military and forces a nuclear response.

Tilford 12 Robert, Writer for The Examiner. "Cyber attackers could shut down the electric grid for the entire east coast." The Examiner. 27 July 2012. http://zpsenergy.com/home/?q=node/83. [Premier]

"Cyber attackers could all too easily **shut down** the **electric grid** for the entire east coast, the west coast, and the middle part of our country", said Senator Grassley on July 26, 2012. "Any **one attack** could leave dozens of major cities and tens of millions of Americans without power. We know, because we were shown in a room here in the Capitol, how an attack could take place and what damage it would do, so we know this is not just make believe", he said. So what would a cyber attack look like anyway? The Senator explained: "Without ATMs or debit card readers, commerce would immediately **grind to a halt.** My daughter, who lives here in the DC area, lost power when the storm hit. They waited for a number of hours, and then they took all the food out of their freezer, they gave away what they could, and they threw the rest away. And that was the way it was all over. Their power was out for about a week, and it made it very difficult. They are fortunate enough to have a basement, and the heat wasn't oppressive down there. Without refrigeration, food would rot on the shelves, the freezers would have to be emptied, and people could actually go hungry. Without gas pumps, transportation arteries would clog with abandoned vehicles. Without cell phones or computers, whole regions of the country would be cut off from communication and families would be unable to reach each other. Without air conditioning and without lifesaving technology and the service of hospitals and nursing homes, the elderly and sick would become much sicker and die. Most major hospitals have backup power, but it is only for a limited amount of time. It depends on how much fuel they can store, and that is very limited", Senator Grassley said. The devastation that the Senator describes is truly unimaginable. To make matters worse a cyber attack that can take out a civilian power grid, for example could also **cripple 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 (see video: Pentagon declares war on cyber attacks http://www.youtube.com/watch?v=_kVQrp_D0kY&feature=relmfu). 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.

Blocks

AT: Privacy

The squo solves all your advantages- the Freedom Act is a major shift in surveillance and solves symbol advantages.

CDT 15 Columbia Daily Tribune. "With USA Freedom Act, America finally moves beyond 9/11." Columbia Tribune. 7 June 2015. http://www.columbiatribune.com/opinion/oped/with-usa-freedom-act-america-finally-moves-beyond/article_b6113c88-ae7c-53ab-8942-7d6f206c295d.html. [Premier]

In the end, Congress did the right thing. The USA Freedom Act, which ends the National Security Agency's bulk collection of American phone records, passed the Senate convincingly Tuesday, ending a long and labored fight.

This is no small achievement. Practically, it ends an unpopular, legally dubious and empirically ineffective domestic espionage program. Politically, **it signals that Congress can still make progress on serious matters when it tries**. And **symbolically, it suggests that, 14 years after the Sept. 11, 2001, attacks, the United States might finally be getting back to normal**.

Perhaps the most potent expression of that symbolism came from the bill's opponents. In successive attempts to block, delay and dilute this legislation, they employed some familiar oratorical excesses: Sen. Mitch McConnell called the bill "a resounding victory for those currently plotting attacks against the homeland." Yet the opponents failed completely.

This indicates, perhaps, **a deeper cultural shift**. If Americans no longer respond to this kind of alarming rhetoric as they once did — if they're no longer quite so comfortable ceding liberties for the false promise of total security — that is both psychic and civic progress. Democracy requires a sturdy spine no less than a level head.

As it happens, McConnell's fears are baseless. The law still allows the NSA to collect phone records, **as long as it has a court order**. It renews other counterterrorism tools that were jeopardized by this fight. And **it preserves the NSA's most important surveillance programs while ensuring that the government can no longer continuously spy on its own citizens**. It was a compromise, supported by everyone from the intelligence community to Human Rights Watch.

It isn't perfect, of course. Some of its language might be prone to misinterpretation, accidental or otherwise. It doesn't address other aspects of the NSA's global spying operation that require more scrutiny. And some of its transparency requirements might prove ineffective.

Yet the new law is of a piece with the long and cyclical history of American espionage, the limits on which change with the tenor of the times. After World War I, the NSA's predecessor organization was found to be overzealously spying on the communications of U.S. allies. Secretary of State Henry Stimson cut off its funding, memorably saying that "Gentlemen do not read each other's mail." When the NSA and its fellow travelers acquired expansive new powers during the Cold War, overreach followed once again, this time in the form of domestic spying, assassination attempts abroad and much more. The resulting Church Committee investigations led to a systematic overhaul of their oversight.

In rolling back some of the extensive powers granted to intelligence agencies after Sept. 11, the USA Freedom Act suggests that this long civic quest to balance liberty and safety remains vigorous. It shows that fearfulness isn't a permanent condition of American politics. And it affirms the value of transparency and liberty, even in a dangerous age.

No NSA abuses – checks the internal link

Lowry 15 Rich, Editor, the National Review. "Lowry: NSA data program faces death by bumper sticker." 27 May 2015. Salt Lake Tribune. http://www.sltrib.com/csp/mediapool/sites/sltrib/pages/printfriendly.csp?id=2557534. [Premier]

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.

No privacy intrusion – legal restraints prevent data collection of non-targets

De 14 Rajesh, General Counsel, National Security Agency. "The NSA and Accountability in an Era of Big Data." JOURNAL OF NATIONAL SECURITY LAW & POLICY, 2014. [Premier]

False Myth: #2: NSA is spying on Americans at home and abroad with questionable or no legal basis.

This false myth reflects both deep philosophical distrust of the secretive NSA by some, and the reality that signals intelligence activities, unlike some other intelligence activities, inevitably implicate the privacy rights of U.S. persons. It also reflects more recent controversy over so-called "warrantless wiretapping" under the President's Terrorist Surveillance Program (TSP). Without getting into details about the TSP (the authorization for which ended in 2007, but much of which is still classified and the subject of litigation) or FISA (an intricate statutory scheme), I would like to make a few general points about our current operations to help dispel this myth.

First, without an individualized determination of probable cause by a federal judge, NSA does not target the communications of any unconsenting U.S. person anywhere in the world when there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes in the United States (note that pursuant to statute and regulation, under certain emergency scenarios the Attorney General can make an initial finding of probable cause, but if within the purview of FISA, the Foreign

Intelligence Surveillance Court must subsequently make that determination). One point worth highlighting in particular is that, amidst the controversy over the recent amendments made to FISA in 2008 and reauthorized in 2012, an important change was made: targeting a U.S. person abroad now requires a probable cause finding by a federal judge, whereas previously it could be approved by the Attorney General alone under Executive Order 12333.

Second, under even one of the more controversial provisions of the recent FISA amendments, Section 702, where no individualized probable cause finding is required, express limits were enacted:

● Section 702 may only be used to target non-U.S. persons reasonably believed to be located outside the United States.

● Section 702 may not be used to intentionally target any person in the United States or a U.S. person outside the United States.

● Section 702 may not be used to conduct "reverse targeting" – i.e., targeting of a person outside the United States if the purpose is to target a particular, known person inside the United States.

● Section 702 may not be used to intentionally acquire a "wholly-domestic communication" – i.e., a communication where all communicants are inside the United States.

● Section 702 must be implemented in a manner consistent with the Fourth Amendment.

AT: Racist

Existing reforms have removed policies based on racial profiling.

Adams, Nordhaus, and Shellenberger 11 Nick Adams is the director of national security and counterterrorism policy at the Breakthrough Institute, Ted Nordhaus is the co-founder of the Breakthrough Institute, Michael Shellenberger is the co-founder of the Breakthrough Institute. "Who Killed the War on Terror?" The Atlantic. August 2011. http://www.theatlantic.com/national/archive/2011/08/who-killed-the-war-on-terror/244273/. [Premier]

The death of Osama bin Laden at the hands of Navy Seals last May marked a turning point in the fight against al Qaeda. But one thing it did not mark was an end to the War on Terror. That's because the War on Terror was already dead, abandoned by the very agencies responsible for implementing it after 9/11. 9-11 Ten Years Later There are, of course, still terrorists plotting to kill Americans, and the U.S. continues to take aggressive measures to stop them. But it would be a mistake to confuse all counterterrorism strategies with the War on Terror. The War on Terror was based on the notion that Islamic terrorism represented a unified, ideologically coherent, and operationally centralized threat, demanding a singular and predominately military response. This notion was rejected by U.S. security officials long before the killing of Bin Laden. Indeed, it was abandoned well before the election of President Obama. By the latter years of the Bush administration, the exceptional tactics that defined the War on Terror -- preventative detentions, pain-based interrogation, ethnic and religious profiling, and widely expanded domestic surveillance powers -- were either abandoned or dramatically scaled back based on overwhelming evidence that they were ineffective. Meanwhile, the actual wars initiated in the name of the War on Terror, in Afghanistan and Iraq, rapidly evolved into counter-insurgency and then counterterrorism campaigns as military leaders recognized that the U.S. was unable to replace theocrats and autocrats with stable, western-style democracies. The War on Terror lives on today only as political theater. Policymakers, from President Obama to Members of Congress, continue to fear the accusation of being "soft on terror," and hence continue to describe contemporary counterterrorism efforts in martial terms. Congress continues to legislate War on Terror approaches that the security establishment, for the most part, hasn't asked for and, in some cases, has even explicitly rejected. But while the political class remains stuck in the past, the security establishment has moved on. Virtually all of the progress that U.S. authorities have made in dismantling al Qaeda and countering terrorism has been accomplished in spite of, not because of the War on Terror. As we consider the future of U.S. counterterrorism after Bin Laden, we would do well to consider what we have learned from the evolving security response to the 9/11 attacks, and how those lessons might keep us safer in a world where the War on Terror may be over but the threat of terrorism still remains. In many ways, the War on Terror ended because the American security state relearned forgotten lessons. Over the past four centuries, modernizing nation-states have become increasingly effective at securing their citizens' safety and allegiance through ever more refined and subtle means. Where sovereignty was once invested in a single monarch -- think Louis XIV's famous quip, L'État, c'est moi ("The state, it is me") -- gradually the state became all of us. Populations who were "subjects" beholden to state authority became "citizens" willing and empowered to defend it. By granting increasing freedoms and privileges to their citizens, extending the bonds of trust and mutualism, and organizing public education campaigns around the notions of etiquette, civic

duty, and love of country, modernizing states inspired their citizens to identify with the state and internalize its security interests. This shift represented a dramatic evolution in the way states achieved security. Earlier brutal intimidation tactics -- publicly torturing and executing deviants in what social historian Michel Foucault dubbed "festivals of pain" -- gradually gave way to softer means of control like "panoptic" powers, which create the impression that one is always being observed, mostly by fellow citizens. The conventional reading of this shift has imagined that state's relinquished coercive security powers in response to citizens' rising demands for new political and economic freedoms, but this is at best only half the story. The evolution of our expanding freedoms has been inseparable from the development of state security practices that are both more effective and more humane. Today, profiling, suspecting, and punishing wide swaths of society have faded from practice because states found it more effective to maintain the good will and allegiance of increasingly empowered citizens. States developed better tools to discern innocence and guilt on an individual basis rather than punishing whole villages. And as states learned more about individual psychology, they found they could get better information out of detained enemies by "befriending" them than brutalizing them. Since World War II, states have also found that they can more effectively accomplish their international objectives using highly targeted military power, as opposed to large occupying forces. During WWII, all sides, including the U.S., deliberately bombed civilians -- think London, Dresden, Tokyo, Hiroshima. Contrast such blanket, deliberate bombardments to the surgical bombings in Libya and the use of drones in Pakistan. Whatever Orwellian anxieties the new technologies of state security may incite, it is difficult to say - when touring the torture chambers of Venice or considering the pogroms of Eastern Europe, for example -- that the move to the use of softer and more sophisticated security powers does not represent a form of human progress. The turn back towards "the dark side," as former Vice President Dick Cheney described it after 9/11, required a deep forgetting and misunderstanding of the previous centuries' evolutions in state security powers. 2. As American security authorities abandoned the War on Terror, they moved in almost every instance towards more discerning and sophisticated practices. Where the War on Terror made blanket assumptions about the nature of the terrorist threat, objectives, and organization, security authorities today increasingly recognize the threat as disparate, decentralized, and motivated more by local grievances than the apocalyptic desire for a Caliphate. Initially, the wars in Afghanistan and Iraq were very much "wars" as described and theorized by Carl von Clausewitz - featuring attacks on military targets with the goal of forcing capitulation. But the invasions of Iraq and Afghanistan did little to end terrorism and, in Iraq, dramatically increased it. The U.S. military quickly shifted to a more discerning counterinsurgency strategy, and today it is moving to even more focused counterterrorist operations. The shift in the U.S.'s non-military security and counterterrorism tactics has been no less stark. One after another, the sweeping measures put in place after 9/11 have been discarded for more discerning policies. The Defense Department recognized the folly of the preventative detentions that filled the cell blocks of Guantanamo Bay Prison. Within months of sweeping up fighting-aged men in Afghanistan, military officials found that they had not only scooped up hundreds of innocents, but also that they had no means (i.e. evidence) with which to prosecute the guilty. They quickly transitioned back to pre-War on Terror battlefield detention protocols and gave trial authority over to local Afghan courts. The FBI also unilaterally abandoned its War on Terror "Interview Project" within months of 9/11. FBI agents repeatedly complained to their superiors that the intimidating interviews targeting immigrants from Muslim-majority countries were generating few leads and undermining their ability to win the trust of potential collaborators. Finally recognizing that they were losing far more than they were gaining, FBI officials shut down the profiling program and refocused

efforts toward fostering cooperative relationships with informants in Muslim communities. The Transportation Security Agency has walked back from its own profiling policies as two would-be bombers - one Jamaican-British, the other Nigerian - were able to avoid heightened screening targeting Arabs and South Asians. Other programs, too, have been scaled back at the request of security officials. FBI Director Robert Mueller and U.S. Deputy Attorney General James Comey both threatened resignation as they held the line against counterproductive policies pursued by the Bush administration. And multiple NSA data-mining programs have been abandoned as independent reports, most notably from the National Academies of Sciences, concluded that they simply push terrorist activity further underground. Perhaps most famously, the signature tactic of the War on Terror -- pain-based interrogation -- was rejected by the FBI, CIA, and military leaders and interrogators during the Bush years because it plainly did not work. "When they are in pain, people will say anything to get the pain to stop," FBI interrogator Ali Soufan explains. "Most of the time they will lie, make up anything, to make you stop hurting them. That means the information you're getting is useless." Torture defenders have repeatedly claimed that classified intelligence documents would vindicate the use of physically coercive interrogation techniques. But time and again, declassified documents have proven the opposite. Khalid Sheik Mohammed (KSM), the mastermind of the 9/11 attacks, was waterboarded 183 times without providing any useful intelligence to his interrogators. It was only many months later, after a skilled CIA interrogator won his admiration and respect, that KSM offered the CIA a series of blackboard lectures on Al Qaeda's modus operandi. Another detainee subject to enhanced interrogation erroneously fingered thirty separate men as Osama bin Laden's personal bodyguard, then provided the "intelligence" that Saddam Hussein was planning to give weapons of mass destruction to Al Qaeda. That information, of course, turned out to be false. In these and many other cases, authorities quickly abandoned the extreme measures some had imagined were necessary. To date, there is no credible evidence that any of the controversial and unprecedented policies adopted after 9/11 helped to foil a single terrorist plot or capture a single terrorist. 3. Immediately after 9/11, policymakers and security authorities concluded that the U.S. was faced with an unprecedented and exceptionally dangerous new enemy. But with the benefit of hindsight, it turns out that al Qaeda was not so exceptional after all. It adopted timeless strategies that terrorist groups -- from the New Left Baader Meinhoff group in Germany to the Irish Republican Army in Northern Ireland -- have utilized throughout history. And the strategies that have proven effective in destroying al Qaeda are the very same that have proven effective in past counterterrorism efforts. Dick Cheney, former CIA director Michael Hayden, and others have insisted that the killing of Bin Laden vindicates their War on Terror. But the facts of the Bin Laden investigation suggest otherwise. Indeed, tracking down Bin Laden was arguably possible only once the security establishment abandoned War on Terror tactics and focused on long-proven, largely uncontroversial, and more discerning approaches -- relying on, tips, informants, and focused surveillance, not torture, illegal wiretapping, or a military occupation. And when military force played a decisive role in the raid on Bin Laden's compound and the drone-strike on his key operational lieutenant a week later, its use was highly targeted -- clearly different than the blunt War on Terror approaches initially used in Iraq and Afghanistan.

Mass surveillance is less discriminatory because it targets everyone equally.

Hadjimatheou 14 Katerina Hadjimatheou, Security Ethics Group, Politics and International Studies, University of Warwick. "The Relative Moral Risks of Untargeted and Targeted Surveillance." Ethical Theory Moral Practice. 2014. [Premier]

There are good reasons to think that both the extent to which surveillance treats people like suspects and the extent to which it stigmatises those it affects increases the more targeted the measure of surveillance. As has already been established, stigmatisation occurs when individuals are marked out as suspicious. Being marked out implies being identified in some way that distinguishes one from other members of the wider community or the relevant group. Being pulled out of line for further search or questioning at an airport; being stopped and searched on a busy train platform while other passengers are left alone; having one's travel history, credit card, and other records searched before flying because one fits a profile of a potential terrorist-these are all examples of being singled out and thereby marked out for suspicion. They are all stigmatising, because they all imply that there is something suspicious about a person that justifies the intrusion. In contrast, untargeted surveillance such as blanket screening at airports, spot screening of all school lockers for drugs, and the use of speed cameras neither single people out for scrutiny nor enact or convey a suspicion that those surveilled are more likely than others to be breaking the rules. Rather, everybody engaged in the relevant activity is subject to the same measure of surveillance, indiscriminately and irrespective of any evidence suggesting particular suspiciousness. Such evidence may well emerge from the application of untargeted surveillance, and that evidence may then be used to justify singling people out for further, targeted surveillance. But untargeted surveillance itself affects all people within its range equally and thus stigmatises none in particular.

Stopping the NSA doesn't stop the TSA, DOJ or other institutions.

Unegbu 13 Cindy C. Unegbu - J.D. Candidate, Howard University School of Law. "National Security Surveillance on the Basis of Race, Ethnicity, and Religion: A Constitutional Misstep." Howard Law Journal. Fall 2013. https://heinonline.org/HOL/LandingPage?handle=hein.journals/howlj57&div=15&id=&page=. [Premier]

Furthermore, the post-9/11 racial profiling of Arabs, Muslims, and South Asians has become publically and politically acceptable, especially in instances of airport security. 157Link to the text of the note Following 9/11, the Assistant Attorney General for Civil Rights, in conjunction with the Department of Justice's Civil Rights Division, had to create the Initiative to Combat Post-9/11 Discriminatory Backlash. 158Link to the text of the note This project was necessitated by an effort to quell violations of civil rights laws against Arab, Muslim, Sikh, and South-Asian Americans, and those perceived to be members of these groups. 159Link to the text of the note The initiative works to combat crimes and discrimination against these groups by ensuring that there are accessible means for individuals to report crimes, that proactive measures to identify crimes and discrimination are implemented, and that outreach programs to affected communities are conducted. 160Link to the text of the note

The NSA will selectively target minorities – it has too much discretion which makes abuses of power inevitable.

Unegbu 13 Cindy C. Unegbu - J.D. Candidate, Howard University School of Law. "National Security Surveillance on the Basis of Race, Ethnicity, and Religion: A Constitutional Misstep." Howard Law Journal. Fall 2013. https://heinonline.org/HOL/LandingPage?handle=hein.journals/howlj57&div=15&id=&page=. [Premier]

The authority to spy and monitor domestic individuals has been granted to various agencies within the government, such as the FBI and the DHS. 104Link to the text of the note This power, granted through the establishment of the NCTC and the DIOG, has led to various improper surveillance practices, such as using race, ethnicity, or religion as a basis for monitoring an individual when there is no suspicion of criminal or terrorist activity. 105Link to the text of the note The government has used race and ethnicity as a basis for selecting individuals to monitor and for conducting threat analysis in the past. 106Link to the text of the note Furthermore, with the additional surveillance power that has been given to the government, **the use of race and ethnicity as a basis for surveillance is disconcerting**. Past Department of Justice national security guidance has **explicitly disallowed** the consideration of race or ethnicity, except to the extent permitted by the Constitution [450] and laws of the nation. 107Link to the text of the note Although a constitutional analysis of the government's surveillance efforts will be conducted later in this Comment, it is important to note that the Justice Department's past guidance stated that "**in absolutely no event** … may Federal officials assert a national security or border integrity rationale as a mere pretext for invidious discrimination." 108Link to the text of the note This 2003 guidance explains what efforts regarding race or ethnicity are allowed and not allowed as a means to protect national security; however, **the DIOG has permitted measures that are contrary to the standards** outlined in the 2003 Department of Justice Guidance. 109

AT: Tech Industry

Snowden revelations prove – NSA spying has minimal impact on tech industry.

Menn 13 Menn, Joseph. "How The NSA Revelations May Actually Be Helping The US Tech Industry." Business Insider. September 2013. http://www.businessinsider.com/how-the-nsa-revelations-may-actually-be-help-the-us-tech-industry-2013-9. [Premier]

Google employees told Reuters that the company has seen no significant impact on its business, and a person briefed on Microsoft's business in Europe likewise said that company has had no issues. At Amazon, which was not named in Snowden's documents but is seen as a likely victim because it is a top provider of cloud computing services, a spokeswoman said global demand "has never been greater." There are multiple theories for why the business impact of the Snowden leaks has been so minimal. One is that cloud customers have few good alternatives, since U.S. companies have most of the market and switching costs money. Perhaps more convincing, Amazon, Microsoft and some others offer data centers in Europe with encryption that prevents significant hurdles to snooping by anyone including the service providers themselves and the U.S. agencies. Encryption, however, comes with drawbacks, making using the cloud more cumbersome. On Thursday, Brazil's president called for laws that would require local data centers for the likes of Google and Facebook. But former senior Google engineer Bill Coughran, now a partner at Sequoia Capital, said that even in the worst-case scenario, those companies would simply spend extra to manage more Balkanized systems. Another possibility is that tech-buying companies elsewhere believe that their own governments have scanning procedures that are every bit as invasive as the American programs.

NSA spying unifies the tech industry.

Lomas 14 Lomas, Natasha. "Zuckerberg: Snowden NSA Revelations Have Brought The Tech Industry Closer." TechCrunch. 24 February 2014http://techcrunch.com/2014/02/24/zuck-on-snowden. [Premier]

Zuckerberg played down the potential impact that fear of government surveillance might have on Internet.org's mission — and indeed argued the reverse, saying that he thought it might make the goal easier because of a new spirit of collaboration in a post-Snowden tech world. "The NSA issues have industry working together better than ever before," he said, adding: "Historically we've had issues working with some of our competitors aligning on policy issues that even help the whole industry – Internet policy issues – but now it's such an important thing, because of how extreme some of the NSA revelations were, I do feel that a lot of the industry is a lot more aligned." Zuckerberg did not name any names, in terms of who exactly used to be hostile to his overtures and is now less so, but one likely candidate here is (presumably) Google. In further comments on the NSA issue, Zuckerberg added that the agreement, secured from the U.S. government, for Facebook to be able to share "everything the government's asking of us" — in terms of requests for user data — has also been "helpful" to dissipating people's fears about the extent of government data-mining of Facebook.

AT: Tech Industry – Data Localization

Localization is driven by the desire for surveillance and freedom from American dependence.

Hill 14 Jonah, Technology policy consultant at Monitor 360, fellow of the Global Governance Futures 2025 program at the Brookings Institution. "THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS." January 14. https://www.researchgate.net/publication/272306764_The_Growth_of_Data_Localization_Post-Snowden_Analysis_and_Recommendations_for_US_Policymakers_and_Business_Leaders. [Premier]

If a government already has a sophisticated communications surveillance capacity, it would not be surprising that that it would want to enhance that capacity – certainly, that is what the United States has done. It would seem naïve to suppose that other governments would act differently. Data localization in both German and India and elsewhere, would offer just such enhancement, through two important intelligence functions. First, it allows domestic intelligence agencies to better monitor domestic data by either forcing data to be stored in local servers (indeed, India has previously required two international firms, Research in Motion and Nokia, to locate servers and data domestically91 for intelligence collection purposes), or by requiring that data to be held by local firms over which domestic intelligence and law enforcement agencies may have greater coercive power. Second, in light of the often-overlooked fact that many intelligence services, such as the BND, cooperate with the NSA in a variety of information sharing programs,92 governments may view localization as a tactic to gain additional bargaining power with the NSA in negotiations over how much information the American spy agency will share.93 Moreover, domestic law enforcement agencies (to the extent that, in most democratic countries, law enforcement is administratively and actually separate from intelligence services) surely have reason to view data localization as a potentially valuable evidence gathering tool, useful in identifying and then prosecuting conventional criminal activities. In connection with investigations and prosecutions, foreign law enforcement often complain that the process by which they request data from U.S. firms (the rules of which are generally negotiated between the United States and foreign governments and then ratified in a Mutual Legal Assistance Treaty) is slow and cumbersome, and that American firms and the U.S. Justice Department are too often uncooperative. The President's Review Group on Intelligence and Communication Technologies estimated that the average time from request to delivery is 10 months, and sometimes years pass before a response arrives.94 There is uncertainty about when data can be shared, with whom, and on what terms; and it all happens with very little transparency.95 This process presents annoying and seemingly unjustified interference to foreign law enforcement officials who want to apprehend criminals. The Brazilian government, for example, has requested information from Google for several pending cases in the Brazilian Supreme Court, but has yet to receive it.96 Similarly, India has often asked the U.S. to serve summonses upon Google, as well as on Facebook, Twitter, and others, for failing to prevent the dissemination of speech prohibited under Indian Law, but has been rejected due to U.S. civil liberties sensibilities.97 Data localization, for frustrated and impatient law enforcement agencies and their political allies, looks like a straightforward mechanism to free themselves from some of this bothersome dependence on Americans.

AT: Tech Industry – Cloud Computing

Surveillance does not significantly impact cloud computing.

Weise 15 Elizabeth. "PRISM revelations didn't hit U.S. cloud computing as hard as expected" 7 April 2015. http://americasmarkets.usatoday.com/2015/04/07/prism-revelations-didnt-hit-u-s-cloud-computing-as-hard-as-expected/. [Premier]

When Edward Snowden revealed the extent of the U.S. National Security Agency's PRISM spying program, there were concerns that American cloud, hosting and outsourcing businesses would lose customers running to non-U.S.-based companies safe from NSA's prying eyes.

"The assertion was that this would be a death blow to U.S. firms trying to operating in Europe and Asia," said Forrester Research analyst Ed Ferrara.

But two recent reports from Forrester find it was less catastrophic than expected.

That's good news for companies like Box (BOX), DropBox and others that make their money by selling U.S.-based data storage.

Forrester had originally predicted U.S. companies could lose as much as $180 billion in sales.

Instead, just 29% of technology decision-makers in Asia, Canada, Europe and Latin America halted or reduced spending with U.S.-based firms offering Internet-based services due to the PRISM scandal, Forrester's Business Technographics Global Infrastructure Survey for 2014 found

"It's a relatively small amount of data," Ferrara said.

That's because most of the companies didn't need to move all their data, much of which was stored in-house. Instead, only 33% of the data held by that 29% of companies was at a third-party data center or in a cloud system.

Forrester believes the overall loss to U.S. cloud providers for 2015 will be about $15 billion and in 2016, $12 billion, a far cry from projections that were ten times that a year ago.

Forrester also found that companies are looking at other ways to protect the integrity of their data, not just from the NSA but also from surveillance by other nations.

Chief among them was encryption. Eighty-four percent of the companies said they're using various encryption methods to protect sensitive material.

The survey's definition of cloud providers is broad, and includes both platform as a service, infrastructure as a service and software as a service companies, said Ferrara.

New protection standards and tech solve cloud computing.

Rubinstein and Hoboken 14 Ira, Senior Fellow at the Information Law Institute (ILI) and NYU School of Law, and Joris Van, Microsoft Research Fellow in the Information Law Institute at New York University, PhD from the University of Amsterdam. "PRIVACY AND SECURITY IN THE CLOUD: SOME REALISM ABOUT TECHNICAL SOLUTIONS TO TRANSNATIONAL SURVEILLANCE IN THE POST- SNOWDEN ERA." 66 Maine L. Rev. 488, September 2014. http://ssrn.com/abstract=2443604. [Premier]

V. CONCLUSION

This Article describes and places in a legal perspective the cloud industry's technological responses to the revelations about ongoing transnational surveillance. By focusing on industry responses and exploring the ways in which the technological design of cloud services could further address surveillance concerns, we provide insights into the prospects of these services shaping lawful government access to the cloud. This intersection of service design, on the one hand, and government demands for access to data, on the other hand, signals a dynamic new chapter in the ongoing debate between industry and governments about the possibility and conditions of secure and privacy-friendly information and communications technologies (ICTs) for global markets.

In particular, we have shown that it is helpful to distinguish between front-door and backdoor access to data in the cloud. Our analysis of industry responses has shown the cloud industry is **moving quickly** to address interception of their customers' data without their knowledge or involvement by adopting technological solutions that limit lawful access (as far as possible) to legal processes directed at the cloud service itself and/or its customers. Many of these measures could have been implemented much earlier on. They are now becoming **industry norms**. Industry standards like SSL/TLS and HTTPS, together with a new generation of PETs offering "end-to-end" protection, can be **effective tools** in preventing bulk acquisition through the targeting of the worldwide communications infrastructure.

In short, technologies can help the industry shape lawful access **even though** they do not change the legal framework, **nor do they overcome the lack of progress in reforming existing legal authorities** (**such as Section 702 of the FAA**) to confine lawful access to the front-door of service providers. We expect that this lack of progress—with respect to transnational legal guarantees of privacy and information security, not only in the U.S. but also elsewhere—will be a strong driver for the wider adoption of more robust and comprehensive privacy technologies in the cloud service context. And we argue that under current conditions, the U.S. cloud industry will increasingly rely on technologies to 'regulate' government data access in an effort to enhance the privacy and information security protections of their foreign customers.

This raises the pertinent question of how the U.S. government may respond to increased resilience of cloud services against lawful surveillance. While FISA and ECPA allow government agencies to obtain orders that ensure the cooperation of providers notwithstanding strong technological protections, existing law does not allow for unlimited bargaining room. Most of the services in question are not subject to CALEA obligations and an extension of CALEA seems neither warranted nor politically feasible under present conditions. Moreover, most of these services have responded to the Snowden revelations by implementing stronger privacy protections (and even some advanced cryptographic protocols). No doubt they await the outcome of the ongoing litigation in the Lavabit case, which may clarify the government's power to compel a service to break its security model in response to a valid surveillance

order. However, the Lavabit case does not yet present a scenario in which a service's use of advanced cryptography makes it impossible to comply with a surveillance order by furnishing unencrypted data. 2014] PRIVACY AND SECURITY IN THE CLOUD 533 A U.S. government win in the Lavabit case may therefore be little more than a pyrrhic victory, for it could simply further incentivize industry to adopt even stronger technological solutions against surveillance, including both actively implemented and client-side encryption protocols **preserving privacy in the cloud**.

AT: Internet Freedom

Existing oversight checks NSA overreach.

Cordero 14 Carrie F. Cordero is the Director of National Security Studies at Georgetown University Law Center. "Fear vs. Facts: Exploring the Rules the NSA Operates Under." 13 June 2014. http://www.cato-unbound.org/2014/06/13/carrie-f-cordero/fear-vs-facts-exploring-rules-nsa-operates-under. [Premier]

There is no doubt the Snowden disclosures have launched a debate that raises significant issues regarding the extent of U.S. government national security surveillance authorities and activities. And Julian Sanchez's essay Snowden: Year One raises a number of these issues, including whether the surveillance is too broad, with too few limits and too little oversight. But an overarching theme of Sanchez's essay is fear – and fear of what might be overshadows what actually is, or is even likely. Indeed, he suggests that by just "tweaking a few lines of code" the NSA's significant capabilities could be misdirected from targeting valid counterterrorism suspects to Americans involved in the Tea Party or Occupy movements.

So really, what would it take to turn NSA's capabilities inward, to the dark corner of monitoring political activity and dissent? It turns out, quite a lot. So much, in fact, that after a considered review of the checks and balances in place, it may turn out to be not worth fearing much at all.

First, a little history. Prior to 1978, NSA conducted surveillance activities for foreign intelligence purposes under Executive authority alone. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which distinguished between surveillance that occurred here at home and that which occurred overseas. FISA requires that when electronic surveillance is conducted inside the United States, the government seek an order from the Foreign Intelligence Surveillance Court (FISC or the Court) based on probable cause. So, if the government wants to conduct surveillance targeting a foreign agent or foreign power here in the United States, it must obtain FISC approval to do so. By law, the Court may not issue an order targeting an American based solely on activities protected by the First Amendment to the Constitution. The Attorney General is required to report on the full range of activities that take place under FISA to four congressional committees: both the intelligence and judiciary committees in Congress. The law requires that the committees be "fully informed" twice each year.

There have been a number of amendments to FISA over the years. In 1994, the statute was amended to require that physical searches for national security purposes conducted inside the United States also happen by an order from the FISC. The USA-PATRIOT Act of 2001 amended several provisions of FISA, one of which enabled better sharing of information between terrorism and criminal investigators. And in 2008, FISA was amended to provide a statutory framework for certain approvals by the Attorney General, Director of National Intelligence, and FISC regarding the targeting of non-U.S. persons reasonably believed to be outside the United States for foreign intelligence purposes, when the cooperation of a U.S. communications service provider is needed.

So how do we know that this system of approvals is followed? Is the oversight over NSA's activities meaningful, or "decorative," as Sanchez suggests?

It is worth exploring. Here is how oversight of the Section 702 surveillance works, as one example, since it has been the subject of a significant part of the debate of the past year. Section 702 was added to FISA by the FISA Amendments Act of 2008. It authorizes the NSA to acquire the communications, for foreign intelligence purposes, of non-U.S. persons reasonably believed to be outside the United States. These are persons with no Constitutional protections, and yet, because the acquisition requires the assistance of a U.S. electronic communications provider, there is an extensive approval and oversight process. There is a statutory framework. Specifically, the Attorney General and Director of National Intelligence jointly approve certifications. According to declassified documents, the certifications are topical, meaning, the way the statute is being implemented, the certifications are not so specific that they identify individual targets; but they are not so broad that they cover any and everything that might be foreign intelligence information. The certifications are filed with the FISC, along with targeting and minimization procedures. Targeting procedures are the rules by which NSA selects valid foreign intelligence targets for collection. Minimization procedures are rules by which NSA handles information concerning U.S. persons. The FISC has to approve these procedures. If it does not approve them, the government has to fix them. The Court reviews these procedures and processes annually. The Court can request a hearing with government witnesses (like senior intelligence officials, even the NSA Director, if the judge wanted or needed to hear from him personally) or additional information in order to aid in its decisionmaking process. Information about the 702 certifications is reported to the Congressional intelligence committees.

Once the certifications are in effect, attorneys from the Department of Justice's (DOJ) National Security Division and attorneys and civil liberties officials from the Office of the Director of National Intelligence (ODNI) review the NSA's targeting decisions and compliance with the rules. They conduct reviews at least every 90 days. During that 90-day period, oversight personnel are in contact with NSA operational and compliance personnel. Compliance incidents can be discovered in one of at least two ways: the NSA can self-report them, which it does; or the DOJ and ODNI oversight personnel may discover them on their own. Sometimes the NSA does not report a compliance incident in the required timeframe. Then the time lag in reporting may become an additional compliance incident. The DOJ and ODNI compliance teams write up semi-annual reports describing the results of their reviews. The reports are approved by the Attorney General and Director of National Intelligence and provided to the FISC and to Congress. According to the one report that has been declassified so far, in August 2013, for a six-month period in 2012, the rate of error for the NSA's compliance under Section 702 collection was .49% - less than half of one percent. If we subtract the compliance incidents that were actually delays in reporting, then the noncompliance rate falls to between .15-.25% - **less than one quarter of one percent**. Hardly an agency run amok.

Reversing surveillance doesn't solve ifreedom

Fontaine 14 Richard Fontaine is the President of the Center for a New American Security (CNAS). Bringing Liberty Online Reenergizing the Internet Freedom Agenda in a Post-Snowden Era. Center for a New American Security. September 2014. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_BringingLibertyOnline_Fontaine.pdf?mtime=20160906080526&focal=none. [Premier]

Such moves are destined to have only a modest effect on foreign reactions. U**.S. surveillance will inevitably continue** under any reasonably likely scenario (indeed, despite the expressions of outrage, not a single country has said that it would cease its surveillance activities). Many of the demands – such as for greater transparency – will not be met, simply due to the clandestine nature of electronic espionage. Any limits on surveillance that a govern - ment might announce will not be publicly verifiable and thus perhaps not fully credible. Nor will there be an international "no-spying" convention to reassure foreign citizens that their communications are unmonitored. As it has for centuries, state-sponsored espionage activities are likely to remain accepted international practice, unconstrained by international law. The one major possible shift in policy following the Snowden affair – a stop to the bulk collection of telecommunications metadata in the United States – will not constrain the activ - ity most disturbing to foreigners; that is, America's surveillance of them. At the same time, U.S. offi - cials are highly unlikely to articulate a global "right o privacy" (as have the U.N. High Commissioner for Human Rights and some foreign officials), akin to that derived from the U.S. Constitution's fourth amendment, that would permit foreigners to sue in U.S. courts to enforce such a right. 39 The Obama administration's January 2014 presidential directive on signals intelligence refers, notably, to the " legiti - mate privacy interests" of all persons, regardless of nationality, and not to a privacy "right.

US surveillance tech industry destroys i-freedom signal.

MacKinnon 12 Rebecca MacKinnon is a blogger and co-founder of Global Voices Online. "The World's No. 1 Threat to Internet Freedom." Foreign Policy. 3 April 2012. http://www.foreignpolicy.com/articles/2012/04/03/The_Worlds_No_1_Threat_to_Internet_Freedom. [Premier]

Internet Freedom Starts at Home The United States needs to practice what it preaches online. Implied though not explicit in Obama's remarks was the idea that if Iran's Internet were freer and more open, Iran's relationship with the world generally -- and the United States in particular -- would be different. Cases like Iran are the main driver of Washington's bipartisan consensus around the idea that a free and open global Internet is in the United States' strategic interest. Yet more than two years after Secretary of State Hillary Clinton gave her first speech declaring "Internet freedom" to be a major component of U.S. foreign policy, it turns out that many of the most sophisticated tools used to suppress online free speech and dissent around the world are actually Made in the USA. American corporations are major suppliers of software and hardware used by all sorts of governments to carry out censorship and surveillance -- and not just dictatorships. Inconveniently, governments around the democratic world are pushing to expand their own censorship and surveillance powers as they struggle to address genuine problems related to cybercrime, cyberwar, child protection, and intellectual property. Even more inconveniently, the U.S. government is the biggest and most powerful customer of American-made surveillance technology, shaping the development of those technologies as well as the business practices and norms for public-private collaboration around them. As long as the U.S. government continues to support the development of a surveillance-technology industry that clearly lacks concern for the human rights and civil liberties implications of its business -- even rewarding secretive and publicly unaccountable behavior by these companies -- the world's dictators will remain well supplied by a robust global industry. American-made technology has turned up around the Middle East and North Africa over the past year -- from Syria to Bahrain to Saudi Arabia, from pre-revolutionary Tunisia to

Egypt -- in contexts that leave no doubt that the software and hardware in question were being used to censor dissenting speech and track activists. While much of this technology is considered "dual use" because it can be used to defend computer networks against cyberattack as well as to censor and monitor political speech, some members of Congress are seeking to prevent its use for political repression. To that end, the Global Online Freedom Act (GOFA), which passed through the House of Representatives Subcommittee on Africa, Global Health, and Human Rights last week, takes aim not only at U.S.-headquartered companies but also overseas companies funded by U.S. capital markets.

Allies' monitoring destroys i-freedom signal

Hanson 10/25/12 Fergus Hanson was a nonresident fellow in the Foreign Policy program at Brookings. "Internet Freedom: The Role of the U.S. State Department." Brookings. 25 October 2012. http://www.brookings.edu/research/reports/2012/10/25-ediplomacy-hanson-internet-freedom.

Another challenge is dealing with close partners and allies who undermine internet freedom. In August 2011, in the midst of the Arab uprisings, the UK experienced a different connection technology infused movement, the London Riots. On August 11, in the heat of the crisis, Prime Minister Cameron told the House of Commons: Free flow of information can be used for good. But it can also be used for ill. So we are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality. This policy had far-reaching implications. As recently as January 2011, then President of Egypt, Hosni Mubarak, ordered the shut-down of Egypt's largest ISPs and the cell phone network, a move the United States had heavily criticized. Now the UK was contemplating the same move and threatening to create a rationale for authoritarian governments everywhere to shut down communications networks when they threatened "violence, disorder and criminality." Other allies like Australia are also pursuing restrictive internet policies. As OpenNet reported it: "Australia maintains some of the most restrictive Internet policies of any Western country…" When these allies pursue policies so clearly at odds with the U.S. internet freedom agenda, several difficulties arise. It undermines the U.S. position that an open and free internet is something free societies naturally want. It also gives repressive authoritarian governments an excuse for their own monitoring and filtering activities. To an extent, U.S. internet freedom policy responds even-handedly to this challenge because the vast bulk of its grants are for open source circumvention tools that can be just as readily used by someone in London as Beijing, but so far, the United States has been much more discreet about criticising the restrictive policies of allies than authoritarian states.

AT: Internet Freedom – Hurts Democracy

Internet centrism and cyber-utopianism wrecks global democracy

Morozov 12 Evgeny, contributing editor at The New Republic and author of two books ; has written for The New York Times, The Economist, The Wall Street Journal, Financial Times, London Review of Books, Times Literary Supplement. "The Net Delusion: The Dark Side of Internet Freedom." 28 February 2012. https://books.google.com/books/about/The_Net_Delusion.html?id=ctwEIggfIDEC. [Premier]

To be truly effective, the West needs to do more than just cleanse itself of cyber-utopian bias and adopt a more realist posture. When it comes to concrete steps to promote democracy, cyber-utopian convictions often give rise to an equally flawed approach that I dub "Internetcentrism." Unlike cyber-utopianism, Internet-centrism is not a set of beliefs; rather, it's a philosophy of action that informs how decisions, including those that deal with democracy promotion, are made and how long-term strategies are crafted. While cyber-utopianism stipulates what has to be done, Internet-centrism stipulates how it should be done. Internet-centrists like to answer every question about democratic change by first reframing it in terms of the Internet rather than the context in which that change is to occur. They are often completely oblivious to the highly political nature of technology, especially the Internet, and like to come up with strategies that assume that the logic of the Internet, which, in most cases, they are the only ones to perceive, will shape every environment than it penetrates rather than vice versa.

While most utopians are Internet-centrists, the latter are not necessarily utopians. In fact, many of them like to think of themselves as pragmatic individuals who have abandoned grand theorizing about utopia in the name of achieving tangible results. Sometimes, they are even eager to acknowledge that it takes more than bytes to foster, install, and consolidate a healthy democratic regime.

Their realistic convictions, however, rarely make up for their flawed methodology, which prioritizes the tool over the environment, and, as such, is deaf to the social, cultural, and political subtleties and indeterminacies. Internet-centrism is a highly disorienting drug; it ignores context and entraps policymakers into believing that they have a useful and powerful ally on their side. Pushed to its extreme, it leads to hubris, arrogance, and a false sense of confidence, all bolstered by the dangerous illusion of having established effective command of the Internet. All too often, its practitioners fashion themselves as possessing full mastery of their favorite tool, treating it as a stable and finalized technology, oblivious to the numerous forces that are constantly reshaping the Internet— not all of them for the better. Treating the Internet as a constant, they fail to see their own responsibility in preserving its freedom and reining in the ever-powerful intermediaries, companies like Google and Facebook.

As the Internet takes on an even greater role in the politics of both authoritarian and democratic states, the pressure to forget the context and start with what the Internet allows will only grow. All by itself, however, the Internet provides nothing certain. In fact, as has become obvious in too many contexts, it empowers the strong and disempowers the weak. It is impossible to place the Internet at the heart of the enterprise of democracy promotion without risking the success of that very enterprise.

The premise of this book is thus very simple: To salvage the Internet's promise to aid the fight against authoritarianism, those of us in the West who still care about the future of democracy will need to ditch

both cyber-utopianism and Internet-centrism. Currently, we start with a flawed set of assumptions (cyber-utopianism) and act on them using a flawed, even crippled, methodology (Internet-centrism). The result is what I call the **Net Delusion.** Pushed to the extreme, **such logic is poised to have significant global consequences that may risk undermining the very project of promoting democracy**. It's a folly that the West could do without.

Instead, we'll need to opt for policies informed by a realistic assessment of the risks and dangers posed by the Internet, matched by a highly scrupulous and unbiased assessment of its promises, and a theory of action that is highly sensitive to the local context, that is cognizant of the complex connections between the Internet and the rest of foreign policymaking, and that originates not in what technology allows but in what a certain geopolitical environment requires.

In a sense, giving in to cyber-utopianism and Internet-centrism is akin to agreeing to box blindfolded. Sure, every now and then we may still strike some powerful blows against our authoritarian adversaries, but in general this is a poor strategy if we want to win. The struggle against authoritarianism is too important of a battle to fight with a voluntary intellectual handicap, even if that handicap allows us to play with the latest fancy gadgets.

AT: Internet Freedom – No Impact

Reject their ahistorical idealism – the internet accelerates the worst parts of humanity

Morozov 12 Evgeny, contributing editor at The New Republic and author of two books ; has written for The New York Times, The Economist, The Wall Street Journal, Financial Times, London Review of Books, Times Literary Supplement. "The Net Delusion: The Dark Side of Internet Freedom." 28 February 2012. https://books.google.com/books/about/The_Net_Delusion.html?id=ctwEIggfIDEC. [Premier]

Even worse, the supposed lawlessness and networked anarchy enabled by the Internet have resulted in greater social pressure to tame the Web. In a sense, the more important the Internet becomes, the greater the onus to rein in its externalities. Promoting the freedom to connect will be a tricky proposal to sell to voters, many of whom actually want the government to promote the freedom to disconnect—at least for particular political and social groups. If the last decade is anything to judge by, the pressure to regulate the Web is as likely to come from concerned parents, environmental groups, or various ethnic and social minorities as it is from authoritarian governments. The truth is that many of the opportunities created by a free-for-all anonymous Internet culture have been creatively exploited by people and networks that undermine democracy. For instance, it's almost certain that a Russian white supremacist group that calls itself the Northern Brotherhood would have never existed in the pre-Internet era. It has managed to set up an online game in which participants—many of them leading a comfortable middleclass existence—are asked to videotape their violent attacks on migrant guest workers, share them on YouTube, and compete for cash awards.

Crime gangs in Mexico have also become big fans of the Internet. Not only do they use YouTube to disseminate violent videos and promote a climate of fear, but they are also reportedly going through social networking sites hunting for personal details of people to kidnap. It doesn't help that the offspring of Mexico's upper classes are all interconnected on Facebook. Ghaleb Krame, a security expert at Alliant International University in Mexico City, points out that "criminals can find out who are the family members of someone who has a high rank in the police. Perhaps they don't have an account on Twitter or Facebook, but their children and close family probably do." It's hard to imagine Mexican police officers becoming braver as a result. And social networking can also help to spread fear: In April 2010, a series of Facebook messages warning of impending gang wars paralyzed life in Cuernavaca, a popular resort, with only a few brave people daring to step outside (it proved to be a false alarm).

The leaders of al-Shabab ("The Lads"), Somalia's most prominent Islamist insurgency group, use text messaging to communicate with their subordinates, avoiding any face-to-face communication and the risks it entails. It's not a particularly contentious conclusion that they have become more effective—and thus more of a menace—as a result.

Plenty of other less notorious (and less violent) cases of networked harm barely receive any global attention. According to a 2010 report from the Convention on International Trade in Endangered Species, an international intergovernmental organization, the Internet has created a new market for trade in extinct species, allowing buyers and sellers to find each other more easily and trade more effectively. Kaiser's spotted newt, found only in Iran, may be the first real victim of the Twitter Revolution. According to reports in the Independent, more than ten companies are selling wild-caught

specimens over the Internet. Not surprisingly, the newt's population was reduced 80 percent between 2001 and 2005 alone.

Another informal market the Internet has boosted is organ trading. Desperate individuals in the developing world are bypassing any intermediaries and are offering their organs directly to those who are willing to pay up. Indonesians, for example, use a website called iklanoke.com, a local alternative to Craigslist, where their postings usually go unmonitored by police. A typical ad from Iklanoke reads, "16-year-old male selling a kidney for 350 million rupiah or in exchange for a Toyota Camry."

Text messaging has been used to spread hate in Africa, most recently in Muslim-Christian squabbles that erupted in the central Nigerian city of Jos in early 2010 that took the lives of more than three hundred people. Human rights activists working in Jos identified at least 145 such messages. Some instructed the recipients how to kill, dispose of, and burn bodies ("kill before they kill you. Dump them in a pit before they dump you"); others spread rumors that triggered even more violence. According to Agence France-Presse, one such message urged Christians to avoid food sold by Muslim hawkers, as it could have been poisoned; another message claimed political leaders were planning to cut water supplies to dehydrate members of one faith.

Two years earlier Kenya lived through an eerily similar tumultuous period. The political crisis that followed Kenya's disputed election that took place on December 27, 2007, showed that the networks fostered by mobile technology, far from being "net goods," could easily escalate into uncontrollable violence. "If your neighbor is kykuyu, throw him out of his house. No one will hold you responsible," said a typical message sent at the peak of the violence; another one, also targeting Kykuyus, said, "Let's wipe out the Mt. Kenya mafia," adding, "Kill 2, get 1 free." But there was also a more disturbing effort by some Kykuyus to use text messaging to first collect sensitive information about members of particular ethnic groups and then distribute that information to attack and intimidate them. "The blood of innocent Kykuyus will cease to flow! We will massacre them right here in the capital. In the name of justice put down the names of all the Luos and Kaleos you know from work, your property, anywhere in Nairobi, not forgetting where and how their children go to school. We will give you a number on where to text these messages," said one such message. At one point, the Kenyan authorities were considering shutting down mobile networks to avoid any further escalation of violence (between 800 and 1,500 people died, and up to 250,000 were displaced).

Even though text messaging also proved instrumental in setting up a system that helped to track how violence spread around Kenya—a success story that gained far more attention in the media—one can't just disregard the fact that text messaging also helped to mobilize hate. In fact, text messages full of hatred and highly intimidating death threats kept haunting witnesses who agreed to testify to the high-level Waki Commission set up to investigate the violence two years after the clashes. ("You are still a young man and you are not supposed to die, but you betrayed our leader, so what we shall do to you is just to kill you" was the text of a message received by one such witness.)

The bloody Uighur-Han clashes that took place in China's Xinjiang Province in the summer of 2009 and resulted in a ten-month ban on Internet communications appear to have been triggered by a provocative article posted to the Internet forum www.sg169.com. Written by an angry twenty-three-year-old who had been laid off by the Xuri Toy Factory in China's Guangdong Province, 3,000 miles from Xinjiang, the article asserted that "six Xinjiang boys raped two innocent girls at the Xuri Toy Factory." (China's official media stated that the rape accusations were fake, and foreign journalists could not find

any evidence to substantiate such claims either.) Ten days later, the Uighur workers at the toy factory were attacked by a group of angry Han people (two Uighurs were killed, and over a hundred were injured). That confrontation, in turn, triggered even more rumors, many of which overstated the number of people who had been killed, and the situation got further out of control soon thereafter, with text messaging and phone calls helping to mobilize both sides (the authorities eventually turned off all phone communications soon thereafter). A gruesome video that showed several Uighur workers being beaten by a mob armed with metal pipes quickly went viral as well, only adding to the tensions.

Even countries with a long democratic tradition have not been sparred some of the SMS-terror. In 2005, many Australians received text messages urging attacks on their fellow citizens of Lebanese descent ("This Sunday every Fucking Aussie in the shire, get down to North Cronulla to help support Leb and wog bashing day. . . . Bring your mates down and let's show them this is our beach and they're never welcome back"), sparking major ethnic fights in an otherwise peaceful country. Ethnic Lebanese got similar messages, only calling for attacks on non-Lebanese Australians. More recently, right-wing extremists in the Czech Republic have been aggressively using text messaging to threaten local Roma communities. Of course, even if text messaging had never been invented, neo-Nazis would still hate the Roma with as much passion; to blame their racism on mobile phones would be yet another manifestation of focusing on technology at the expense of political and social factors. But the ease, scale, and speed of communications afforded by text messaging makes the brief and previously locally contained outbursts of neo-Nazi anger resonate in ways that they could have never resonated in an era marked by less connectedness.

Perhaps, the freedom to connect, at least in its current somewhat abstract interpretation, would be a great policy priority in a democratic paradise, where citizens have long forgotten about hate, culture wars, and ethnic prejudice. But such an oasis of tolerance simply does not exist. Even in Switzerland, commonly held up as a paragon of decentralized democratic decision making and mutual respect, the freedom to connect means that a rather small and marginalized fraction of the country's population managed to tap the power of the Internet to mobilize their fellow citizens to ban building new minarets in the country. The movement was spearheaded by right-wing blogs and various groups on social networking sites (many of them featuring extremely graphic posters—or "political Molotov cocktails," as Michael Kimmelman of the New York Times described them—suggesting Muslims are threatening Switzerland, including one that showed minarets rising from the Swiss flag like missiles), and even peace-loving Swiss voters could not resist succumbing to the populist networked discourse. Never underestimate the power of Twitter and Photoshop in the hands of people mobilized by prejudice.

AT: Whistleblowing

Agencies are focusing on collecting electronic data.

Davenport 14 Christian, has served as an editor on the Metro desk and as a reporter covering military affairs. "Federal agencies embrace new technology and strategies to find the enemy within." Washington Post. 7 March 2014. http://www.washingtonpost.com/business/economy/federal-agencies-embrace-new-technology-and-strategies-to-find-the-enemy-within/2014/03/07/22ce335e-9d87-11e3-9ba6-800d1192d08b_story.html. [Premier]

After years of focusing on outside threats, the federal government and its contractors are turning inward, aiming a range of new technologies and counterintelligence strategies at their own employees to root out spies, terrorists or leakers. Agencies are now monitoring their computer networks with unprecedented scrutiny, in some cases down to the keystroke, and tracking employee behavior for signs of deviation from routine. At the Pentagon, new rules are being written requiring contractors to institute programs against "insider threats," a remarkable cultural change in which even workers with the highest security clearances face increased surveillance. The "if you see something, say something" mind-set of the post-9/11 world has fully arrived in the workplace, with new urgency following high-profile leaks such as the revelations of former National Security Agency contractor Edward Snowden. "People's sensitivity to this has changed substantially," said Lynn Dugle, president of a Raytheon business unit that markets an insider threat detection system called SureView. "I can tell you five years ago, when we were talking to agencies or companies about insider threat, we would normally be talking to (chief information officers) who were under budget stress. . . . And that was a very tough sell. Now we see boards of directors and CEOs really understanding what the threat can mean to them, and the risk it poses to them." In response to the breach by former Army intelligence analyst Pfc. Bradley Manning, President Obama in 2011 issued an executive order that established a National Insider Threat Task Force and required all federal agencies that handle classified material to institute programs designed to seek out saboteurs and spies. While corporate security has long been part of Beltway culture, the heightened focus and the emergence of new monitoring technology touched off a burgeoning industry. In addition to Raytheon, Lockheed Martin has developed an insider-threat detection service, as have several start-ups in the Washington area. Even Booz Allen Hamilton, which faced national embarrassment when Snowden, one of its employees, walked off with some of the country's most guarded secrets, counsels its clients on how to detect rogue employees. A recent job posting said the company was looking for an "insider threat analyst," which required a security clearance and more than five years of experience in counterintelligence. The posting spread on the Web and sparked ridicule over the notion that the company that employed Snowden was now looking to help turn the historic breach into a profitable lesson learned. Raytheon's SureView program allows agencies to create all sorts of internal alerts indicating when something may be amiss. A company could, for example, program the software to detect whenever a file containing the words "top secret" or "proprietary" is downloaded, e-mailed or moved from one location on the system to another. Once that wire is tripped, an alert almost immediately pops up on a security analyst's monitor, along with a digital recording of the employee's screen. All the employee's actions — the cursor scrolling over to open the secure file, the file being copied and renamed — can be watched and replayed, even in slow motion. It's the cyber equivalent of the security camera that records robbers sticking up a convenience store. Lockheed Martin provides a service called Wisdom, which acts as "your eyes and ears on the Web," according to a company official. At its broadest use, the service can monitor mountains of data on the Web — Facebook, Twitter, news sites or blogs — to help predict everything from a foreign coup or riot to political elections. But it can also be turned inward, at employees' online habits, to predict who within the organization might go rogue. Counterintelligence officials use Wisdom to "evaluate employee behavior patterns, flagging individuals who exhibit high risk characteristics," the company says in a brochure. "I like to think of it as a digital intuition that is being developed," said Jason O'Connor, Lockheed's vice president for analysis and mission solutions. A trade-off for companies The market is much broader than the defense and intelligence industries. It extends to hospitals, which need to protect patients' information; retailers, which hold customers' credit card numbers; and financial institutions. Some worry that the programs are an overreaction to a relatively rare threat that will do more to hinder the free flow of information than to deter crime, while creating repressive working environments. Despite the soon-to-come federal mandate, many defense contractors have "already implemented fairly imposing controls to minimize the unauthorized use of data," said Loren Thompson, a defense industry consultant who has worked with Lockheed Martin and other contractors. But he warned that this "clearly is a trade-off in which values like efficiency and collaboration will be sacrificed in order to reduce the likelihood of internal wrongdoers from succeeding." After Sept. 11, many agencies were criticized for not sharing sensitive information that could have prevented the attacks, so steps were taken to consolidate data within the government. Thompson fears

the current climate of worry about Snowden-like leaks could lead to a return to the old habits, with key information once again compartmentalized. “Insider threats are a real problem, but mandating a particular standard for all contractors will cost huge amounts of money and quite possibly result in the wrong steps being taken,” he said. In addition to the cases that have made headlines worldwide, there are an untold number of incidents in the broader corporate world where insiders wreak havoc — from the systems administrator at what was then UBS Paine Webber who planted a “logic bomb” on the company’s network, to the Chinese national who was convicted of stealing trade secrets from Ford Motor Co.

Leaks are bad – they risk terrorism.

Clapper 15 James R. Clapper, Director of National Intelligence. *Worldwide Threat Assessment of the US Intelligence Community,* Senate Armed Services Committee. 26 February 2015. [Premier]

COUNTERINTELLIGENCE

We assess that the leading state intelligence threats to US interests in 2015 will continue to be **Russia and China**, based on their capabilities, intent, and broad operational scopes. Other states in South Asia, the Near East, and East Asia will pose increasingly sophisticated local and regional intelligence threats to US interests. For example, Iran’s intelligence and security services continue to view the United States as a primary threat and have stated publicly that they monitor and counter US activities in the region.

Penetrating the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions dealing with defense, energy, finance, dual-use technology, and other areas will be a **persistent threat** to US interests.

Non-state entities, including transnational **organized criminals and terrorists**, will continue to employ human, technical, and cyber intelligence capabilities that present a significant counterintelligence challenge. Like state intelligence services, these non-state entities **recruit sources** and perform physical and technical surveillance to facilitate their illegal activities and avoid detection and capture.

The internationalization of critical US supply chains and service infrastructure, including for the ICT, civil infrastructure, and national security sectors, increases the potential for subversion. This threat includes individuals, small groups of “hacktivists,” commercial firms, and state intelligence services.

Trusted insiders who **disclose sensitive** US Government information without authorization will remain a significant threat in 2015. The technical sophistication and availability of information technology that can be used for nefarious purposes exacerbates this threat. Pg. 2

Leaks undermine intel cooperation.

Walsh 15 James Igoe Walsh, Professor of political science @ University of North Carolina. “How the latest leak hurts intelligence cooperation.” *The Washington Post*. 25 February 2015. https://www.washingtonpost.com/news/monkey-cage/wp/2015/02/25/how-the-latest-leak-hurts-intelligence-cooperation/. [Premier]

The leak is likely to have important implications for the willingness of intelligence agencies to share information in the future. At its heart, intelligence sharing involves the exchange of not simply information, but information that must be kept secret from others. States that share secrets worry that

their partners will divulge them, deliberately or inadvertently. The current leak is the latest case, after Wikileaks and the Edward Snowden revelations, where an intelligence "insider" has broken this promise of secrecy.

States' reaction to this leak will have important consequences for their own security. Greater limits on intelligence sharing might restrict states' ability to counter transnational terrorist groups and other threats to peace and stability. Leaks by insiders have fast become the biggest challenge to the current intelligence sharing regime. To some extent, these leaks are a public good. They have provided a lot of information about intrusions on civil liberties and human rights by intelligence agencies around the world.

Intelligence agencies are likely to want to share less after this document leak. It makes sense to share only with those whom you trust to keep information secret. Insider leaks may lead states to update their assessments of the trustworthiness of their partners. But limiting sharing to only the most trustworthy states imposes quite serious costs. Only a handful of countries have foreign intelligence services of any size, and none comes close to matching the United States. For smaller countries, this means there are relatively few partners who can provide intelligence on a wide range of issues. After the Wikileaks and Snowden revelations, many commentators suggested that foreign intelligence services would limit sharing with the United States, but it is not clear that this has actually happened.

But cooperating with only the most trustworthy states is not the only way to share intelligence. As I discuss in my book, "International Politics of Intelligence Sharing," cooperating states can construct institutions and practices that limit their vulnerability to exploitation by their partners. The United States, for example, provides funding and technical support to the intelligence agencies of a number of smaller states. This not only builds partner states' capacity to develop mutually useful intelligence, but also provides the United States with leverage it can use to punish partners who violate sharing agreements.

This and earlier insider threats suggest it is becoming increasingly difficult for intelligence services to keep their secrets secret. Although we do not yet know the motives of the leaker or leakers in the South African case, many of the previous leakers were unhappy about their governments' willingness to aggressively exploit their growing capacity to monitor communications, even when doing so threatens civil liberties.

AT: Cybersecurity

Cybersecurity is bad because of lax governmental policies.

Castro 15 Daniel, Contributing writer at The Hill. "Government apathy is the barrier to better cybersecurity," The Hill. 17 June 2015. http://thehill.com/blogs/pundits-blog/technology/245262-government-apathy-is-the-barrier-to-better-cybersecurity. [Premier]

When the federal government announced earlier this month that Chinese hackers had stolen sensitive personnel records of 4.2 million current and former government employees (myself included), the biggest surprise was that it had taken so long for this kind of breach to occur. The truth is that it was less an indicator of the Chinese government's technical prowess than it was proof of the U.S. federal government's lackadaisical approach to securing its computer systems.

Many of the security vulnerabilities that likely contributed to the data breach had already been uncovered by government auditors. Obviously, this was to no avail. But rather than pointing fingers merely to score political points, policymakers should use this unprecedented breach to catalyze substantive change to the federal government's approach to information security by creating a zero-tolerance policy that drives real change.

The most frustrating part of this whole affair is that it might have been prevented if the target of the breach, the Office of Personnel Management (OPM), had followed the federal rules for information security. The Federal Information Security Management Act outlines steps an agency must take to secure its systems. In 2014, the inspector general for OPM found many areas where it did not follow these baseline security practices. For example, it failed to routinely scan its servers for vulnerabilities, implement multi-factor authentication for remote access or maintain a comprehensive inventory of systems. Findings this substantial should have sent shockwaves through the government, but they instead elicited a collective shrug from officials who have grown accustomed to subpar security practices.

While OPM's problems were more severe than other agencies, it is certainly not alone. For example, not counting the Department of Defense, **only 41 percent of federal agencies have implemented the minimum authentication requirements for accessing federal networks**. Federal agencies are routinely targets for cyberattacks, so ignoring these vulnerabilities comes at great risk. The long-term solution to this problem is to build a culture in federal agencies that does not tolerate such poor performance.

Achieving this will require strong leadership from within agencies and vigorous oversight from Congress. When agencies fall short in meeting baseline standards, agency leaders should be held responsible. Agencies that fail to address these problems should face budget cuts and agency heads should be replaced. The purpose of these accountability measures is not to assign blame, but to drive structural change by creating a sense of urgency for improving federal information security practices.

In the short-term, President Obama should issue an executive order to address one of the primary reasons this most recent attack was possible: improperly secured data. The president should require agencies to submit to Congress within 90 days a confidential, comprehensive and prioritized inventory of every system that stores sensitive information in an unencrypted format. In addition, federal chief information officers (CIOs) should be required to submit plans to secure these systems, including any

additional funding they might need. Congress can then decide if these agencies are deficient due to a lack of resources or their own inadequacies, and if the former, they should provide immediate funding to address the shortcomings. CIOs should provide Congress with an update every six months until the job is accomplished.

Given the scope and sensitivity of the personal information that the U.S. government collects, doing a job that is "good enough for government" is no longer acceptable when it comes to information security. Attacks on the government's information systems are not going to stop. The question is whether or not we will be prepared.

No impact to cyberattacks – empirics – their ev is fear-mongering.

Valeriano and Maness 15 Brandon, Senior Lecturer in Social and Political Sciences at the University of Glasgow, and Ryan C., Visiting Fellow of Security and Resilience Studies at Northeastern University. "The Coming Cyberpeace: The Normative Argument Against Cyberwarfare." Foreign Affairs. 13 May 2015. https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace. [Premier]

The era of cyberconflict is upon us; at least, experts seem to accept that cyberattacks are the new normal. In fact, however, evidence suggests that cyberconflict is not as prevalent as many believe. Likewise, the severity of individual cyber events is not increasing, even if the frequency of overall attacks has risen. And an **emerging norm against the use of severe state-based cybertactics** contradicts fear-mongering news reports about a coming cyberapocalypse. The few isolated incidents of successful state-based cyberattacks do **not a trend** make. Rather, what we are seeing is cyberespionage and probes, not cyberwarfare. Meanwhile, the international consensus has stabilized around a number of limited acceptable uses of cybertechnology—one that prohibits any dangerous use of force.

Despite fears of a boom in cyberwarfare, there have been **no major or dangerous hacks** between countries. The closest any states have come to such events occurred when Russia attacked Georgian news outlets and websites in 2008; when Russian forces shut down banking, government, and news websites in Estonia in 2007; when Iran attacked the Saudi Arabian oil firm Saudi Aramco with the Shamoon virus in 2012; and when the United States attempted to sabotage Iran's nuclear power systems from 2007 to 2011 through the Stuxnet worm. The attack on **Sony from North Korea** is just the latest overhyped cyberattack to date, as the corporate giant has recovered its lost revenues from the attack and its networks are arguably more resilient as a result. Even these are more probes into vulnerabilities than full attacks. Russia's aggressions show that **Moscow** is willing to use cyberwarfare for disruption and propaganda, but not to inflict injuries or lasting infrastructural damage. The Shamoon incident allowed **Iran** to punish Saudi Arabia for its alliance with the United States as Tehran faced increased sanctions; the attack destroyed files on Saudi Aramco's computer network but **failed to do any lasting damage**. The **Stuxnet** incident also failed to create any lasting damage, as Tehran put more centrifuges online to compensate for virus-based losses and strengthened holes in their system. Further, these supposedly successful cases of cyberattacks are balanced by **many more examples of unsuccessful ones**. If the future of cyberconflict looks like today, the international community must **reassess the severity of the threat.**

Cyberattacks have demonstrated themselves to be **more smoke than fire**. This is not to suggest that incidents are on the decline, however. Distributed denial-of-service attacks and infiltrations increase by

the minute—every major organization is probed constantly, but only for weaknesses or new infiltration methods for potential use in the future. Probes and pokes do not destabilize states or change trends within international politics. Even common cyber actions have little effect on levels of cooperation and conflict between states.

Cyberattacks won't result in nuclear war - airgapping solves.

Green 2 Joshua, editor of The Washington Monthly. "The Myth of Cyberterrorism." Washington Monthly. 2002. http://www.washingtonmonthly.com/features/2001/0211.green.html. [Premier]

There's just one problem: There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying. "I don't lie awake at night worrying about cyberattacks ruining my life," says Dorothy Denning, a computer science professor at Georgetown University and one of the country's foremost cybersecurity experts. "Not only does [cyberterrorism] not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential physical threats like car bombs or suicide bombers."

Which is not to say that cybersecurity isn't a serious problem--it's just not one that involves terrorists. Interviews with terrorism and computer security experts, and current and former government and military officials, yielded near unanimous agreement that the real danger is from the criminals and other hackers who did $15 billion in damage to the global economy last year using viruses, worms, and other readily available tools. That figure is sure to balloon if more isn't done to protect vulnerable computer systems, the vast majority of which are in the private sector. Yet when it comes to imposing the tough measures on business necessary to protect against the real cyberthreats, the Bush administration has balked.

Crushing BlackBerrys

When ordinary people imagine cyberterrorism, they tend to think along Hollywood plot lines, doomsday scenarios in which terrorists hijack nuclear weapons, airliners, or military computers from halfway around the world. Given the colorful history of federal boondoggles--billion-dollar weapons systems that misfire, $600 toilet seats--that's an understandable concern. But, with few exceptions, it's not one that applies to preparedness for a cyberattack. "The government is miles ahead of the private sector when it comes to cybersecurity," says Michael Cheek, director of intelligence for iDefense, a Virginia-based computer security company with government and private-sector clients. "Particularly the most sensitive military systems."

Serious effort and plain good fortune have combined to bring this about. Take nuclear weapons. The biggest fallacy about their vulnerability, promoted in action thrillers like WarGames, is that they're designed for remote operation. "[The movie] is premised on the assumption that there's a modem bank hanging on the side of the computer that controls the missiles," says Martin Libicki, a defense analyst at the RAND Corporation. "I assure you, there isn't." Rather, nuclear weapons and other sensitive military

systems enjoy the most basic form of Internet security: they're "air-gapped," meaning that they're not physically connected to the Internet and are therefore inaccessible to outside hackers. (Nuclear weapons also contain "permissive action links," mechanisms to prevent weapons from being armed without inputting codes carried by the president.) A retired military official was somewhat indignant at the mere suggestion: "As a general principle, we've been looking at this thing for 20 years. What cave have you been living in if you haven't considered this [threat]?"

When it comes to cyberthreats, the Defense Department has been particularly vigilant to protect key systems by isolating them from the Net and even from the Pentagon's internal network. All new software must be submitted to the National Security Agency for security testing. "Terrorists could not gain control of our spacecraft, nuclear weapons, or any other type of high-consequence asset," says Air Force Chief Information Officer John Gilligan. For more than a year, Pentagon CIO John Stenbit has enforced a moratorium on new wireless networks, which are often easy to hack into, as well as common wireless devices such as PDAs, BlackBerrys, and even wireless or infrared copiers and faxes.

The September 11 hijackings led to an outcry that airliners are particularly susceptible to cyberterrorism. Earlier this year, for instance, Sen. Charles Schumer (D-N.Y.) described "the absolute havoc and devastation that would result if cyberterrorists suddenly shut down our air traffic control system, with thousands of planes in mid-flight." In fact, cybersecurity experts give some of their highest marks to the FAA, which reasonably separates its administrative and air traffic control systems and strictly air-gaps the latter. And there's a reason the 9/11 hijackers used box-cutters instead of keyboards: It's impossible to hijack a plane remotely, which eliminates the possibility of a high-tech 9/11 scenario in which planes are used as weapons.

Another source of concern is terrorist infiltration of our intelligence agencies. But here, too, the risk is slim. The CIA's classified computers are also air-gapped, as is the FBI's entire computer system. "They've been paranoid about this forever," says Libicki, adding that paranoia is a sound governing principle when it comes to cybersecurity. Such concerns are manifesting themselves in broader policy terms as well. One notable characteristic of last year's Quadrennial Defense Review was how strongly it focused on protecting information systems.

AT: Soft Power

Trump makes soft power impossible.

Collinson 17 Stephen, White House Reporter for CNN. “Donald Trump's undiplomatic diplomacy.” CNN. 3 February 2017. www.cnn.com/2017/02/03/politics/donald-trump-diplomacy/index.html. [Premier]

President Donald Trump is quickly becoming the world's most undiplomatic -- and unpredictable -- diplomat. Over the course of a week, he had a bruising telephone call with the leader of Australia, one of America's closet allies. He complained to the Mexican President about that country's "handling" of "tough hombres." Trump on Friday warned in a tweet that Iran was "playing with fire" with its ballistic missile tests, part of an emerging strategy designed to show his administration will take a much harder line with the Islamic Republic. But his administration stuck to the tools of traditional diplomacy by using a statement from Trump's press secretary Sean Spicer to warn Israel that new Israeli settlement activity could potentially hamper the peace process, a new stance for a White House that's remained adamant in its support for Prime Minister Benjamin Netanyahu. Throughout his campaign, Trump hailed the virtues of being unpredictable on the world stage. Much to the happiness of some of his supporters, he's following through. But in the process, Trump is confusing much of the world. He's also handing some leaders, such as those in the United Kingdom and Mexico, political headaches of their own after encountering Trump. And some of America's **allies are beginning to warn that Trump is putting over 70 years of transatlantic cooperation at risk**. His style of diplomacy is very different from his recent predecessors," former Australian Prime Minister Kevin Rudd told CNN International's Hala Gorani Thursday. "He is much more in your face. I suppose the diplomacy of the rest of us is kind of going to have to get used to that." Michael Fullilove, the executive director of the Lowy Institute, a top Australian think-tank, said that while the US-Australia alliance would remain strong in the aftermath of the tense phone call, **Trump's approach would inevitably have an impact**. "It's a level of discourtesy that we don't expect," he said. "It will continue to inform the Australian public's view of Mr. Trump. I think inevitably it would inform public opinion about the alliance." Transactional diplomacy Trump seems to view diplomacy through the prism of a business transaction, where there are winners and losers and a belief that even allies can take advantage of the US. The great big Rex Tillerson to-do list His foreign policy thinking -- at least so far -- appears to be focusing more on the mechanics of individual national relationships and less on a strategic vision in which allies are a vehicle for expressing US power and influence around the globe. The President's phone call with Australian Prime Minister Malcom Turnbull went off the rails when discussion turned to a deal concluded by former President Barack Obama to allow 1,250 refugees from an offshore detention center to come to the United States. Trump tweeted Thursday that the deal was "dumb," even though Spicer has said the US would honor the agreement and despite the President's order to temporarily halt all refugees from entering the country. The President was still fulminating about the deal by Thursday afternoon. "I just said why?... Why are we doing this? What's the purpose?" Trump told reporters. "We have wonderful allies and we're going to keep it that way but we need to be treated fairly also." Trump's decision to question the deal has rattled relations with Australia, a crucial pillar of US Asia-Pacific strategy, a member of the Five Eyes intelligence sharing agreement and an ally that has battled alongside the United States dating back to World War I. Trump continues to question refugee deal after heated call with Australian PM Sen. John McCain, who fought with Australians in Vietnam, took it upon himself to smooth over relations on Thursday following Trump's showdown with Turnbull, telephoning Australia's ambassador to Washington. "This in my view was unnecessary and frankly, harmful," the Arizona Republican said, adding that the dispute was far less important than cooperation, including joint training missions involving US Marines in the northern Australian city of Darwin. Senior Democrats were also disturbed by the argument. Virginia Sen. Tim Kaine said to have a "contentious conversation and name call (a) country or the Prime Minister of a country that is one of our greatest allies in Asia is foolish." "**He is doing kind of amateur hour stuff on matters of significant national importance**," said Kaine, who was the 2016 Democratic vice presidential nominee. Lesson for foreign leaders Foreign policy experts said the US-Australia relationship remains too strong to be damaged. But the spat will be seen by other foreign leaders as a lesson in the difficulty of dealing with Trump. British Prime Minister Theresa May found out that leaders who align themselves with Trump can get burned. The President didn't tell her he was signing an executive order restricting travel from seven predominantly Muslim countries soon after she left the White House last Friday, exposing her to a torrent of political criticism back home. US planning additional sanctions on Iran following missile test Trump's frequent criticisms of the European Union, which he has branded corrupt while apparently rooting for more nations to join Britain by voting to leave, is irking US allies, who see the block, for all its faults, as the root of decades of peace in Europe, a continent previously wracked by centuries of war. "It is unacceptable that there should be, through a number of statements by the US President, pressure on what Europe should be or what it should no longer be," French President Francois Hollande said at the EU summit in Malta on Friday, "There is no future with Trump if it's not worked together," Hollande said, according to an official Twitter account for France's representative to the EU. Trump has also criticized the other bulwark of European security, NATO, as obsolete and has far more in common with populist leaders seeking to make an

impact in elections this year in the Netherlands, France and Germany than the ruling elites in those nations. Despite anodyne government readouts, there were also hints of tension in Trump's weekend call with German Chancellor Angela Merkel, whom the President has criticized for welcoming Syrian refugees. Her office said Merkel "explained" to Trump that the Geneva Conventions require nations to offer a haven from refugees fleeing war. But Trump is unapologetic about the bracing conversations he is having with world leaders -- a sign the White House is more concerned about Trump projecting a strong image on the world stage than stepping on diplomatic toes. "The world is in trouble, but we're going to straighten it out. OK? That's what I do. I fix things. We're going to straighten it out," Trump said at the National Prayer Breakfast on Thursday. "Believe me. When you hear about the tough phone calls I'm having, don't worry about it. Just don't worry about it. They're tough. We have to tough ... We're taken advantage of by every nation in the world virtually. It's not going to happen anymore." Trump's pugnacious approach to diplomacy is not surprising given his personality, which he used to great effect in his business career. While his attitude dismays foreign policy elites, it's likely to be welcomed by voters who turned to him in search of strong leadership and see his encounters as a manifestation of his "America First" philosophy. But several diplomats have said Trump's acute course corrections in foreign policy and blunt manner make it difficult to decipher exactly where the United States now stands on key global issues. Private vs. public arguments Getting tough with America's friends also represents a break from previous administrations where disagreements often erupted but were not litigated in public. **The White House may find in future that creating political problems for friendly leaders will make it more difficult for them to compromise with Washington or even to send troops to help fight America's wars.**

Soft power trades off with hard power — the impact is World War.

Ungar 11 Ariel Ungar is a Professor at the Department of Political Studies, Judea and Samaria College, PhD from Columbia University. “The limits of soft power.” Haaretz. http://www.haaretz.com/opinion/the-limits-of-soft-power-1.361425. [Premier]

The decline of soft power’s efficacy as a force for good should make Western Europe and those favoring a Europeanized American foreign policy take notice. A Western world denuded of its military capabilities can no longer rely on soft power any more than the **League of Nations** in the 1930s **could provide an effective bulwark against aggressors** by simply invoking its name. Unless Europe ceases its headlong rush into disarmament, the halfhearted intervention in Libya may prove to be the **swan song** of humanitarian intervention, as soft power has been exposed as a poor excuse for its military abdication.

Soft power is resilient—other elements, democracy, and empirics

Nye 18 Joseph S. Nye, Jr, is a professor at Harvard University and the author of The Future of Power. "America's soft power is robust and resilient." Gulf News. 9 February 2018. https://gulfnews.com/opinion/thinkers/america-s-soft-power-is-robust-and-resilient-1.2170982. [Premier]

Fortunately, America is more than the government. Unlike hard-power assets (such as armed forces), many soft-power resources are separate from the government and are only partly responsive to its purposes. In a liberal society, the absence of official cultural policies can itself be a source of attraction. Hollywood movies like The Post, which showcase independent women and press freedom, can attract others. So, too, can the charitable work of US foundations or the benefits of freedom of inquiry at American universities.

It is true that firms, u**niversities, foundations and other non-governmental groups** develop soft power of their own which may reinforce or be at odds with the US foreign policy goals. And all of these private sources of soft power are likely to become increasingly important in the global information age. That is

all the more reason for governments to make sure that their own actions and policies create and reinforce rather than undercut and squander their soft power.

Domestic or foreign policies that appear hypocritical, arrogant, indifferent to others' views, or based on a narrow conception of national interests can undermine soft power. For example, the steep decline in the attractiveness of the US in opinion polls conducted after the invasion of Iraq in 2003 were a reaction to the George W. Bush administration and its policies, rather than to the US generally.

The Iraq War was not the first government policy that made the US unpopular. In the 1970s, many people around the world objected to the US war in Vietnam, and America's global standing reflected the unpopularity of that policy. When the policy changed and the memories of the war receded, the US recovered much of its lost soft power. Similarly, in the aftermath of the Iraq war, the US managed to recover much of its soft power in most regions of the world.

Sceptics might still argue that the rise and fall of American soft power does not matter much, because countries cooperate out of self-interest. But this argument misses a crucial point: Cooperation is a matter of degree, and the degree is affected by attraction or repulsion. Moreover, the effects of a country's soft power extend to non-state actors — for example, by aiding or impeding recruitment by terrorist organisations. In an information age, success depends not only on whose army wins, but also on whose story wins.

One of the greatest sources of America's soft power is the openness of its democratic processes. Even when mistaken policies reduce its attractiveness, America's ability to criticise and correct its mistakes makes it attractive to others at a deeper level. When protesters overseas were marching against the Vietnam War, they often sang 'We Shall Overcome', the anthem of the US civil rights movement.

America, too, will almost certainly overcome. Given past experience, there is every to hope that the US will **recover its soft power.**

AT: Efficiency

New data programs solve info overload.

Lavenda 15 David, Technology strategist . "How Smartphone Metadata Can Help Prevent Information Overload." CMs Wire. 21 March 2015. http://www.cmswire.com/cms/mobile-enterprise/how-smartphone-metadata-can-help-prevent-information-overload-024591.php?pageNum=2. [Premier]

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.

AT: Democracy

Data while inevitably exist and no threat of tyranny exists.

Etzioni 17 Amatai, Professor of International Relations at the George Washington University. Intelligence and National Security. The New Normal: Finding a Balance Between Individual Rights and the Common Good. 8 September 2017. https://books.google.com/books?id=dqw0DwAAQBAJ. [Premier]

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.

The NSA is well-regulated and constrained by judicial oversight.

Cohen 15 Michael A. Cohen, fellow at The Century Foundation. "NSA Surveillance Debate Drowned Out on Both Sides by Fear Tactics." 3 June 2015. World Politics Review. http://www.worldpoliticsreview.com/articles/15905/nsa-surveillance-debate-drowned-out-on-both-sides-by-fear-tacticsa. [Premier]

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.

It also doesn't spill over to other countries.

Edgar 15 Timothy, visiting fellow at the Institute and adjunct professor of law at the Georgetown University Law Center. "The Good News About Spying" 13 April 2015. Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying. [Premier]

Despite high hopes for a fresh start on civil liberties, during his first term in office, Obama ratified and even expanded the surveillance programs that began under former President George W. Bush. After NSA contractor Edward Snowden began revealing the agency's spying programs to The Guardian in 2013, however, Obama responded with a clear change of direction. Without great fanfare, his administration has made changes that open up the practices of the United States intelligence community and protect privacy in the United States and beyond. The last year and a half has been the **most significant period of reform** for national security surveillance since Senator Frank Church led the charge against domestic spying in the late 1970s.

In 2013, at Obama's direction, the Office of the Director of National Intelligence (ODNI) established a website for the intelligence community, IC on the Record, where previously secret documents are posted for all to see. These are not decades-old files about Cold War spying, but recent slides used at recent NSA training sessions, accounts of illegal wiretapping after the 9/11 attacks, and what had been highly classified opinions issued by the Foreign Intelligence Surveillance Court about ongoing surveillance programs.

Although many assume that all public knowledge of NSA spying programs came from Snowden's leaks, many of the revelations in fact came from IC on the Record, including mistakes that led to the unconstitutional collection of U.S. citizens' emails. Documents released though this portal total more than 4,500 pages—surpassing even the 3,710 pages collected and leaked by Snowden. The Obama administration has instituted other mechanisms, such as an annual surveillance transparency report, that will continue to provide fodder for journalists, privacy activists, and researchers.

The transparency reforms may seem trivial to some. From the perspective of an intelligence community steeped in the need to protect sources and methods, however, they are deeply unsettling. At a Brown University forum, ODNI Civil Liberties Protection Officer Alexander Joel said, "The intelligence community is not designed and built for transparency. Our culture is around finding our adversaries' secrets and keeping our own secrets secret." Accordingly, until only a few years ago, the intelligence community resisted making even the most basic information public. The number of FISA court opinions released to the public between 1978 and 2013 can be counted on one hand.

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.

THOSE IN GLASS HOUSES

Obama's reforms make great strides toward transparency and protecting civil liberties, but they have been **neither celebrated nor matched abroad**. When Chancellor Angela Merkel of Germany found out she had been the target of American eavesdropping, her reaction was swift. "This is not done," she said, as if scolding a naughty child. Many Germans cheered. They and other Europeans believe that their laws protect privacy better than U.S. laws. But that is only partly true: Although Europe has stronger regulations limiting what private companies (such as Google and Facebook) can do with personal data, citizens are granted comparatively little protection against surveillance by government agencies. European human rights law requires no court approval for intelligence surveillance of domestic targets, as U.S. law has since 1978. Similarly, European governments do not observe limits on electronic surveillance of non-citizens outside of their own territories, as the United States now does under Obama's presidential policy directive.

By blaming only the NSA for mass surveillance, the public and foreign leaders let other intelligence services off the hook. No wonder that some human rights organizations, including Privacy International and Big Brother Watch UK, have filed legal challenges against mass surveillance by the NSA's British counterpart, the Government Communications Headquarters (GCHQ). But foreign leaders have taken few steps to limit government surveillance, and none have done **anything remotely comparable** to what Obama did in last year's directive.