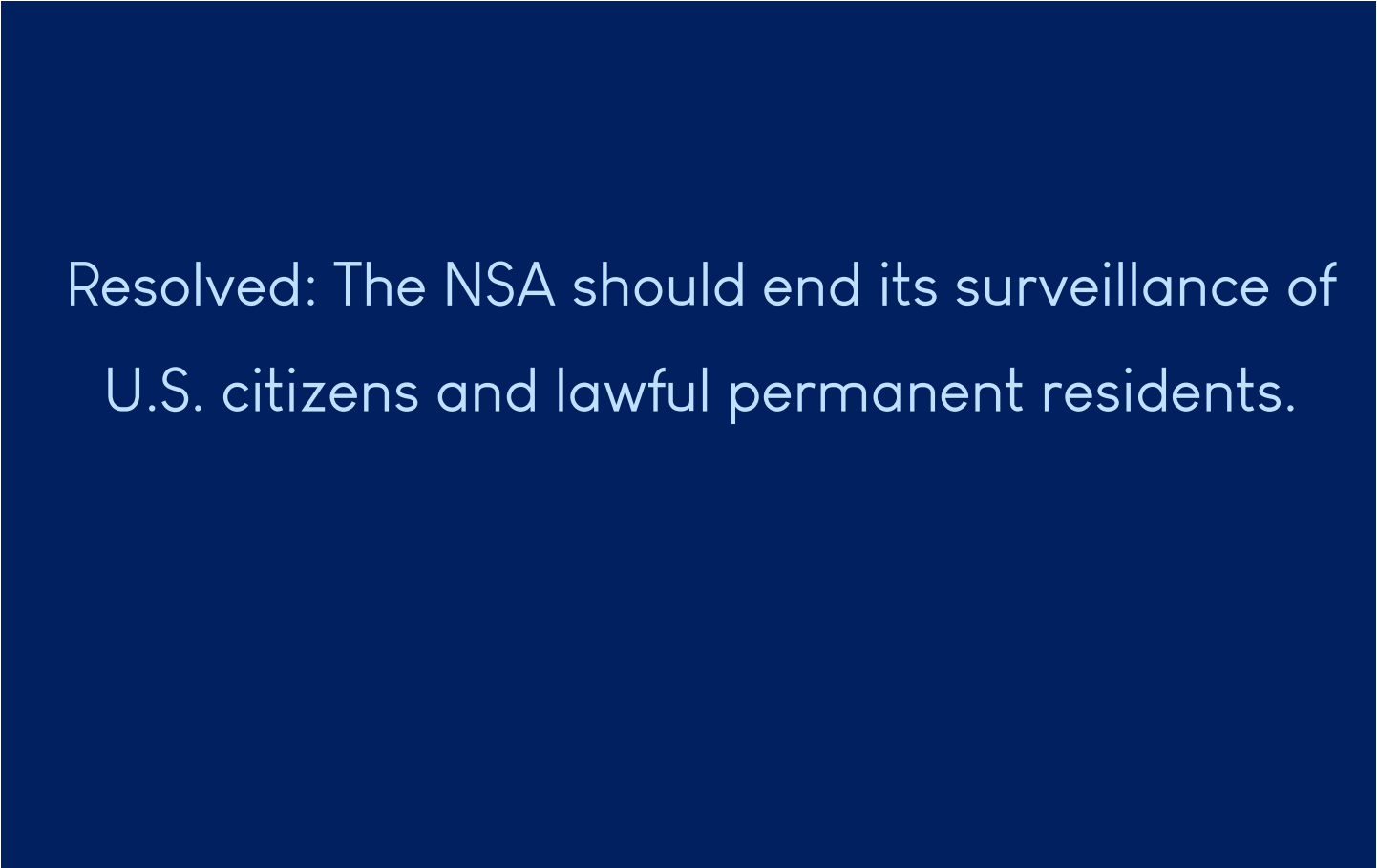




SILVER BULLET BRIEFS

JANUARY 2021

Resolved: The NSA should end its surveillance of
U.S. citizens and lawful permanent residents.





Copyright 2020 by Silver Bullet Briefs, LLC

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by an information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

TABLE OF CONTENTS

WHY SBB?	6
ABOUT US	7
TOPIC ANALYSIS	8
History and Context.....	8
Analysis of the Resolution	9
Why are we debating this resolution now?	10
Argument Rundown.....	11
PRO ARGUMENTS	13
BIG DATA COLLECTION	14
What's the argument?	14
Why does the argument matter?	14
Main Players	14
Strategy Considerations.....	15
Evidence for Big Data Collection.....	16
INTELLECTUAL PROPERTY AND INNOVATION	Error! Bookmark not defined.
What's the argument?	21
Why does the argument matter?	21
Main Players	21
Strategy Considerations.....	22
Evidence for Intellectual Property and Innovation	23
SOFT POWER / INTERNATIONAL RELATIONS	30
What's the argument?	30
Why does the argument matter?	30
Main Players	31
Strategy Considerations.....	31
Evidence for Soft Power / International Relations	32
HUMAN RIGHTS / PRIVACY	37
What's the argument?	37
Why does the argument matter?	37
Main Players	38
Strategy Considerations.....	38
Evidence for Human Rights / Privacy	39
DEMOCRACY	45
What's the argument?	45
Why does the argument matter?	45
Main players	46
Strategy Considerations.....	46
Evidence for Democracy	47
CON ARGUMENTS	51
STOPPING TERRORISM	52
What's the argument?	52
Why does the argument matter?	52

Main Players	52
Strategy Considerations.....	52
Evidence for Stopping Terrorism	54
DISCOVERING ESPIONAGE	57
What's the argument?	57
Why does the argument matter?	57
Main Players	57
Strategy Considerations.....	58
Evidence for Discovering Espionage	59
CYBER ATTACKS.....	65
What's the argument?	65
Why does the argument matter?	65
Main Players	65
Strategy Considerations.....	66
Evidence for Cyber Attacks	67
ELECTION SECURITY	69
What's the argument?	69
Why does the argument matter?	69
Main players	69
Strategy Considerations.....	70
Evidence for Election Security.....	71
STOPPING IP THEFT	75
What's the argument?	75
Why does the argument matter?	75
Main Players	75
Strategy Considerations.....	75
Evidence for Stopping IP Theft.....	77
A2 PRO	80
A2 BIG DATA COLLECTION	81
A2 INTELLECTUAL PROPERTY AND INNOVATION.....	83
A2 SOFT POWER / INTERNATIONAL RELATIONS	85
A2 HUMAN RIGHTS / PRIVACY.....	88
A2 DEMOCRACY	90
A2 CON	93
A2 STOPPING TERRORISM	94
A2 DISCOVERING ESPIONAGE	97
A2 CYBER ATTACKS	99
A2 ELECTION SECURITY	102
A2 STOPPING IP THEFT	104
INDICTS TO PRO EVIDENCE.....	107
A2 HOLMES AND KIRKPATRICK.....	108

A2 GOODWIN	109
A2 PENNY	110
<i>INDICTS TO CON EVIDENCE</i>	<i>111</i>
A2 NSA	112
A2 NSA	113
A2 WHITESIDES	114

WHY SBB?

As debaters and coaches, we have always hunted for the “silver bullet” that will slay our debate monsters: the perfect meta-analysis, the unbeatable narrative, or the argument that is so inherently true that there is no response. We learned that the elusive silver bullet was as much a myth as the monsters that it was designed to slay, but the aspiration of finding it pushed us to gain a deeper understanding of every topic. Thus, we created Silver Bullet Briefs with two goals in mind:

First, debate provides an invaluable opportunity to learn, and we hope to advance that opportunity. Debate teaches competitors not only to research and prepare, but to think on their feet and consider solutions to real-world problems. It teaches young people the significance of viewpoint diversity and gives them an awareness of real-world issues. Most importantly, it leaves competitors with the power and confidence to advocate for themselves – to argue for the things in which they believe. Silver Bullet is an extension of debate. We believe that true success does not come from the evidence that a debater reads. Instead, it stems from the knowledge that a debater can reap from that evidence, and the story that they can tell using it. SBB is not meant to provide an endless stream of redundant evidence, but to give debaters a deeper understanding of each topic and the real-world issue behind it.

Second, we hope to level the playing field. Debate is an unequal activity. Gender minorities are less likely to win rounds and participate in the activity in the first place. The same is true for black and Hispanic debaters, as racial stereotypes and implicit biases limit their success. The structure of the activity has also made debate increasingly inaccessible. Tournament entry fees, travel and hotel expenses, private coaches, summer camps, and even tournament attire are only available to those with the means to afford them. While the advent of online competition has alleviated some of these problems, it has created others. Competition now requires stable internet connection and access to a personal computer. All of these factors have made debate inaccessible for many.

Doing our part: We created Silver Bullet Briefs as a way to increase accessibility to debate. Therefore, while SBB intends to sell debate briefs to those who can afford them, we will provide our briefs at a reduced cost to those who cannot, **AND** we will donate **100%** of the profits from the sale of these briefs to organizations that increase equity and access within the debate community, such as the National Association of Urban Debate Leagues.

Let's make a difference together.

ABOUT US

Maggie Mills competed in Public Forum debate for Chagrin Falls High School for all four years of high school. Maggie served as President and Vice President of Chagrin Falls High School's Speech and Debate team. Throughout her four-year career, she and her partner, Sasha, qualified for the Ohio state speech and debate tournament four times and for the Tournament of Champions three times. During her senior year, Maggie and Sasha won the Ohio state tournament without dropping a ballot. In June, the team won the 2020 NSDA national championship. Maggie plans to study Economics and Political Science as a member of the University of Chicago's class of 2024.

Sasha Haines competed in Public Forum Debate for Chagrin Falls High School for four years and was a co-captain of the team during her junior and senior year. Sasha often competed nationally, reaching elimination rounds at numerous national tournaments including the Sunvitational, the Season Opener at UK, UPenn, and Stanford. Throughout her career, Sasha qualified three times to the Gold division of the Tournament of Champions, was the Ohio State Champion and won the 2020 NSDA Nationals. Sasha plans to study Public Affairs and Philosophy, Politics, and Economics at The Ohio State University.

Albi Manfredi did Public Forum Debate for five years at Lake Mary Prep in Orlando, Florida. Throughout his time as a competitor, he amassed a total of 17 bids to the Tournament of Champions, semi-finaled at the Yale Invitational and the Tournament of Champions, was the Florida State Runner-Up, and championed the Blue Key Round Robin, the Crestian Tradition, and the Sunvitational. Individually, he achieved top speaker at the Blake Tournament, Emory's Barkley Forum, and Florida States. He finished his career placing 5th at NSDA Nationals. As a first year out, Albi has been a successful coach, most recently helping Sasha and Maggie win the prestigious NSDA national tournament. Albi is a sophomore at the University of Pennsylvania studying Chemical and Biomolecular Engineering and Legal Studies.

Ana Kevorkian competed in Public Forum debate for Chagrin Falls High School for 3 years. During her senior year, she served as Secretary of the school's Speech and Debate team, handling tournament registration and results reporting. She also founded the Ohio chapter of Beyond Resolved and served as the organization's first Director of Research and the Director of the Clothing Drive Initiative. In high school, she was a National Merit Scholar, National AP Scholar, AP Capstone Diploma recipient, and graduated Cum Laude. Ana spent the fall organizing on a Senate campaign and is currently on a gap year.

Richard Haber has been the Coach of Public Forum Debate at Chagrin Falls High School for 8 seasons. He first became involved as a debate coach when his daughter Victoria began competing as a freshman in High School. Leveraging his 30 years as a trial lawyer, he continued to coach even after Victoria graduated because he believed in the value of the activity. As an accomplished trial lawyer, Richard has been honored as an Ohio Super Lawyer® from 2004 to the present; as one of the top 100 lawyers in the state of Ohio from 2010 to 2017; and has been named from 2010 to the present in The Best Lawyers in America® published by Best Lawyers in conjunction with U.S. News Media Group. As a debate coach, Richard has coached two teams to state championships in the last 3 years; qualified three teams to NSDA Nationals, coached teams to four Tournament of Championship qualifications in the last three years and along with Albi Manfredi coached Maggie and Sasha to the 2020 National Speech and Debate Association Public Forum Championship. Richard is a devout advocate of traditional public forum debate and helped found Silver Bullet Briefs to promote this style of debate.

TOPIC ANALYSIS

History and Context

The history of the National Security Agency (NSA) and government surveillance is one that goes hand-in-hand with the history of the infamous “War on Terror”. Just weeks after the 9/11 attacks on the World Trade Centers and the Pentagon, Congress deferred and enhanced presidential war powers by passing the Patriot Act. The Bill was passed almost unanimously, with only one vote in dissent¹. The intention was to put a swift and decisive end to international terrorism and take any measures necessary to prevent another attack on US soil.

Most infamously and relevant to this debate, the policy made it much easier for the government to spy on ordinary citizens via collecting phone records, bank information, email communication, and other forms of personal data². All of this data can be collected without a search warrant and requires little to no judicial oversight, as it is, in large part, secretive and classified. As a result, between 2003 and 2006, the FBI issued 192,499 national security letters to obtain personal information, but only 53 criminal referrals were made, none of which involved terrorism³.

At first, these programs were unknown to most Americans and governmental agencies. Sometimes, they were even touted for their efforts to stop terrorist attacks. The success of surveillance became entangled with the outrage of international terrorism. Consequently following the intensification of conflict in Afghanistan, the NSA’s surveillance capabilities were expanded by the FISA Amendments Act of 2008. These gave the NSA a blank check to monitor almost all personal internet and communication activity, so much so that virtually every email that goes into or out of the United States is scanned for suspicious keywords⁴.

It is this environment of unrestrained surveillance power that prompted the infamous 2013 NSA leaks from whistleblower Edward Snowden. He unveiled the true extent of NSA surveillance to the American people, generating significant backlash from the American people and members of government. After the Snowden leaks,

¹ Lind, Dara. “Everyone’s heard of the Patriot Act. Here’s what it actually does.” *Vox News*. 2 June 2015. <https://www.vox.com/2015/6/2/8701499/patriot-act-explain>

² “Surveillance Under the Patriot Act.” *American Civil Liberties Union*. 2011.

<https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>

³ “Surveillance Under the Patriot Act.” *American Civil Liberties Union*. 2011.

<https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>

⁴ “NSA Surveillance.” *American Civil Liberties Union*. 2013. <https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance>

some 54% of Americans disapproved of NSA surveillance and 74% said they should not give up personal freedoms for the sake of safety⁵. On an individual level, tech corporations and citizens began an encryption campaign for end-to-end encryption that protects user data to make it much harder for the government to find its way in. Nowadays, when the NSA attempts to install backdoors into Apple devices or Microsoft computers to spy on citizens, tech companies are able to push back and deny the administration, a battle they probably would have lost before the Snowden leaks⁶.

However, several years later, not much has changed from a legal standpoint. Section 215 of the Patriot Act that allowed the NSA to collect information from third parties to amass metadata was repealed and replaced with the USA Freedom Act. However, the Freedom Act did not eliminate mass metadata collection and merely mandated the NSA give congress annual activity reports that end up being vague and incomplete⁷. We are debating this topic at a time where the Government can still gather data on Americans without warrants, collect telephone metadata, and spy on foreign leaders⁸.

Analysis of the Resolution

“Resolved: The NSA should end its surveillance of US citizens and lawful permanent residents.”

This resolution, thankfully, is fairly straight-forward. It mandates a change to the status quo, where the NSA can legally spy on US citizens and asks us to evaluate those potential implications. That being said, I want to draw attention to two parts of the resolution: the term “surveillance” and the distinction of U.S. citizens and lawful permanent residents.

Government surveillance and the surveillance state is notoriously associated with the dystopia depicted in George Orwell’s 1984, where residents live under the constant state of being watched by “Big Brother.” Unsurprisingly, the NSA uses a plethora of big-brother-esque tactics depicted in the novel to conduct its surveillance. Using a

⁵ Gao, George. “What Americans think about NSA surveillance, national security, and privacy.” *Pew Research Center*. 29 May 2015. <https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/>

⁶ Shackford, Scott. “5 Years After Snowden, Has Anything Changed?” *Reason Magazine*. 6 June 2018. <https://reason.com/2018/06/06/5-years-after-snowden-has-anything-chang/>

⁷ Shackford, Scott. “5 Years After Snowden, Has Anything Changed?” *Reason Magazine*. 6 June 2018. <https://reason.com/2018/06/06/5-years-after-snowden-has-anything-chang/>

⁸ Childress, Sarah. “How the NSA Spying Programs Have Changed Since Snowden.” *PBS*. 9 February 2015. <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/>

program called PRISM, the NSA collects electronic data from services like Google, Facebook, Apple, and Microsoft⁹. On top of this, they skim emails, text messages, social media and phone conversations for suspicious activity. In the event their own hackers can't access the data, the NSA can force third parties to disclose private information to them in certain circumstances. They then store and encrypt this data should they ever need to return to it. In short, it is very sophisticated, very Orwellian, and very worrisome for those who value privacy.

The resolution is so specific when discussing NSA surveillance that it clarifies the surveillance on both U.S. citizens and lawful permanent residents. This specificity intentionally excludes non-citizens and undocumented residents. This was most likely done to enhance the debate and allow pro teams to argue that foreign espionage and military intelligence would not be compromised. In the affirmative world, the US can still spy on Russia, Iran, terrorist organizations, and collect foreign intelligence.

However, it is also important to consider the effect of NSA surveillance on temporary legal residents and undocumented immigrants. There undoubtedly exists systemic Islamophobia in high levels of government, so it is no surprise that NSA surveillance can disproportionately harm Muslim residents. For instance, the NSA already disproportionately monitors the data of Muslim Americans and travelers¹⁰. This is unsurprising given that in 2018, even the Supreme Court upheld an executive order labeled by scholars as the "Muslim Ban." For undocumented immigrants, NSA internet surveillance goes hand-in-hand with supporting ICE deportations and detentions. This issue is so prominent that scholars have labeled it Data-Driven Deportation¹¹. Clearly, the exclusion of these groups from the purview of the resolution has wide-ranging ramifications that need to be considered when crafting cases and formulating arguments. For the sake of these groups struggling with the challenges of systemic racism and xenophobia, it cannot be overlooked.

Why are we debating this resolution now?

For better or for worse (but mostly for worse), 2020 has brought many radical changes to our way of life. Among the most prominent changes was the rapid and sudden shift to life in the digital world. Work, school, entertainment, and even competitive high school debate have all found a new normal in online platforms and

⁹ Sottek, TC and Janus Kopfstein. "Everything you need to know about PRISM." *The Verge*. 17 June 2013. <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>

¹⁰ Sorkin, Amy Davidson. "The NSA's Spying on Muslim-Americans." *The New Yorker*. 10 July 2014. <https://www.newyorker.com/news/amy-davidson/the-n-s-a-s-spying-on-muslim-americans>

¹¹ Bedoya, Alvaro. "The Cruel New Era of Data-Driven Deportation." *Slate Magazine*. 22 September 2020. <https://slate.com/technology/2020/09/palantir-ice-deportation-immigrant-surveillance-big-data.html>

digital devices. Because of our increased dependence on technology to function in society, user data privacy and security is an issue close to the heart of many nowadays, and one where laws are normally lax and deferential to corporations. California has taken the lead in the United States, voting to strengthen consumer privacy in the 2020 election¹². While metadata is mostly stored, collected, sold, and utilized by the private sector, this mass data monitor originated with NSA surveillance. Beyond that, the NSA frequently steals data from third parties to monitor residents. Thus, with the expansion of technology, NSA surveillance must get put back into the public spotlight.

This topic also comes at a time amid national security threats that places emphasis on the NSA's role in defense policy. While tensions with Iran de-escalated since January and may continue to do so with the change in executive administration, conflict is not outside the realm of possibility. Last November, Trump's advisors even discussed options to attack Iran with the hopes of foiling their nuclear program¹³. The vast intelligence resources the NSA harbors become important tools for conflict resolution and escalation, especially when it comes to foreign espionage, offensive cyber operations, and cyber terrorism.

Argument Rundown

The central question of this debate is not a new one: how much privacy should citizens relinquish for the sake of national security? The PRO arguments of this debate revolve around the right to privacy, arguing that NSA surveillance unnecessarily suppresses personal freedoms to the point of significant harm. There are a few strategies that teams can utilize to emphasize this answer. First, on a principled level, violating individual privacy is unconstitutional and immoral. Violating individual autonomy with constant government surveillance dehumanizes individuals, destroys fundamental rights, and tramples on the social contract between the government and its citizens: the primary and original obligation the government has. Turning a blind-eye to human rights abuse destroys individual agency and compromises the US global standing as a human rights advocate to make civil liberties worse off around the world.

Second, government surveillance on citizens creates a chilling effect on free speech and political activity that threaten the very foundation of a functioning democracy. If citizens fear government persecution based on their words and actions, they self-censor and disengage from political processes. People lose faith in

¹² De Groot, Juliana. "What is the California Consumer Privacy Act?" *Digital Guardian Blog*. 1 December 2020. <https://digitalguardian.com/blog/what-california-data-privacy-protection-act>

¹³ Schmitt, Eric, Maggie Haberman, and David Sanger. "Trump Sought Options for Attacking Iran to Stop Its Growing Nuclear Program." *New York Times*. 2 December 2020. <https://www.nytimes.com/2020/11/16/us/politics/trump-iran-nuclear.html>

government, making it more likely they turn to populist demagogues (i.e., Donald Trump) or, worse, allow the government to become autocratic and totalitarian on its own.

Finally, from a more pragmatic perspective, NSA surveillance destroys data security by installing backdoors in programs and pooling metadata that is vulnerable to hacks and leaks. This makes the economy and national security worse-off as foreign and domestic hackers steal corporate intellectual property and launch cyber-attacks against critical infrastructure. Overall, PRO teams should further the narrative that security that comes at the cost of civil liberties is both pragmatically counterproductive and morally destructive. In the more eloquent words of Benjamin Franklin, “They who would give up essential liberty to obtain temporary safety, deserve neither liberty nor safety.”

CON teams will push back against that idea and argue that the government's first and primary obligation must be national security in order to protect civil rights and liberties. However, because of the underground nature of NSA operations, it is hard to calculate just how helpful the NSA is in furthering national security objectives. It would be smarter to articulate how much more difficult it would be for the FBI to operate absent the intelligence shared with the NSA. It would be logistically impossible for the NSA to receive a search warrant for every piece of user data they request. If they did, domestic terrorists would have an easier time planning and coordinating attacks on US soil or funding operations abroad. Beyond focusing purely on traditional terrorist attacks however, I think CON teams have a unique advantage in discussing the prevention of cyberterrorism and cyberattacks. Fighting in the cyber realm would be virtually impossible without some degree of surveillance or intelligence on domestic devices and users, necessitating the NSA have its current capabilities.

Strategically, CON teams should argue that personal privacy is already reduced by the natural expansion of technology and weak corporate user agreements, not the National Security Administration. Additionally, they also have the upper hand when it comes to argument comparison. Weighing the tangible number of lives lost from terrorist attacks or even cyber terrorism is much easier than weighing ambiguous principles of democracy and privacy that are difficult to measure. After all, it's worth scrolling past a few targeted advertisements if it means preventing acts of terror and saving countless lives.

PRO ARGUMENTS

BIG DATA COLLECTION

What's the argument?

The NSA collects private information on hundreds of millions of Americans every single day (Duckett). In 2017, the NSA collected over 534 million phone records, which was a threefold increase over the previous year (Savage). The NSA stores this data in millions of gigabytes and recklessly searches through American's private information. This is problematic for two key reasons.

First, the NSA's databases are vulnerable to hackers. In 2017, the NSA was hacked by a group called the Shadow Brokers, resulting in the compromise of key cyberweapons (Greene). Moreover, tools that the NSA uses to get around firewalls and into computer systems were leaked and stolen by this group, risking the safety of millions of US citizens' data.

Second, NSA policies actually encourage internet companies to collect more data by setting a standard of mass surveillance (Waddell). It is difficult to hold private companies accountable to privacy standards that the government itself fails to follow. These practices lead to further violations of privacy and erode freedom with the United States.

Why does the argument matter?

One potential impact is political polarization, as mass surveillance by private companies facilitates the use of targeted algorithms. These algorithms drive people further into echo chambers by encouraging interaction with like-minded individuals (Sirbu et al.). As a result, the opinions and voices of polarized groups are magnified, emboldening citizens, and leading to more conflict and clash within our political system. While our democracy hinges on differing viewpoints, immense amounts of polarization decrease the productivity of the government.

Main Players

Tech companies, American consumers

Strategy Considerations

Of the two, the average PF judge is more likely to buy the first warrant to this argument. The vast amount of data that the NSA collects is a treasure trove for hackers seeking access to Americans' information. If they are able to gain access to the database, millions upon millions of pieces of information about American citizens and permanent residents fall into jeopardy. However, teams will likely struggle to prove that foreign actors can and will use this data to tangibly harm people's lives as there is little precedent to support the argument.

The second warrant is more difficult to prove and terminalize but has a more direct impact. Teams must demonstrate that private companies' surveillance of Americans will decrease, or at least plateau, if we end the NSA practice of mass surveillance. The easiest way that this can be done, in my opinion, is through a political analysis (i.e., in the status quo, holding private companies accountable is like the pot calling the kettle black). By proving that the NSA sets a national precedence for data surveillance, teams can argue that private companies will follow suit.

Evidence for Big Data Collection

Massive volume of data collected

The NSA collects hundreds of millions of records each year

Savage, Charlie. "NSA Triples Collection of Data from US Phone Companies." *New York Times*. 4 May 2018. <https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html>

The National Security Agency vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year – more than three times what it collected in 2016, a new report revealed on Friday. Intelligence analysts are also more frequently searching for information about Americans within the agency's expanding collection of so-called call detail records – telecom metadata logging who contacted whom and when, but not the contents of what they said. The new report – an annual set of surveillance-related statistics issued by the Office of the Director of National Intelligence – did not explain why the number of records increased so dramatically. But in an interview, Alex Joel, the office's chief civil liberties officer, said the N.S.A. had not reinterpreted its legal authorities to change the way it collects such data. He cited a variety of factors that might have contributed to the increase, potentially including changes in the amount of historical data companies are choosing to keep, the number of phone accounts used by each target and changes to how the telecommunications industry creates records based on constantly shifting technology and practices. "Based on what we have learned from this data, we expect it will continue to fluctuate from year to year," Mr. Joel said. Still, the large and growing volume of data gathered shows that the N.S.A. continues to collect significant amounts of information about Americans' phone and text messages after changes made by Congress in a 2015 law, the USA Freedom Act, which overhauled how the N.S.A. can gain access to domestic telecom data. That law ended a once-secret program by which the N.S.A. had systematically collected Americans' domestic phone logs in bulk – billions of records per day. The program traced back to the aftermath of the Sept. 11 attacks and was revealed in 2013 by leaks from Edward J. Snowden, the former intelligence contractor, setting off a wide debate over surveillance and privacy. Though Congress ended that program, lawmakers still wanted the N.S.A. to retain its function: the ability to analyze links between people in search of hidden associates of terrorism suspects. So it authorized a new system in which the bulk records stay with the phone companies but the N.S.A. can get copies of all records of a target and everyone with whom a target has been in contact. The phone companies turn over both whatever historical records they have for targets and for their associates, as well as new logs from calls and texts after the order. The system requires the Foreign Intelligence Surveillance Court to agree that there is "reasonable, articulable suspicion" that the seed target is linked to terrorism. In 2016, the first full year for which that replacement system was in operation, the government obtained orders to target 42 people and collected just over 151 million call detail records. In 2017, the government obtained orders for 40 targets. (The orders generate data for 180 days, so some of the 2016 orders kept generating additional data in 2017, and some of the 2017 orders may have been reauthorizations of expiring 2016 orders pegged to the same targets.) After the N.S.A. put the record sets obtained from the telecoms into its databases, intelligence analysts queried that data using 31,196 search terms associated with Americans last year, up from 22,360 a year earlier. The large volume of records generated from a relatively small number of targets is attributable to several factors. One is the exponential math associated with gathering the communications logs not just of targets, but of every person with whom a target has been in contact. Another is that some conversations generate more than one record at phone companies. These apparently include back-and-forth via text messages, as well as calls involving cellphone users on the move, whose calls are handled by different cellphone towers. Officials have also cautioned that some records gathered by the N.S.A. are duplicates: A call between an AT&T customer and a Verizon customer, for example, generates records at both companies. The report listed several other notable statistics about surveillance activities. For example, it showed that the number of people whom the surveillance court granted approval to target with wiretaps for national-security purposes dropped somewhat, from 1,687 in 2016 to 1,337 last year. By contrast, the number of targets for the N.S.A.'s warrantless surveillance program – noncitizens abroad whose communications are collected from American companies like Google – grew significantly, from 106,469 in 2016 to 129,080 last year. The warrantless surveillance program also grew out of the once-secret post-Sept. 11 programs, and is now conducted under a law called Section 702 of the FISA Amendments Act. It has attracted controversy because when foreign targets communicate with Americans, the government collects those Americans' emails and other private messages without a warrant, too. Congress reauthorized that law without major changes this year. The report contains several statistics about how the government has used Americans' information that it gathered without a warrant under Section 702. Analysts queried metadata harvested from that program for information about an American 16,924 times in 2017. That was down from 30,355

times the previous year; the report did not explain the drop. F.B.I. agents did not open any criminal investigations into an American that had no connection to national security in 2017 based on Section 702 data, the report said. Nor did they scrutinize any communications in the Section 702 database that came up in response to queries for an American's information when agents were working on a criminal case that had no connection to foreign intelligence. But the report did not disclose how many times the bureau did either of those things when agents did deem their work to have a foreign intelligence or security link. It also did not disclose the volume of Americans' communications or metadata gathered by the N.S.A.'s work abroad, where its activities are regulated by Executive Order 12333, not the Foreign Intelligence Surveillance Act, and it is permitted to engage in bulk collection.

NSA collects 29 million gigabytes of data each day, despite not actively reviewing all of that data

Duckett, Chris. "NSA hunger demands 29 petabytes of data a day." *ZDNet*. 12 August 2013. <https://www.zdnet.com/article/nsa-hunger-demands-29-petabytes-of-data-a-day/>

As the National Security Agency (NSA) spying furore rumbles on, the agency has claimed to be looking at only 0.00004 percent of the world's total internet traffic. In a document (PDF) on the nsa.gov website, the agency said that the internet carries 1,826 Petabytes of information per day, and that **its activity "touches"** 1.6 percent of that data – approximately 29 petabytes, or **29 million gigabytes, of data each day. Of that number, the agency says 0.025 percent is selected for review.**

NSA is vulnerable to hackers

NSA subject to major security breach

Greene, David. "NSA's Hackers Were Themselves Hacked In Major Cybersecurity Breach." *NPR*. 14 November 2017. <https://www.npr.org/2017/11/14/564006460/nsas-hackers-are-hacked-in-major-cybersecurity-breach#:~:text=A%20group%20known%20as%20The,have%20been%20hacked%2C%20it%20appears.&text=Matthew%20Olsen%20worked%20at%20the,of%20the%20National%20Counterterrorism%20Center>

And let's talk now about an extraordinary security breach at the NSA. A group known as The Shadow Brokers have stolen sophisticated tools the agency uses to penetrate computer networks. In other words, **the NSA's own hackers have been hacked**, it appears. This all began last year, and it looks like The Shadow Brokers have tried to sell some of the NSA's cyberweapons. Matthew Olsen worked at the NSA as general counsel. He was later director of the National Counterterrorism Center. He's in our studio this morning.

Thanks for coming in. MATTHEW OLSEN: Thanks for having me. GREENE: So who are The Shadow Brokers? OLSEN: You know, **The Shadow Brokers is**, you know, as the name implies, **a very shadowy group of hackers**, and apparently very sophisticated hackers. We don't know, though, exactly who they are or even where they are. GREENE: You don't know, and presumably **the NSA has not been able to figure this out**, which is part of the alarm here. OLSEN: It certainly is part of the ongoing investigation - find out who these folks are, how they got these tools, where the tools came from. Remember, this is an ongoing investigation, and at this point, nobody's been identified as who those hackers are. GREENE: So this could be a foreign government. This could be just some hackers who wanted to get this stuff. This could, in theory, involve employees at the NSA itself. I mean, a lot of possibilities here. OLSEN: Lots of possibilities, lots of speculation. But the, you know, one of the main candidates is possibly a foreign government because of how sophisticated these hackers appear to be. GREENE: And what exactly are the tools that they have been able to steal? OLSEN: Yeah. It's exactly as you said, David. **Very sophisticated, very sensitive, high-end, really weapons-grade computer code. These are hacking tools that are used to get around firewalls, to defeat anti-virus, to get into computer systems. They're exactly the kind of tools that nations build in order to exploit communications.** GREENE: You said weapons-grade. I mean, help people understand, you know, what a cyberweapon is as opposed to a more traditional weapon. OLSEN: Yeah. Well, there's lots of

hackers out there. We all hear about hackers and cyberattacks all the time, but there's levels of gradation in terms of how sophisticated those types of weapons are, those types of attacks are. Code like this that's used to break into very sophisticated and well-defended computer systems, that takes years and years to develop, and lots and lots of money and very, very sophisticated computer scientists and engineers. And that's what's so troubling here, is that apparently these tools have now fallen into the wrong hands. GREENE: OK. So I don't want to speculate too much, but you say that there's the possibility that this is a foreign government. We've heard all about, you know, Russia's capabilities and other nations. If a nation like Russia had these tools, what could they do with them and how damaging could it be to U.S. national security? OLSEN: Well, the really dangerous thing now is that these tools are out in the wild. So what we're seeing, and we've seen this over the last year, is that these tools are being used to facilitate computer attacks. So we saw ransomware attacks earlier this year that affected millions of people. GREENE: Using these tools. OLSEN: Using these tools to really advance the attacks, really to carry out these exploits. GREENE: There were some hospitals in Britain, I think, that were turning away patients because of one of these attacks. OLSEN: Exactly right. So they're used - they've been used also to go after really critical organizations like hospitals both here in the United States and in Europe. And so now these tools that were really possibly just in the hands of a very small number of people, inside governments, are now out and available on the internet. So, you know, pretty much anyone who's sophisticated can now get access to them. GREENE: A lot of people hear NSA, and they think about the name Edward Snowden and that leak. People are suggesting this might be far worse than that in terms of the credibility of the agency and also the potential damage. Is that true? OLSEN: It does seem like that's potentially true. I mean, Edward Snowden did damage, no doubt. He talked about programs that had been classified and were secret and gave insights to our adversaries about those programs. But this could be worse in the sense that this isn't just about the programs generally, but it's the computer code, the actual weapons, the actual information that can be used to carry out attacks. And so that's why it's potentially even worse. GREENE: I think Americans like to think of their government being very good at counterterrorism, very good at intelligence, and they would wonder, how in the world could this happen, how in the world does it keep happening? OLSEN: So our government is very good at this, and very good at defending information and also collecting foreign intelligence. I mean, take a step back and remember NSA's job is to go out around the world and collect foreign intelligence, identify the communications of our adversaries, terrorists, other nations and pull in those communications. But that job has gotten a lot harder in the digital age. This is not James Bond picking up a single digital cassette tape, for example. This is trying to find signals around the world and pick those up in this vast digital noise, and they're very, very good at it. GREENE: Just briefly, how bad is morale right now inside the agency? OLSEN: Yeah, I can understand the concern about morale in the agency, but I worked with these folks. These are some of the most dedicated and most brilliant people I've ever worked with. They are only going to redouble their efforts, I think. GREENE: Matthew Olsen was the general counsel at the NSA, former director of the National Counterterrorism Center, talking to us about a significant hack of the agency that they're confronting right now. Thanks for coming in. We appreciate it. OLSEN: Thanks for having me, David.

NSA policies encourage internet companies to collect more data

Private companies collect the same data that the NSA does

Waddell, Kaveh and National Journal. "The NSA's Bulk Collection is Over, but Google and Facebook are still in the Data Business." *The Atlantic*. 3 June 2015.

<https://www.theatlantic.com/politics/archive/2015/06/the-nsas-bulk-collection-is-over-but-google-and-facebook-are-still-in-the-data-business/458496/>

Don't be fooled: Congress may have finally passed the bill reining in the National Security Agency's bulk-surveillance programs, but your data is still being collected on the Internet. Lost in the debate over the NSA is the fact that companies like Google and Facebook continue to vacuum up vast troves of consumer data and use it for marketing.

The private-sector tech companies that run the social networks and email services Americans use every day are relatively opaque when it comes to their data-collection and retention policies, which are engineered not to preserve national security but to bolster the companies' bottom lines. Critics say the consumer data that private companies collect can paint as detailed a picture of an individual as the metadata that got caught up in the NSA's dragnets. Companies like Google and Facebook comb through customers' usage statistics in order to precisely tailor marketing to their users, a valuable service that advertisers pay the companies dearly to access. "What both types of information collection show is that metadata—data about data—can in many cases be more revelatory than content," said Gabe Rottman, legislative counsel at the American Civil Liberties Union. "You see that given the granularity with which private data collection can discern very intimate details about your life." And there's no guarantee what is collected by the private sector will stay with the private sector. "The government has a huge number of tools to get data from private companies," said Chris Calabrese, senior policy director at the Center for

Democracy and Technology. "That's obviously a very difficult situation for companies to be in." Law-enforcement agencies are looking for even more ways to access private companies' data. Some social-networking sites have begun encrypting the data that's sent through their servers, prompting the FBI to ask companies to make their data available to the agency when asked. "We suggest, and we are imploring, Congress to help us seek legal remedies towards that as well as asking the companies to provide technological solutions to help that," said Michael Steinbach, assistant director of the FBI's counterterrorism division, at a congressional hearing Wednesday. "Privacy above all other things, including safety and freedom from terrorism, is not where we want to go." Still, comparing NSA spying and private-sector data-gathering is "a little bit apples to oranges," Calabrese said. "There's real concerns around government overreach that have to do with our constitutional values and what we care about as a nation." Unlike the private sector, Rottman said, "government can take your life or liberty." When users sign onto Google or Facebook, they choose to give up their personal information in order to get valuable services from the companies, which sets up a dynamic fundamentally different from government surveillance. But more often than not, Calabrese says, user consent is not enough to justify data collection, because of the lack of transparency in the process. "People aren't always aware of the amount of information being collected about them when they surf online," he said. "People should be voting with their feet when companies aren't supporting the most aggressive privacy policies," Rottman said. But users are often not informed voters. "You can't vote with your feet unless you know you need to vote with your feet," said Rottman. Although the Senate's attention has been caught up lately in the debate over government surveillance, legislation introduced earlier this year aimed to bolster data privacy by placing limits on the private sector. Sen. Ed Markey, D-Mass., is behind two such bills this year. Along with Sen. Orrin Hatch, R-Utah, Markey reintroduced legislation last month that would place security requirements on companies that deal in student data and would forbid them from using student data for advertising. Markey also reintroduced a more general bill in March aimed at improving the accuracy of personal information stored online. It would require "data brokers"—that is, companies that collect and sell personal data—to have a system by which users can verify that their information is correct and to allow users to choose not to make their data available for marketing. And Sen. Bernie Sanders, the Democratic presidential candidate, a longtime advocate of data privacy, has turned his trademark ire against both the government's and the private sector's data-collection policies. He calls government surveillance "Orwellian" and presents a bleak picture of agencies obsessed with tracking Americans' every movement, but his criticism is not limited to the government. "While today we are focusing appropriately on the role of the federal government in issues of civil liberties, we must also understand that it is not just the government that is collecting information on law-abiding Americans," Sanders said in a speech last month. "In fact, the private sector's collection of information is just as intrusive and equally dangerous." Sanders said during that speech that he will introduce legislation calling for a "comprehensive review of data collection by public and private entities and the impact that that data is having on the American people." That legislation has not yet materialized, and the senator's office remains tight-lipped about the bill. For their part, various tech companies are paying attention to the trend. Google on Monday unveiled a frequently asked questions page to address users' privacy concerns, answering questions like "Does Google sell my personal information?" and "How does Google keep my information safe?" It also revamped its account settings page, offering privacy and security "checkups" to walk users through steps to keep their data safe. On the same day, Facebook announced it will offer the option to send sensitive information, like password reset links, in encrypted emails. ("New Facebook feature shows actual respect for your privacy," read a Wired headline on an article about the announcement.) Facebook already encrypts traffic to and from its site, and offers privacy fanatics—or those who fear government retribution for their actions on the social network—access to its services via the Tor browser, widely regarded as the most secure and private way to access the Internet. The companies' changes are moves in the right direction, according to Calabrese. Although Google's announcement did not include any changes in data-collection policy, it did represent an important increase in transparency and accessibility. "Usability really does matter," Calabrese said. "Too often, privacy controls are hard for consumers to figure out. They tend to get frustrated and not use them."

Algorithms based on surveillance data fuel political polarization

Algorithmic bias increases polarization by creating an echo chamber

Sirbu, Alina. "Algorithmic bias amplifies opinion fragmentation and polarization: A bounded confidence model." *PLoS ONE*. 5 March 2019.

<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0213246>

Algorithmic bias is a mechanism that encourages interaction among likeminded individuals, similar to patterns observed in real social network data. We found that, for this model, algorithmic bias hinders consensus and favors opinion fragmentation and polarization through different mechanisms. On one hand, consensus is hindered by a very strong slowdown of convergence, so that even when one cluster is asymptotically obtained, the time to reach it is so long that in practice

consensus will never appear. Additionally, we observed fragmentation of the population as the bias grows stronger, with the number of clusters obtained increasing compared to the original model. At the same time, the average opinion distance also grew in the population, indicating emergence of polarization. A fragmented initial condition also enhances the fragmentation and polarization, augmenting the effect of the algorithmic bias. Additionally, we observed that small populations may be less resilient to fragmentation and polarization, due to finite size effects. The results presented here are based on the mean field bounded confidence model, and may be influenced by this choice. A first assumption is that bounded confidence exists, i.e individuals with very distant opinions do not exchange information hence do not influence each other. However, our conclusions regarding the fact that algorithmic bias hinders consensus still stand even when bounded confidence is removed from this model (i.e. $\epsilon = 1$). In this case, consensus still becomes extremely slow as the bias increases, hence is never achieved in practice, a result that we believe will apply to many other models with attractive dynamics. Secondly, adding noise to the model could change results, since noise in the bounded confidence model can facilitate consensus [37]. Adaptive noise, on the other hand, could generate metastable clusters [38]. A different issue is the structure of the opinion clusters. In our model clusters form and then they become static, with no further changes possible (neither increase or decrease in opinion distances). However in reality polarization may increase or decrease in time also after clusters form. Adding noise could also be an answer for this issue, however we intend to study alternative mechanisms to embed this type of situation in the model.

HURTING US BUSINESSES ABROAD

What's the argument?

The basic gist of this argument is that NSA surveillance makes it difficult for U.S. businesses to work with foreign nations or companies because of fears of data breaches. After the Snowden leaks, foreign countries were disillusioned with the U.S. and feared that any data stored by U.S.-based cloud service providers was not secure. Princeton technologist Ed Felton wrote that the leaks would harm U.S. companies, as people would believe that they “lack the ability to protect their customers” (Hill). Security expert Bruce Schneier wrote that foreign buyers will assume that “[U.S.] companies have been co-opted” (Hill). Technology companies have been forced to win back customers in any way possible, with IBM spending “more than a billion dollars to build data centers overseas to reassure foreign customers that their information is safe from prying eyes in the U.S. government” (Miller).

Why does the argument matter?

After NSA surveillance programs were exposed, it was predicted that U.S. companies would lose between \$21.5 billion and \$35 billion, with cloud service providers taking the biggest hits (Enderle). (Cloud service providers are companies that supply individuals or businesses with offline infrastructure for data storage or network services.) Many organizations have estimated that the losses were much higher, with Forrester Research calculating that losses “could be as high as \$180 billion,” which is 25% of the cloud computing industry’s total revenue (Miller). In fact, a 2014 survey found that 25% of companies in the UK and Canada planned to pull data out of the U.S. (Enderle). Companies from other countries have reported massive upticks in users as consumers abandon U.S. businesses in search of better security elsewhere. For example, Runbox, an Norwegian email service, “reported a 34 percent annual increase in customers after news of the N.S.A. surveillance” (Miller).

Main Players

U.S. cloud computing companies, U.S. tech companies, foreign investors and consumers

Strategy Considerations

This argument is effective because it provides a good foil for popular arguments, such as NSA surveillance preventing IP theft and keeping businesses from losing money to cyber-attacks. If foreign and domestic buyers alike are reluctant to support U.S. tech companies, those companies are going to move abroad or go out of business, which would harm the U.S.'s global standing in terms of innovation. Regarding the economy, if companies are losing tens of billions of dollars, you can argue that this outweighs the monetary consequences of small-scale cyber-attacks.

There are a few specific examples of companies losing money and business that can be used as anecdotal examples of NSA surveillance harming businesses. Applying a specific name to large impacts of "\$180 billion lost" can help make your argument feel more concrete and immediate. First, AT&T wanted to make a bid on Vodafone, a company that owns cell phone networks across Europe, but the deal eventually fell through. Officials feared that an AT&T acquisition "could turn local carriers into data siphons for American intelligence agencies" (Robertson). Second, Cisco Systems, another tech company, stated that discovery of NSA surveillance has prompted "uncertainty or concern," which has harmed demand. Namely, new orders in developing nations fell 12%, while other countries saw demand slip as much as 30% (Waters).

Evidence for Hurting US Businesses Abroad

NSA Surveillance Costs Tech Companies Money

The Snowden leaks caused foreign companies to lose faith in US data security promises.

Hill, Kashmir. "How the NSA Revelations are Hurting Businesses." *Forbes*. 10 September 2013. <https://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/?sh=12c970162c64>

The NSA leaks just keep on comin'. Last week, we found out that the nation's suddenly-not-so-secretive spy agency has made huge strides in compromising some forms of encryption that help keep information private on the Web. This was done through known workarounds, "covertly introducing weaknesses into encryption standards" and strong-arming companies into handing over encryption keys, or according to the New York Times, stealing them. The recent revelations suggest that the reason Edward Snowden email-provider Lavabit shut down this summer was because the government was trying to force it to hand over encryption keys so that agents would have the power to read users' emails. It's yet another revelation in the "summer of Snowden leaks" that's making life difficult for American businesses. Princeton technologist Ed Felten -- who used to be government-employed at the Federal Trade Commission -- writes, "This is going to put U.S. companies at a competitive disadvantage, because people will believe that U.S. companies lack the ability to protect their customers--and people will suspect that U.S. companies may feel compelled to lie to their customers about security." "I can't imagine foreign buyers trusting American products," says security expert Bruce Schneier. "We have to assume companies have been co-opted, wittingly or unwittingly. If you were a company in Sweden, are you really going to want to buy American products?" Earlier this summer, technology analyst Daniel Castro authored a report suggesting that revelations about corporate cooperation with the government through programs like PRISM would take a toll on cloud computing businesses to the tune of \$22 to \$35 billion over the next three years "if foreign customers decide the risks of storing data with a U.S. company outweigh the benefits." "Members of Congress didn't want U.S. companies to use Huawei products because the Chinese might spy on American citizens. I expect that argument will now be leveled by many countries at the entire U.S. tech sector," says Castro by email of the recent encryption news. "One of the important questions that needs to be cleared up is whether the NSA merely broke some crypto standards or whether they really did weaken them and implement versions of these standards with backdoors. If it's the former, then all companies who use these standards are in trouble, not just US firms. If the latter, then U.S. companies will be hurting the most from this news."

NSA programs have cost companies billions of dollars and reduce the US' intelligence capability

Enderle, Rob. "US Surveillance Programs are Killing the Tech Industry." *CIO*. 12 June 2015. <https://www.cio.com/article/2934887/u-s-surveillance-programs-are-killing-the-tech-industry.html>

The Information Technology & Innovation Foundation, ranked as the most authoritative science and technology think tank in the U.S. (second in the world behind Max Planck Institutes of Germany), has just released its latest report on the impact of the existence and disclosure of the broad NSA national and international spying programs. It was initially reported that the revenue loss range would be between \$21.5 billion and \$35 billion, mostly affecting U.S. cloud service providers. However, they

have gone back and researched the impact and found it to be both far larger and far broader than originally estimated. In fact, it appears the surveillance programs could cause a number of U.S. technology firms to fail outright or to be forced into bankruptcy as they reorganize for survival. The damage has also since spread to domestic aerospace and telephony service providers. The programs identified in the report are PRISM; the program authorized by the FISA Amendments act, which allowed search without the need for a warrant domestically and abroad, and Bullrun; the program designed to compromise encryption technology worldwide. The 2014 survey indicates that 25 percent of companies in the UK and Canada plan to pull data out of the U.S. Of those responding, 82 percent indicated they now look at national laws as the major deciding factor with regard to where they put their data. The irony here is that if the U.S. loses the technology industry and it moves to Asia and Europe the U.S. spy agencies will lose virtually all of their spying digital capability anyway, or it will drop to the same level as a non-tech third-world country, because they won't be able to force the foreign firms to give them inside access. It could also be noted that they will also lose the capability to develop leading tech-based tools and weapons as those skills also migrate out of the U.S. So, in a foolish effort to make the country safer, not only is the collateral damage unacceptable to the U.S. economy it will likely result in a dramatically reduced intelligence capability. This is a level of self-correction the U.S. might not recover from.

Foreign countries and companies no longer trust US companies to protect their data

Miller, Claire Cain. "Revelations of NSA Spying Cost US Tech Companies." *The New York Times*. 21 March 2014. <https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>

Microsoft has lost customers, including the government of Brazil. IBM is spending more than a billion dollars to build data centers overseas to reassure foreign customers that their information is safe from prying eyes in the United States government. And tech companies abroad, from Europe to South America, say they are gaining customers that are shunning United States providers, suspicious because of the revelations by Edward J. Snowden that tied these providers to the National Security Agency's vast surveillance program. Even as Washington grapples with the diplomatic and political fallout of Mr. Snowden's leaks, the more urgent issue, companies and analysts say, is economic. Technology executives, including Mark Zuckerberg of Facebook, raised the issue when they went to the White House on Friday for a meeting with President Obama. It is impossible to see now the full economic ramifications of the spying disclosures – in part because most companies are locked in multiyear contracts – but the pieces are beginning to add up as businesses question the trustworthiness of American technology products. The confirmation hearing last week for the new N.S.A. chief, the video appearance of Mr. Snowden at a technology conference in Texas and the drip of new details about government spying have kept attention focused on an issue that many tech executives hoped would go away. Despite the tech companies' assertions that they provide information on their customers only when required under law – and not knowingly through a back door – the perception that they enabled the spying program has lingered. "It's clear to every single tech company that this is affecting their bottom line," said Daniel Castro, a senior analyst at the Information Technology and Innovation Foundation, who predicted that the United States cloud computing industry could lose \$35 billion by 2016. Forrester Research, a technology research firm, said the losses could be as high as \$180 billion, or 25 percent of industry revenue, based on the size of the cloud computing, web hosting and outsourcing markets and the worst case for damages. The business effect of the disclosures about the N.S.A. is felt most in the daily conversations between tech companies with products to pitch and their wary customers. The topic of surveillance, which rarely came up before, is now "the new normal" in these conversations, as one tech company executive described it. "We're hearing from customers, especially global enterprise

customers, that they care more than ever about where their content is stored and how it is used and secured," said John E. Frank, deputy general counsel at Microsoft, which has been publicizing that it allows customers to store their data in Microsoft data centers in certain countries. At the same time, Mr. Castro said, companies say they believe the federal government is only making a bad situation worse. "Most of the companies in this space are very frustrated because there hasn't been any kind of response that's made it so they can go back to their customers and say, 'See, this is what's different now, you can trust us again,'" he said. In some cases, that has meant forgoing potential revenue. Though it is hard to quantify missed opportunities, American businesses are being left off some requests for proposals from foreign customers that previously would have included them, said James Staten, a cloud computing analyst at Forrester who has read clients' requests for proposals. There are German companies, Mr. Staten said, "explicitly not inviting certain American companies to join." He added, "It's like, 'Well, the very best vendor to do this is IBM, and you didn't invite them.'"

The result has been a boon for foreign companies. Runbox, a Norwegian email service that markets itself as an alternative to American services like Gmail and says it does not comply with foreign court orders seeking personal information, reported a 34 percent annual increase in customers after news of the N.S.A. surveillance. Brazil and the European Union, which had used American undersea cables for intercontinental communication, last month decided to build their own cables between Brazil and Portugal, and gave the contract to Brazilian and Spanish companies. Brazil also announced plans to abandon Microsoft Outlook for its own email system that uses Brazilian data centers. Mark J. Barrenechea, chief executive of OpenText, Canada's largest software company, said an anti-American attitude took root after the passage of the Patriot Act, the counterterrorism law passed after 9/11 that expanded the government's surveillance powers. But "the volume of the discussion has risen significantly post-Snowden," he said. For instance, after the N.S.A. surveillance was revealed, one of OpenText's clients, a global steel manufacturer based in Britain, demanded that its data not cross United States borders.

Costs of Snowden leak and NSA surveillance are not short-term

Riechmann, Deb. "Costs of Snowden Leak Still Mounting 5 Years Later." *The Associated Press*. 4 June 2018. <https://apnews.com/article/797f390ee28b4bfbb0e1b13cfedf0593>

WASHINGTON (AP) – Whistleblower or traitor, leaker or public hero? National Security Agency contractor Edward Snowden blew the lid off U.S. government surveillance methods five years ago, but intelligence chiefs complain that revelations from the trove of classified documents he disclosed are still trickling out. That includes recent reporting on a mass surveillance program run by close U.S. ally Japan and on how the NSA targeted bitcoin users to gather intelligence to support counterterrorism and to combat narcotics and money laundering. The Intercept, an investigative publication with access to Snowden documents, published stories on both subjects. The top U.S. counterintelligence official said journalists have released only about 1 percent taken by the 34-year-old American, now living in exile in Russia, "so we don't see this issue ending anytime soon." "This past year, we had more international, Snowden-related documents and breaches than ever," Bill Evanina, who directs the National Counterintelligence and Security Center, said at a recent conference. "Since 2013, when Snowden left, there have been thousands of articles around the world with really sensitive stuff that's been leaked." On June 5, 2013, The Guardian in Britain published the first story based on Snowden's disclosures. It revealed that a secret court order was allowing the U.S. government to get Verizon to share the phone records of millions of Americans. Later stories, including those in The Washington Post, disclosed other snooping and how U.S. and British spy agencies had accessed information from cables carrying the world's telephone and internet traffic. Snowden's defenders maintain that the U.S. government has for years exaggerated the damage his disclosures caused. Glenn Greenwald, an Intercept co-founder and former journalist at The Guardian, said there are "thousands upon thousands of documents" that journalists have chosen not to publish because they would harm peoples' reputation or privacy rights or because it would expose "legitimate surveillance programs." "It's been almost five years since newspapers around the world began reporting on the Snowden archive and the NSA has offered all kinds of shrill and reckless rhetoric about the 'damage' it has caused, but never any evidence of a single case of a life being endangered let alone harmed," Greenwald said.

Examples of specific companies losing money

AT&T's acquisition of Vodafone failed due to NSA surveillance news

Troianovski, Anton, Thomas Gryta, and Sam Schechner. "NSA Fallout Thwarts AT&T." *The Wall Street Journal*. 30 October 2013.

<https://www.wsj.com/articles/SB10001424052702304073204579167873091999730>

AT&T Inc.'s 1.06% ambitions to expand in Europe have run into unexpected hurdles amid the growing outcry across the region over surveillance by the National Security Agency. German and other European officials said any attempt by AT&T to acquire a major wireless operator would face intense scrutiny, given the company's work with the U.S. agency's data-collection programs. Resistance to such a deal, voiced by officials in interviews across Europe, suggests the impact of the NSA affair could extend beyond the diplomatic sphere and damage U.S. economic interests in key markets. AT&T Chief Executive Randall Stephenson has signaled repeatedly in recent months that he is interested in buying a mobile-network operator in Europe, highlighting the potential for growth on the continent at a time when the U.S. company faces headwinds at home. On Wall Street, many bankers, investors and analysts expect AT&T to make a bid for Vodafone Group PLC, which owns cellphone networks across Europe, as early as the first half of next year. Such a deal would be one of the largest corporate acquisitions ever and present a degree of risk for AT&T's management. In 2011, AT&T's \$39 billion takeover of T-Mobile USA, then a unit of Deutsche Telekom AG, collapsed over competition concerns by U.S. regulators. Europe's anger over the NSA's collection of electronic communications has reduced the likelihood a European deal could happen anytime soon. AT&T is among the U.S. phone companies that provide calling data to the NSA to feed the far-reaching surveillance programs disclosed by former NSA contractor Edward Snowden. The Wall Street Journal reported in June. AT&T and Vodafone declined to comment for this article. In Germany, Europe's biggest market and one in which Vodafone is the No. 2 mobile operator, the surveillance controversy has played prominently in the headlines for months. Allegations last week that the U.S. monitored Chancellor Angela Merkel's phone added even more fuel to the fire in the privacy-sensitive country. "One would really have to ask: Should this be allowed? Does this make sense? What does this mean for our standards of data privacy?" Anton Hofreiter, co-leader in parliament of the minority left-leaning Greens, said of a potential AT&T deal. Peter Schaar, Germany's federal commissioner for data protection, said AT&T would need to make it clear before closing a deal for a telecommunications company doing business in Germany that it wouldn't provide any data to the NSA without adhering to Germany's strict privacy laws. Mr. Snowden's disclosures in recent months have shown how the NSA is able to collect data about people in other countries when that data passes through the U.S. And Journal reporting has shown that the NSA can intercept such communications on the U.S. Internet backbone via relationships with telecom companies including AT&T. "One would need to create transparency ahead of time so that everyone knows what the legal basis is" for how AT&T treats German data, Mr. Schaar said in an interview. "The public and the regulators have become much more attentive now that we know, and also in part suspect, how far the surveillance goes."

NSA surveillance prevented AT&T expansion

Robertson, Adi. "NSA Surveillance Revelations Hobble AT&T's Attempts at a European Expansion." *The Verge*. 31 October 2013.

<https://www.theverge.com/2013/10/31/5050164/nsa-surveillance-revelations-hobble-at-ts-attempts-at-a-european>

AT&T's attempts to move into Europe by acquiring local telecoms could be stymied by the recent leaks of NSA surveillance data, European officials tell The Wall Street Journal. Along with Sprint and Verizon, AT&T is implicated in the Obama administration's widespread data collection: the FISA Amendments Act allows the NSA to request all phone metadata records from the companies. A potential expansion, officials fear, could turn local carriers into data siphons for American intelligence agencies. That means they're likely to heavily scrutinize or outright block any potential deals. "We'd need to have a concrete discussion to make sure that European data wouldn't be leaving Europe," one official tells the Journal. The stream of leaked documents have revealed tight collaboration between the NSA and other intelligence agencies, as well as routine wiretapping of government leaders' phones. Since it was revealed that the US had collected phone data from German chancellor Angela Merkel starting in 2002, tensions between the two countries have been particularly high, with both German parliament members and the generally pro-surveillance Senator Dianne Feinstein (D-CA) calling for an investigation. AT&T has reportedly been in talks with UK carrier Vodafone, which it tentatively hopes to acquire in order to expand its European presence. But Vodafone's huge presence in Europe, particularly in Germany, raises serious concerns. If AT&T were to take over Vodafone, German commissioner for data protection Peter Schaar says it would need to "create transparency ahead of time," laying out how it would treat communications under Germany's data protection laws. "The public and the regulators have become much more attentive now that we know, and also in part suspect, how far the surveillance goes."

Cisco blames NSA for sales slump

Waters, Richard. "Cisco Cites Emerging Markets Backlash on NSA Leaks for Sales Slump." *The Financial Times*. 13 November 2013. <https://www.ft.com/content/445c67ce-4cb1-11e3-958f-00144feabdc0>

Cisco Systems warned its revenues could fall as much as 10 per cent in the current quarter, sparking fears that the US networking equipment company is losing ground amid big technology transitions in some of its markets. Recent revelations about internet surveillance by the US National Security Agency had prompted a "level of uncertainty or concern" among customers internationally that had contributed to sliding demand, Frank Calderone, chief financial officer, said. New orders fell 12 per cent in the developing world, with Brazil down 25 per cent and Russia off 30 per cent, a sharp reversal from the 8 per cent jump experienced in the preceding three months. The collapse coincided with the international furore over disclosures that the NSA had taken advantage of the strong position of US technology companies to extend its surveillance of the global internet, raising concerns about a backlash against American companies such as Cisco. The forecast came as a shock to Wall Street analysts who had been expecting growth of 6 per cent, leading to a 10 per cent fall in Cisco's shares in after-market trading on Wednesday. Chief executive John Chambers blamed the decline on a slump in demand from customers in emerging markets and suggested a range of technology companies were likely to be similarly affected. He said the decision to cut back Cisco's TV set-top box operations to focus on more profitable parts of the business had also played a role.

Impacts

The US is already falling behind in innovation for other reasons

Condliffe, Jamie. "The US is getting left behind as an innovator." *MIT Technology Review*. 23 January 2018. <https://www.technologyreview.com/2018/01/23/146065/america-may-be-getting-left-behind-as-an-innovator/>

A new ranking claims countries in Europe and Asia have nudged America off the leaderboard of the world's 10 most innovative nations. The findings: Every year, Bloomberg scores countries on metrics relating to innovation—**R&D activity, patents, productivity, and so on**. This year, South Korea and Sweden came first and second (same as last year). Singapore was third, up from sixth in 2017. **And America is 11th—outside the top 10 for the first time.** American weaknesses: Sure, the US invests heavily in R&D. But Bloomberg argues that it's struggling to produce enough science and engineering graduates, and is adding less value through manufacturing than it has in the past. Hence the fall. Broader concerns: America is being left behind on other research metrics as well, like how many academic papers it publishes. Maria Zuber, vice president for research at MIT, said such news raises "concerns about impacts on [America's] economy and workforce."

The information technology sector is important to the health of the economy

Henry-Nicki, Makada et al. "Trends in the Information Technology Sector." *The Brookings Institute*. 29 March 2019. <https://www.brookings.edu/research/trends-in-the-information-technology-sector/>

Digital technologies have risen to prominence as a critical determinant of economic growth, national security, and international competitiveness. The digital economy has a profound influence on the world's trajectory and the societal well-being of ordinary citizens. It affects everything from resource allocation to income distribution and growth. But how do we measure the digital economy and its contributions to growth and pertinent social indicators? Watanabe (2016), Brynjolfsson (2018), Nakamura (2018), Moulton (2018), and many other experts acknowledge the difficulty of precisely evaluating a digital economy characterized by rapidly changing products and services. Researchers estimate that "the digital economy is worth \$11.5 trillion globally, equivalent to 15.5 percent of global GDP and has grown two and a half times faster than global GDP over the past 15 years." [2] For its part, the Bureau of Economic Analysis (BEA) attributes the challenges of measuring the digital economy to a lack of consensus around activities included in the definition and the rapid pace at which the underlying nature of digital technologies evolves. The BEA estimates that **the U.S. digital economy grew at an annual average rate of 5.6 percent between 2006 and 2016 and "accounted for 6.5 percent of current-dollar GDP."** [3] National statistical accounting challenges notwithstanding, tracking the digital economy's growth trajectory is essential because it serves as an integral forward-looking barometer of U.S. economic growth and international competitiveness. Conceptually, the digital economy comprises goods and services that either were produced using digital technologies or include these technologies. The information and communications technology (ICT) industry stands at the center of much of this activity, underpinning the digital economy and serving as a reliable yardstick of its performance. Niebel (2018) confirms the link between ICT industry investments and economic growth, finding that between 1995 and 2010, **"ICT contribute[d] substantially to economic growth" for developed, developing, and emerging countries.** [4] **In the digital era, innovation, entrepreneurial dynamism, and information and ICT production will drive America's competitive edge.**

The ICT industry and ICT-enabled industries make important contributions to economic growth. This paper attempts to value those contributions and benchmark the importance of the ICT sector in the U.S. economy by assessing its contributions to economic growth, job creation. The sector's downstream contributions to the small business ecosystem and investments in reskilling and upskilling initiatives are examined. Finally, systemic challenges related to data privacy, trade, and immigration facing the sector are reviewed.

Political tides are influencing the ICT industry with regard to data protection and broader concerns. In terms of regulations, escalating trade tariff frictions between the U.S. and China concerning trade imbalances have deflected attention from the silent rise of regional data protectionist policies. In 2018, China, India, and Vietnam introduced data protectionist legislation to circumscribe cross-border data flow. These sovereign governments have pointed to data protection as paramount in mandating local storage of consumer data. **Regardless of the motivating factors, such restrictions limit the free flow of data across international borders with important consequences**

for the IT industry. Potential outcomes include increased compliance risks, growing infrastructure costs to maintain fractionalized enterprise data storage systems, and a corresponding rise in investments to navigate transient compliance requirements. Digital privacy protection is of critical importance in a vibrant digital society that respects consumers' rights to control access to their data and balances safeguards within an ecosystem that supports innovation and growth. However, the pace of massive data breaches has eclipsed regulators' ability to constrain these events and improve institutional accountability. The lack of a cogent national regulatory framework to address data privacy challenges emerging from massive amounts of business and consumer-related data, coupled with shifts in individuals' privacy preferences, presents inherent threats to the IT industry. Operational planning is particularly at risk. The absence of clear, consistent signals from federal authorities on the future of data privacy regulation in the U.S. could be costly for the IT industry, along with non-IT stakeholders. Nevertheless, two regulatory models provide insight into future directions for an eventual U.S. policy on digital privacy.

SOFT POWER / INTERNATIONAL RELATIONS

What's the argument?

Following the Snowden leaks in 2013, many experts argue that President Obama's negotiating leverage and soft power were undermined by the embarrassing revelations regarding NSA surveillance (Quinn). Perhaps even more concerning, other countries such as China, Russia, Iran, and Pakistan view NSA surveillance as an erosion of the moral high ground the US often relies upon when pressuring them into taking certain actions. The surveillance also erodes trust within our relationships with key allies such as France and Germany (Kehl).

The decrease in global confidence has tangible impacts beyond the somewhat nebulous sphere of international relations. Countries distrust in the government translates over to corporations, resulting in the boycott of US technology. Following the Snowden leaks, Cisco reported a 12 percent slump in sales - just one example of the major financial damage suffered by the US economy (Timm). More broadly, international relations experts contend that soft power is more critical than hard power in eliciting concessions and, thus, any hindrance could have disastrous consequences (Nye). Emerging from the Trump administration, soft power has already suffered, as the US was recently ranked 23rd globally in terms of trustworthiness (Handley).

Why does the argument matter?

Soft power, in the modern era, is how the US navigates the vast majority of our international interests. As countries become more militaristically advanced and intertwined within each other, hard power's influence decreases. Thus, the power of negotiation and diplomacy proves most important in creating impactful, long lasting global change. Continuing to hurt US soft power will eventually translate to a decrease in hegemony, hindering our ability to alter other countries behaviors, and emboldening our adversaries. A program like NSA surveillance, which undermines our credibility significantly, could damage our ability to elicit favorable agreements from both allies and adversaries.

Main Players

Foreign adversaries, US diplomats, foreign allies

Strategy Considerations

Soft power arguments are notoriously difficult to impact, despite our intuitive understanding of their importance. For that reason, teams must have a bulletproof understanding of each individual link to get to their impact and be able to explain the link chain clearly to the judge. This type of argument is won on the strength of the links, not necessarily the magnitude of the impact. However, teams should not shy away from running soft power as, when done correctly, this argument is convincing, important, and true - a rare combination. If teams are looking for a more quantified impact, economic loss due to distrust is the way to go.

Evidence for Soft Power / International Relations

The NSA taints the US' image on a global scale

Quinn, Adam. "Obama's Soft Power a Hard Sell after NSA Revelations." *The Conversation*. 28 October 2013. <https://theconversation.com/obamas-soft-power-a-hard-sell-after-nsa-revelations-19572>

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. Obama's day-to-day foreign policy struggles should not be simplistically taken as signs of collapsing American influence. But if the long-term plan is to carefully manage relative decline so as to preserves maximum influence, episodes such as those his country has faced since August do nothing to boost the prospects of success.

NSA surveillance encourages other countries to follow suit, erodes US credibility, and decreases our soft power

Kehl, Danielle. "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity." *Open Technology Institute*. July 2014. https://static.newamerica.org/attachments/534-surveillance-costs-the-nas-impact-on-the-economy-internet-freedom-cybersecurity/Surveillance_Costs_Final.pdf

The effects of the NSA disclosures on the Internet Freedom agenda go beyond the realm of Internet governance. The loss of the United States as a model on Internet Freedom issues has made it harder for local civil society groups around the world—including the groups that the State Department's Internet Freedom programs typically support²⁰³—to advocate for Internet Freedom within their own governments.²⁰⁴ The Committee to Protect Journalists, for example, reports that in Pakistan, "where freedom of expression is largely perceived as a Western notion, the Snowden revelations have had a damaging effect. The deeply polarized narrative has become starker as the corridors of power push back on attempts to curb government surveillance."²⁰⁵ For some of these groups, in fact, even the appearance of collaboration with or support from the U.S. government can

diminish credibility, making it harder for them to achieve local goals that align with U.S. foreign policy interests.²⁰⁶ The gap in trust is particularly significant for individuals and organizations that receive funding from the U.S. government for free expression activities or circumvention tools. Technology supported by or exported from the United States is, in some cases, inherently suspect due to the revelations about the NSA's surveillance dragnet and the agency's attempts to covertly influence product development. Moreover, revelations of what the NSA has been doing in the past decade are eroding the moral high ground that the United States has often relied upon when putting public pressure on authoritarian countries like China, Russia, and Iran to change their behavior. In 2014, Reporters Without Borders added the United States to its "Enemies of the Internet" list for the first time, explicitly linking the inclusion to NSA surveillance. "The main player in [the United States'] vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden's revelations, has come to symbolize the abuses by the world's intelligence agencies," noted the 2014 report.²⁰⁷ The damaged perception of the United States²⁰⁸ as a leader on Internet Freedom and its diminished ability to legitimately criticize other countries for censorship and surveillance opens the door for foreign leaders to justify—and even expand—their own efforts.²⁰⁹ For example, the Egyptian government recently announced plans to monitor social media for potential terrorist activity, prompting backlash from a number of advocates for free expression and privacy.²¹⁰ When a spokesman for the Egyptian Interior Ministry, Abdel Fatah Uthman, appeared on television to explain the policy, one justification that he offered in response to privacy concerns was that "the US listens in to phone calls, and supervises anyone who could threaten its national security."²¹¹ This type of rhetoric makes it difficult for the U.S. to effectively criticize such a policy. Similarly, India's comparatively mild response to allegations of NSA surveillance have been seen by some critics "as a reflection of India's own aspirations in the world of surveillance," a further indication that U.S. spying may now make it easier for foreign governments to quietly defend their own behavior.²¹² It is even more difficult for the United States to credibly indict Chinese hackers for breaking into U.S. government and commercial targets without fear of retribution in light of the NSA revelations.²¹³ These challenges reflect an overall decline in U.S. soft power on free expression issues. Broader Foreign Policy Costs Beyond Internet Freedom, the NSA discloses "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 to 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.

Surveillance hurts the US economy

Timm, Trevor. "How NSA Mass Surveillance is Hurting the US Economy." *EFF*. 25 November 2013. <https://www.eff.org/deeplinks/2013/11/how-nsa-mass-surveillance-hurting-us-economy>

Privacy may not be the only casualty of the National Security Agency's massive surveillance program. Major sectors of the US economy are reporting financial damage as the recent revelations shake consumer confidence and US trade partners distance themselves from companies that may have been compromised by the NSA or, worse, are secretly collaborating with the spy agency. Member of Congress, especially those who champion America's competitiveness in the global marketplace, should take note and rein in the NSA now if they want to stem the damage. In September, analysts at Cisco Systems reported that the fallout "reached another level," when the National Institute of Standards and Technology (NIST) told companies not to use cryptographic standards that may have been undermined by the NSA's BULLRUN program. The Cisco analysts said that if cryptography was compromised "it would be a critical blow to trust required across the Internet and the security community." This forecast was proven true in mid-November, when Cisco reported a 12 percent slump in its sales in the developing world due to the NSA revelations. As the Financial Times reported, new orders fell by 25 percent in Brazil and 30 percent in Russia and Cisco predicts its overall sales could drop by as much 10 percent this quarter. Cisco executives were quoted saying the NSA's activities have created "a level of uncertainty or concern" that will have a deleterious impact on a wide-range of tech companies ... Many commentators have been warning about the economic ramifications for months. Princeton technologist Ed Felten, who previously at the Federal Trade Commission, best explained why the NSA revelations could end up hurting US businesses: "This is going to put US companies at a competitive disadvantage, because people will believe that U.S. companies lack the ability to protect their customers—and people will suspect that U.S. companies may feel compelled to lie to their customers about security." The fallout may worsen. One study released shortly after the first Edward Snowden leaks said the economy would lose \$22 to \$35 billion in the next three years. Another study by Forrester said the \$35 billion estimate was too low and pegged the real loss figure around \$180 billion for the US tech industry by 2016. Much of the economic problem stems from the US government's view that it's open season when it comes to spying on non-U.S. persons. As Mark Zuckerberg said in September, the government's position is "don't worry, we're not spying on any Americans. Wonderful, that's really helpful for companies trying to work with people around the world."

Soft power is more influential than hard power and very important in fostering and maintaining relationships

Nye, Joseph S. Jr. "Soft Power." *Foreign Policy*. Autumn 1990.

<http://www.jstor.com/stable/1148580>

These trends suggest a second, more attractive way of exercising power than traditional means. A state may achieve the outcomes it prefers in world politics because other states want to follow it or have agreed to a situation that produces such effects. In this sense, it is just as important to set the agenda and structure the situations in world politics as to get others to change in particular cases. This second aspect of power—which occurs when one country gets other countries to want what it wants—might be called co-optive or soft power in contrast with the hard or command power of ordering others to do what it wants. Parents of teenagers have long known that they have shaped their child's beliefs and preferences, their power will be greater and enduring than if they rely only on active control. Similarly, political leaders and philosophers have long understood the power of attractive ideas or the ability to set the political agenda and determine the framework of decision in a way that shapes others' preferences ability to affect what other countries want to be associated with intangible power resources such as culture, ideology, and institutions.

Soft co-optive power is just as important as hard command power. If a state can make its power seem legitimate in the eyes of others, it will encounter less resistance to its wishes. If its culture and ideology are attractive, others will more willingly follow. If it can establish international norms consistent with its society, it is less likely to have to change. If it can support institutions that make other states wish to channel or limit their activities in ways the dominant state prefers, it may be spared the costly exercise of coercive or hard power. In general, power is becoming less transferable, less coercive, and less tangible. Modern trends and changes in political issues are having significant effects on the nature of power and the resources that produce it. Co-optive power—getting others to want what you want—and soft power resources—cultural attraction, ideology, and international institutions—are not new. In the early postwar period, the Soviet Union profited greatly from such soft resources as communist ideology, the myth of inevitability, and transnational communist institutions. Various trends today are making co-optive behavior and soft power resources relatively more important. Given the changes in world politics, the use of power is becoming less coercive, at least among the major states. The current instruments of power range from diplomatic notes through economic threats to military coercion.

In earlier periods, the costs of such coercion were relatively low. Force was acceptable and economies were less interdependent. Early in this century, the United States sent marines and customs agents to collect debts in some Caribbean countries; but under current conditions, the direct use of American troops against small countries like Nicaragua carries greater costs. Manipulation of interdependence under current conditions is also more costly. Economic interdependence usually carries benefits both directions; and threats to disrupt a relationship, if carried out, can be very expensive. For example, Japan might want to

US soft power is already on the decline

Handley, Lucy. "The US is the world's top 'soft' power – but Trump has damaged its reputation, survey says." *CNBC*. 25 February 2020. <https://www.cnn.com/2020/02/25/the-us-is-the-worlds-top-soft-power-but-trump-has-damaged-its-reputation.html>

The U.S. is seen as a global force in terms of its "soft power" and influence, despite controversy around President Trump's administration, which has damaged the country's reputation, according to new research. The Global Soft Power Index, by consultancy Brand Finance, surveyed more than 50,000 consumers in 87 countries to rank countries in terms of their familiarity, reputation and influence, among other measures. The U.S. came in top, with Germany, the U.K., Japan and China following. France, Canada, Switzerland, Sweden and Russia make up the rest of the top 10. The term "soft power"

was coined by political scientist Joseph Nye in the late 1980s and relates to a nation's ability to attract or persuade other nations, rather than coerce using military or economic means. But while the U.S. was ranked highly by respondents in terms of its influence in entertainment, media, sport and science, its reputation, governance and political stability are seen less positively by people around the world. "The mixed international reception of controversies surrounding President Trump's administration is likely to be the reason behind relatively low ratings for reputation," the report authors noted. The U.S. came 13th for reputation, 13th for ethical standards, 19th for political standards and 44th for relations with other countries. People also ranked it low for climate action (28th) and

trustworthiness (23rd), according to the study, published Tuesday. "This is perhaps understandable given America's decisions to unilaterally pull out of the Paris Agreement on climate change and the Joint Comprehensive Plan of Action on Iranian nuclear policy, undermining the nation's reliability as a partner on the world stage," the report stated. Trump's

impeachment trial also had an impact, according to David Haigh, chair and CEO of Brand Finance, but other measures helped it to the top spot. "Soft power cannot be rapidly achieved, nor lost. The United States has shown that ultimately, despite the reputational challenges of impeachment and unpredictable foreign policy, its position as the rule-maker in the international system ... is unrivalled," Haigh said in a release. A spokesperson for the White House was not immediately available for comment when contacted by CNBC. Like the U.S., China and Russia rank higher for influence than for reputation. China is ranked as the world's second-most influential country but comes in at 24th for reputation. Russia ranks 7th for influence and 26th for reputation. "China and Russia are the

nexus of change for global political, economic, and social world order. Western democracies can no longer rely on the end-of-history assumption that liberal values have won globally and have to adapt to a world shared with these new colossal soft power players," the report states. Despite leaving the European Union, the U.K.'s reputation appears undented, due in part to the importance of Queen Elizabeth II, its standing in media (which the report attributes to the BBC's reputation) and culture. Peter Fisk,

professor of leadership and strategy at Madrid's IE Business School, said that soft power is likely to continue to have an impact on nations, describing it as "meta power." "Meta power is not about having the largest army, it is about having the best story," he stated in the report.

HUMAN RIGHTS / PRIVACY

What's the argument?

Opponents of NSA surveillance often argue that it is inherently immoral and/or in violation of human rights standards. Historically, this argument has been legally substantiated, with several court cases condemning the NSA and FBI for violating the US Constitution's guarantee of privacy (Goitein; OC Register). This is due to the fact that the Patriot Act, one of the most expansive pieces of legislation in terms of giving the government the authority to surveil Americans, only legalized the obtaining of records that are relevant to an authorized investigation. Instead, the NSA surveilled nearly every American (Goitein). Opponents of this surveillance argue that technological advancements since the writing of the Fourth Amendment have created a grey area that the NSA has exploited to violate the rights of Americans (OC Register).

Human rights advocates argue that privacy is inherently a human right, and that it should generally be thought of as the 'right to be left alone' (Grant). Thus, a violation of privacy committed by the NSA is a human rights violation on the part of the United States government. Further, human rights standards such as the Necessary and Proportionate Principles, which is specifically designed for regulating online communications surveillance, are in direct conflict with the tactics used by the NSA. Specifically, the program of mass surveillance lacks due process, as there is no opportunity for a public hearing, and the program applies less favorable standards to foreign persons than US citizens, another indiscretion (Greene and Rodriguez).

Why does the argument matter?

Generally speaking, the federal government should work to uphold human rights standards both globally and domestically. Destroying individual privacy dehumanizes people by relinquishing their individual agency and autonomy. A failure to protect these rights is in violation of the social contract - a political theory pioneered during the Age of Enlightenment which contends that individuals give up some freedom in order to maintain the common good. If a government revokes those freedoms without upholding the common good, theorists such as Hobbes, Locke, and Rousseau contend, citizens can withdraw their obligation to obey. Thus, it is in everyone's best interest to maintain the social contract.

There are also significant legitimacy concerns when the United States, supposedly the role model for human rights initiatives around the globe, is spying on its own citizens similar to China, Russia, and North Korea. This questions the legitimacy of the government and the constitution in addition to violating the innate human rights of the whole population.

Main Players

Human rights advocates, US government, marginalized communities

Strategy Considerations

In the real world, this is the most commonly made argument in favor of ending surveillance: it is a violation of individuals' natural and constitutional right to privacy. For this reason, there is an abundance of literature to read and analysis to make in favor of the philosophical argument of what rights humans are entitled to and which sacrifices we ought to make in favor of the common good. This argument lends itself to deep, philosophical weighing, which for some teams could be both enjoyable and fruitful. Philosophically speaking, the right to privacy and autonomy is often seen as a fundamental prerequisite to other rights like speech, religion, press etc. The removal of autonomy also creates a slippery slope that can allow the government to remove other quintessential rights to effectively destroy individuality. Is the promise of future safety really worth the basis of freedom itself? However, while these arguments are interesting, the impacts to this argument will be difficult to terminalize and quantify.

Evidence for Human Rights / Privacy

Violates Fourth Amendment

FBI searches of the database were ruled unconstitutional

Goitein, Elizabeth. "How the FBI Violated the Privacy Rights of Tens of Thousands of Americans." *Brennan Center*. 22 October 2019. <https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans>

Earlier this month, the Office of the Director of National Intelligence released three redacted opinions of the Foreign Intelligence Surveillance Court (also known as the FISA Court) and the FISA Court of Review (FISCR). In the first opinion, the FISA Court held that the FBI's procedures for accessing Americans' communications that are "incidentally" collected under Section 702 of FISA violated both the statute and the Fourth Amendment. The government appealed, and in the second opinion, the FISCR upheld the FISA Court's decision. The FBI was forced to revise its procedures to conform with the court's ruling, and in the third opinion, the court approved the revised procedures. The government will no doubt try to sell this as an oversight success story. After all, the Department of Justice's audits had detected instances of FBI non-compliance with legal requirements, and the Department reported those instances to the FISA Court. The court solicited the assistance of amici and adopted their position in significant part. It ordered remedies that the FBI is now required to implement. And all of this became public because Congress in 2015 required the disclosure of significant FISA Court opinions. The system worked, right? I see a very different story. This is now the fourth major FISA Court opinion on Section 702 in 10 years documenting substantial non-compliance with the rules meant to protect Americans' privacy. The opinion, moreover, reveals that the FBI is conducting literally millions of backdoor searches — including so-called "batch queries" that rest on the same discredited legal theory used to justify the NSA's bulk collection of Americans' phone records. Despite the enormous implications for Americans' privacy and the government's dismal record, the remedy suggested by amici and imposed by the court was just more record-keeping. And the government sat on the opinion for a year, hoping for an appellate victory that would help mitigate the PR damage from disclosure. To put the court's recent opinions in context, some background is necessary. Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), passed in 2008, the National Security Agency (NSA), operating inside the United States, is authorized to collect communications of foreigners overseas for foreign intelligence purposes. No warrant is required for this collection because courts have held that foreigners have no Fourth Amendment rights. Instead, each year, the FISA Court must sign off on the procedures that govern the surveillance. Although ostensibly targeted at foreigners, Section 702 surveillance inevitably sweeps in massive amounts of Americans' communications. Recognizing the impact on Americans' privacy, Congress required the NSA to "minimize" the sharing, retention, and use of this "incidentally" collected U.S. person data. But the government and the FISA Court have embraced an interpretation of "minimize" that is remarkably... maximal. The NSA shares raw data with multiple other agencies — including the FBI and the CIA — and all of them retain the data for a functional minimum of five years. Moreover, the FBI routinely combs through it looking for Americans' communications to use in purely domestic cases, even in situations where the FBI lacks a factual predicate to open a full investigation. In 2011, the government disclosed to the FISA Court that it had misrepresented the nature of its "upstream" collection activities under Section 702. ("Upstream" collection takes place as the communications are transiting over the Internet backbone; "downstream" collection acquires stored communications, usually from the servers of Internet Service Providers.) When conducting upstream surveillance, the government was acquiring, not just communications to or from the targets of surveillance, but communications that simply mentioned certain information about them (known as "abouts" collection). As a result, the government was acquiring packets of data containing multiple communications, some of which had nothing to do with the target. This included tens of thousands of wholly domestic communications. The court was not pleased to learn about this significant issue three years into the program's operation. It held that the government's handling of the data violated the Fourth Amendment, and it required the government to develop special rules — approved by the court in 2012 — for segregating, storing, retaining, and accessing communications obtained through "upstream" collection. In 2015, the court was under the impression that these rules were being followed. However, in approving Section 702 surveillance that year, it noted several incidents of non-compliance with other rules designed to protect Americans' privacy — including FBI violations of protections for attorney-client communications, a "failure of access controls" by the FBI, and the NSA's failure to purge certain improperly collected data. Once again, the court expressed displeasure at being notified of infractions long after they occurred. In 2016, the FISA Court learned that the NSA had been violating the rules established in 2012. Because those rules were designed to remedy a Fourth Amendment violation occurring since the start of the program, the NSA's non-compliance meant that its upstream collection activities had been operating unconstitutionally for eight years. Moreover, the government did not report this issue for several months after discovering it. Unable to bring itself into compliance, the NSA made the only decision it could: In the spring of 2017, it abandoned "abouts" collection, which was at the root of the problem. When Section 702 came up for reauthorization in late 2017, civil liberties advocates pointed

to this troubled history. They also pointed to a growing body of case law holding that searches of government databases can, in certain circumstances, constitute a separate Fourth Amendment event. They argued that government agencies should be required to obtain a warrant before searching Section 702-obtained data for the communications of Americans (a practice formally called “U.S. person queries” and informally dubbed “backdoor searches”). They also urged Congress to ban “abouts” collection, lest the government attempt to resume it. Congress rejected these proposals. Although Congress did require the FBI to obtain the FISA Court’s permission to conduct U.S. person queries in a tiny sliver of cases, it blessed the vast majority of these searches, which previously had no foundation in the text of Section 702. It simply required the FBI to develop “querying procedures” that the FISA Court would have to approve. It also required the FBI to keep records of each U.S. person query it conducted. With respect to “abouts” collection, Congress required the government to obtain FISA Court approval and to give Congress advance notice before resuming the practice. In March 2018, the government submitted its annual certifications and procedures to the FISA Court for its approval. In a decision dated October 18, 2018, and released last week, the FISA Court held that the FBI’s minimization procedures violated both the statute and the Fourth Amendment. The court’s opinion addresses three main practices by the FBI: downstream collection of certain communications; the FBI’s failure to record USP queries; and the FBI’s improper use of USP queries. Downstream collection and “abouts” communications. Although this section of the opinion is highly redacted, it appears that the government is engaged in a new form of downstream collection that raised a flag for the FISA Court. The court solicited amici’s advice about whether the statutory preconditions for resuming “abouts” collection apply to downstream collection, and whether certain activities in the government’s 2018 certifications involve the acquisition of “abouts” communications. Amici argued that the answer to both questions was yes; the government’s answer was no in both cases. The court split the baby, holding that the statutory requirements apply to any kind of “abouts” collection, but that no such collection would occur under the government’s certifications. The heavy redactions make it difficult to assess the significance of this part of the opinion. However, on its face, the definition of “abouts” collection – basically, anything other than a communication to or from the target – should not be difficult to apply. It is worrisome that the government and amici reached different conclusions about whether a certain form of collection merited the label “abouts.” The uncertainty strongly supports a suspicion civil liberties advocates have held for some time: that the selectors the government uses to identify the communications to be collected are not necessarily unique identifiers (such as email addresses), but can sweep in people other than the intended targets (as would, for instance, IP addresses). The statutory requirement to count U.S. person queries. In its January 2018 reauthorization of Section 702, Congress ordered the government to adopt querying procedures that included “a technical procedure whereby a record is kept of each United States person query term used for a query.” Instead, in the querying procedures that the FBI submitted to the FISA Court, the Bureau announced that it “intends to satisfy the record-keeping requirement by keeping a record of all queries” – in other words, the FBI would lump together U.S. person queries and non-U.S. person queries, without distinguishing between them. The government defended this approach with a weak argument that the statutory text was somehow ambiguous, and that both the legislative history and policy considerations weighed against requiring the FBI to document U.S. person queries. In a refrain often heard when an intelligence or law enforcement agency is asked to devote time or resources to safeguarding civil liberties, the government claimed that requiring the FBI to figure out whether a particular investigative subject was a U.S. person would “divert resources from investigative work . . . to the detriment of public safety.” The FISA Court has historically yielded to such pleas, and on this occasion, the court seemed sympathetic. Ultimately, however, the court concluded that it had no choice. It stated: “Regardless of how persuasive the FBI’s considerations may be, the court is not free to substitute its understanding of sound policy – or, for that matter, the understanding of the Director of the FBI – for the clear command of the statute.” The law, the court held, was unambiguous in its directive to count U.S. person queries. On appeal, the FISCRC upheld the court’s ruling on this question. The FISCRC, however, seemed somewhat less sympathetic to the government’s position. Under the FBI’s querying procedures, “U.S. person query term” is defined as “a term that is reasonably likely to identify one or more specific United States persons.” This definition does not require a high level of certainty. Moreover, the procedures provide for the application of default assumptions in cases where specific information is lacking. Under these circumstances, it is hard to argue with the FISCRC’s assessment that counting U.S. person queries is not “a burdensome substantive requirement,” and that it would simply mean “adding one (largely ministerial) item to the checklist that FBI personnel most likely already work through when conducting queries for investigative purposes.” Somewhat oddly, the FISCRC did not resolve the other major issue on appeal: whether the FBI’s repeated violations of its own querying and minimization procedures rendered those rules unlawful and unconstitutional as implemented. Those violations, and the FISA Court’s failure to require an adequate remedy for them, will be the subject of Part II of this post. Improper queries of Section 702 communications. The most eye-opening part of the October 2018 opinion is the section addressing the “large number” of queries undertaken by the FBI since April 2017 that did not comply with internal rules, the statute, or the Fourth Amendment. To begin, the opinion provides the first glimpse of just how prevalent the FBI’s U.S. person queries really are. In the past, the FBI has claimed it has no way even to estimate this number. It was nonetheless clear that the number was significant, as the Privacy and Civil Liberties Oversight Board (PCLOB) reported that the FBI runs queries of databases containing Section 702 data at the earliest stage of every assessment or investigation. The court’s October 2018 opinion reveals that the FBI in 2017 conducted 3.1 million queries on one system alone. This number encompasses U.S. person and non-U.S. person queries alike, but as the court observed: “[G]iven the FBI’s domestic focus it seems likely that a significant percentage of its queries involve U.S.-person query terms.” Almost certainly, then, the total number of U.S. person queries run by the FBI each year is well into the millions. In theory, the FBI’s procedures are supposed to limit these searches. The key limitation, as set forth in the querying procedures, is as follows: “Each query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures.” This requirement essentially mirrors the one previously contained in the FBI’s minimization procedures. The FISA Court once again held, as it has in the past, that this limitation, “as written,” satisfies both the statute and the Fourth Amendment. But that didn’t end the court’s analysis. The court went on: “FISC review of minimization procedures under Section 702 is not confined to the procedures as written; rather, the court also examines how the procedures have been and will be implemented.” The court then noted that, “[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime.” These included multiple one-off incidents of FBI personnel running U.S. person queries accidentally or for improper personal purposes. (In a frank statement that reveals why limits on access are a poor substitute for adequate limits on collection, the FISA Court commented that it was less concerned about personal misuses of the data, because “[i]t would be difficult to completely prevent personnel from querying data

for personal reasons.”) They also included several incidents indicative of more systemic problems, including: In March 2017, the FBI, against the advice of the FBI’s Office of General Counsel, conducted queries using 70,000 identifiers “associated with” people who had access to FBI facilities and systems. On a single day in December 2017, the FBI conducted over 6,800 U.S. person queries using Social Security Numbers. Between December 7-11, 2017, an FBI official improperly reviewed raw FISA information resulting from 1,600 U.S. person queries. On more than one occasion, the FBI conducted dozens of U.S. person queries to gather information about potential informants. The government told the FISA Court that these errors stemmed from “fundamental misunderstandings by some FBI personnel [about] what the standard ‘reasonably likely to return foreign intelligence information’ means.” This is a remarkable admission, given that this standard has been in place for several years, and given the government’s repeated assurances to the FISA Court during this time that access to Americans’ data was restricted to personnel who were carefully trained in the applicable limits. The court expressed “serious concern” about “the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it.” It identified three factors that heightened its concern. First, it cited limitations on existing oversight mechanisms. It noted that some FBI offices field offices go for periods of two years or more between oversight visits, and ultimately, Justice Department overseers “review only a small portion of the queries conducted.” It also observed that “the documentation available to [overseers] lacks basic information that would assist in identifying problematic queries.” Given these limitations, the court wrote, “it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the court.” Second, the court — for the first time — acknowledged the tension between the substantive limits on queries contained in the FBI’s procedures, and the Bureau’s vigorous encouragement to its personnel to run queries early and often. Indeed, an FBI official submitted a declaration to the court stating that “FBI encourages its personnel to make maximal use of queries — provided they are compliant with the FBI’s minimization procedures” FBI officials are thus simultaneously told to maximize and minimize their access to U.S. person information. In the court’s words: “On the one hand, the FBI is obligated to query Section 702 and other FISA information only in circumstances satisfying a querying standard that does not apply to FBI information generally. On the other hand, it has set up its systems to facilitate running the same query simultaneously across FISA and non-FISA datasets . . . and encourages personnel to make maximal use of such queries, even at the earliest investigative stages. Those policy decisions may well help FBI personnel work efficiently and ‘connect dots’ to protect national security . . . but they also create an environment in which unduly lax applications of the Section 702 querying standards are more likely to occur.” Third, the court discussed the FBI’s use of “batch queries” — perhaps the most explosive revelation in the opinion. The FBI’s querying procedures require that “[e]ach query” must be reasonably likely to retrieve foreign intelligence information or evidence of a crime. The government, however, has taken the position that “an aggregation of individual queries” — also referred to as a “batch query” — “can satisfy the querying standard, even if each individual query in isolation would not be reasonably likely to return foreign-intelligence information or evidence of a crime.” So, for instance, if the FBI has information that an employee at a particular company is planning illegal actions, but the FBI has no knowledge of who the employee is, the Bureau would be justified (the government argues) in running queries for every employee at that company. This is presumably the theory on which the FBI ran the massive numbers of queries described above (e.g., 70,000 queries on individuals with access to FBI systems and facilities). If this sounds familiar, it should. This is the same rationale the NSA used to justify “bulk collection” of Americans’ telephone records. Even though the applicable statute, Section 215 of the

Patriot Act, allowed the government to obtain records only if they were “relevant” to an authorized investigation, the FISA Court allowed the NSA to collect the phone records of nearly every American — most of which were, of course, entirely irrelevant to any investigation — on the ground that some relevant records were likely buried within them. When this practice was made public as a result of Edward Snowden’s disclosures, it was

unable to withstand either judicial review (the Second Circuit Court of Appeals held that it violated the statute) or the judgment of Congress (which changed the law in 2015 with the goal of prohibiting bulk collection). As the NSA’s bulk collection program illustrates, there is no logical limit to how many queries the FBI could aggregate based on the theory that the result will likely yield foreign intelligence or evidence of a crime. Indeed, the larger the number of individuals swept in, the more likely it is that the queries, in aggregate, will turn up results. It is a small step from “batch queries” to “bulk queries.” The court did not seem alarmed by the implications of the theory — it opined that “[p]erhaps in the abstract it would be reasonable for the FBI to run such an aggregated query” — but it nonetheless expressed skepticism that such an approach could be reconciled with the text of the FBI’s querying procedures, which require “[e]ach query” to be reasonably likely to return foreign intelligence information or evidence of a crime. Ultimately, the court held that the extent of improper querying rendered the FBI’s procedures, as implemented, inconsistent with Section 702’s “minimization” requirement. It also held that the FBI’s practices violated the Fourth Amendment’s reasonableness requirement. Although it found the government’s interest in acquiring foreign intelligence information to be “particularly intense,” it quoted a decision by the Foreign Intelligence Surveillance Court of Review (FISCR) stating that if “the protections that are in place for individual privacy interests are . . . insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.” The court concluded: “Here, there are demonstrated risks of serious error and abuse, and the court has found the government’s procedures do not sufficiently guard against that risk.” To cure these defects, the court recommended — and the FBI ultimately adopted, after the government’s unsuccessful appeal to the FISCR — a remedy proposed by amici. Specifically, any time the FBI runs a U.S. person query that returns Section 702 data, FBI personnel are not permitted to view the content (although they may still view non-content “metadata”) unless they first document the reasons why they believed the query was likely to return foreign intelligence or evidence of a crime. The court opined that this requirement would force FBI personnel to think more carefully about the applicable standard before running queries, and would assist oversight personnel in determining whether the standard was indeed being honored. The FISA Court identified serious problems with the government’s submissions, engaged amici to provide advice, considered and partly agreed with their arguments, held the government’s actions to be not only unlawful but unconstitutional, and adopted a remedy proposed by amici — all of which was made public, albeit with redactions. Taken in isolation, these facts might seem to tell a resounding success story for oversight of foreign intelligence surveillance. But such a conclusion would ignore many other salient facts. For one thing, the government sat on the FISA Court’s October 2018 opinion for almost a year, instead of promptly declassifying and releasing it as envisioned by Congress in the 2015 USA FREEDOM Act. Clearly, the government was

hoping for a win on appeal that would neutralize the negative impact on public opinion. Had the appeal taken several additional months to resolve, there is no doubt that we would still be in the dark about the FBI's activities today. As for the substance of the opinion, the illusion of accountability fades when one considers the many aspects of the court's own ruling that were left entirely unaddressed by its chosen remedy. The court's opinion cited the following major problems and sources of concern: FBI personnel are fundamentally confused about what "reasonably likely to return foreign intelligence or evidence of a crime" means. Oversight is limited because overseers review only a tiny fraction of queries. Oversight is limited because overseers lack documentation of the justification for queries. There is a mismatch between the FBI's querying procedures, which purport to place substantive limits on queries, and the FBI's policy of encouraging routine use of those queries at the earliest stage of every investigation. "Batch" queries are seemingly inconsistent with the text of the FBI's querying procedures. The remedy imposed by the court – a requirement that FBI personnel document their reasons for performing a U.S. person query before viewing content information – addresses only one of these problems (lack of documentation for overseers to review). After all, if FBI agents truly do not understand what "reasonably likely to return foreign intelligence or evidence of a crime" means, requiring them to document their misconceptions will not produce any greater understanding; it will merely reaffirm the confusion that the court already observed. In theory, the documentation could be used as a mechanism to identify personnel who require remedial training or even administrative discipline. But the court did not order any such measures, and the FBI's revised procedures don't contemplate them. In any case, it is clear from the court's opinion that the Justice Department would require expanded oversight capacity to detect non-compliance in anything more than a fraction of cases. The court did not direct the Justice Department to devote more resources to oversight, and so virtual piles of documentation recording FBI agents' various interpretations of the legal standard for queries will languish unexamined. Knowing this, FBI agents are unlikely to spend much time or thought on writing out their rationales. Nor does the court's remedy do anything about the mixed message the FBI sends its personnel by simultaneously limiting (in its querying and minimization procedures) and urging (in its policies and rhetoric) the use of queries. It was an important step forward for the court to recognize this fundamental disconnect in the FBI's practice. But the disconnect will continue unless and until the court orders the FBI to harmonize its policies and its rhetoric with its Section 702 procedures. The court also strongly suggested that "batch queries" are inconsistent with the text of the FBI's querying procedures. However, it did not order the FBI either to stop batch queries or to alter its procedures to allow them. The FBI's revised procedures, which the FISA Court approved in September 2019, still have the language that would seem to foreclose batch queries. But there is no indication, either in the procedures or in any other public document, that the FBI has stopped the practice; and the FISA Court apparently forgot to ask, as its September 2019 opinion does not even mention the issue. More to the point, the court should have barred "batch queries" outright. The FISA Court's finding that Section 702 surveillance is constitutionally reasonable has always hinged on a delicate balance between the government's interest in collecting foreign intelligence and Americans' privacy interests in their communications. The ostensible existence of strict limitations on government officials' access to Americans' communications – including the requirement that queries must be designed to return foreign intelligence or evidence of a crime – has been a key factor in the court's conclusion that the balance tips in the government's favor. Allowing the FBI to conduct tens of thousands of queries in a "batch," when it is apparent that the vast majority of them will not yield any such information or evidence, would require a significant repositioning of the scales. One final observation: The court's modest record-keeping remedy is particularly inadequate in light of the government's history of Section 702 violations. On four separate occasions, as recounted in Part I of this post, the FISA Court has found that the government was improperly handling or accessing Americans' communications. On three of those occasions, the court held or otherwise indicated that these actions violated the Fourth Amendment. Astonishingly, at no point in Section 702's existence has the government operated the program in full compliance with constitutional requirements. In light of this history, the court should have required changes far more substantial than (as the FISCR described it) "adding one (largely ministerial) item to the [FBI's] checklist." After a decade of trial and error, the FISA Court should have required FBI agents to obtain warrants before searching for Americans' communications. In my opinion, the court erred when it held that recent case law does not support a warrant requirement for U.S. person queries of Section 702 data. Nonetheless, even if a warrant requirement were not compelled by the case law, the court still could have concluded that warrants are necessary here. In light of the repeated failure of the government, over the course of more than a decade, to adhere to the procedural requirements that the court has held the Fourth Amendment does require, the court could easily have determined that nothing short of a warrant requirement will guard against the "risks of serious error and abuse" that have thus far rendered the government's practices unconstitutional. Now that would have been a triumph of foreign intelligence surveillance oversight.

NSA is inherently unconstitutional

Editorial Board. "Edward Snowden Was Right, the NSA Has Violated Our Rights." *OC Register*. 10 September 2020. <https://www.ocreger.com/2020/09/10/edward-snowden-was-right-the-nsa-has-violated-our-rights/>

Seven years after it was exposed by former National Security Agency contractor Edward Snowden, a federal appeals court has ruled that the NSA's bulk collection of phone metadata was illegal and unnecessary. Once again, Americans are reminded that government will too often trample over our rights in the name of security when it is neither just nor necessary to do so. A three-judge panel of the United States Court of Appeals for the 9th Circuit ruled on Sept. 2 that "the metadata collection exceeded the scope of Congress's authorization ... which required the government to make a showing of relevance to a particular authorized investigation before collecting the records ..." Further, the court concluded that "the government may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act ('FISA') when it collected the telephony metadata of millions of Americans." The case at hand involved appeals from four Somali immigrants who were convicted for "sending, or conspiring to send, \$10,900 to Somalia to support a foreign terrorist organization." Notably, the panel, having condemned the metadata collection program, affirmed the convictions, since lawful wiretaps gave the government more than enough information to go after the individuals. Evidence collected by way of the metadata program wasn't essential to the case. "Seven years ago, as the news declared I was being charged as a criminal for speaking the truth, I never imagined that I would live to see our courts condemn the NSA's activities as unlawful and in the same ruling credit me for exposing them," tweeted Edward Snowden in response to the ruling. "And yet that day has arrived." The ruling comes not long after President Trump mentioned he was considering pardoning Snowden. Snowden broke the law, sure, but he did so in the interests of revealing to the American people the extent to which government was willing to go to spy on them. He deserves a pardon. The NSA, Snowden revealed, was all too willing to stretch the limits of its authority and even the Constitution to collect sweeping amounts of information on Americans through a litany of programs. The Fourth Amendment is clear: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Just because technology has advanced considerably since the day those words were first written doesn't mean they don't hold true today. While Americans can all understand why government agencies would want broad access to electronic information, that doesn't mean government can or should be able to access it without constraints. Constraints on government power exist for a reason.

Infringement on human rights

Privacy is a human right

Grant, Susan. "Privacy is a Human Right – It Can't Be Bought or Sold." *Consumer Federation of America*. 17 December 2019. <https://consumerfed.org/privacy-is-a-human-right-it-cant-be-bought-or-sold/>

One of the arguments that some people make about privacy legislation is that individuals' personal information should be treated as their property. At first blush, this may seem like an appealing idea. Why shouldn't we be paid when companies use our data? But that's the wrong approach to privacy. Privacy is a human right. This concept is the foundation for the privacy regulation around the world. In their landmark 1890 Harvard Law Review article, Samuel D. Warren and Louis D. Brandeis discuss how the concept of privacy must be thought of broadly, beyond the narrow confines of property rights, as a "right to be left alone." In 1948, the United Nations issued the Universal Declaration of Human Rights which states, in Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. The European General Data Protection Regulation (GDPR) also recognizes privacy as a right to which every person is entitled. It begins with this observation: Whereas: (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. The GDPR goes on to describe specific rights of individuals to access, correct, port, and delete data about them, and to object to profiling using that data. None of this is predicated on the individuals' owning the data. It is based on their rights to the protection of their personal data. Many U.S. states enshrine the right to privacy in their constitutions. For instance, Article 1 Section 1 of the California state constitution says: All people are by nature

free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. While it's common to use phrases such as "your data" or "the consumer's data" in talking about privacy, this is not meant in the sense of the data being property owned by the individual. It's simply short-hand for data about the individual. What's wrong with the idea of treating data about individuals as their property? Property is a commodity that you can sell or even give away. Privacy is a human right, however, not a commodity.

Surveillance violates international human rights standards

Greene, David and Katitza Rodriguez. "Unnecessary and disproportionate: How the NSA violates international human rights standards." *Electronic Frontier Foundation*. 28 May 2014.

<https://www EFF.org/deeplinks/2014/05/unnecessary-and-disproportionate-how-nsa-violates-international-human-rights>

Even before Ed Snowden leaked his first document, human rights lawyers and activists were concerned about law enforcement and intelligence agencies spying on the digital world. One of the tools developed to tackle those concerns was the development of the International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles"). This set of principles was intended to guide governments in understanding how new surveillance technologies eat away at fundamental freedoms, and outlined how communications surveillance can be conducted consistent with human rights obligations. Furthermore, the Necessary and Proportionate Principles act as a resource for citizens—used to compare new tools of state surveillance to global expectations of privacy and due process. We are now able to look at how the NSA's mass surveillance programs, which we have learned about in the past year, fare when compared to the Necessary and Proportionate

Principles. As you might expect, the NSA programs do not fare well. To mark the first anniversary of the Snowden disclosures, we are releasing Unnecessary and Disproportionate, which details how some of the NSA spying operations violate both human rights standards and the Necessary and Proportionate Principles. Some of the conclusions are as follows: The NSA surveillance lacks "legality" in that NSA surveillance laws are largely governed by a body of secret law developed by a

secret court, the Foreign Intelligence Surveillance Court (FISC), which selectively publishes its legal interpretations of the law; The NSA surveillance is neither "necessary," nor "proportionate," in that the various programs in which communications data are obtained in bulk violate the privacy rights of millions of persons who are not suspected of having any connection to international terrorism; The NSA surveillance programs are not supported by competent judicial authority because the only judicial approval, if any, comes from the FISC, which operates outside of normal adversarial procedures such that the individuals whose data are collected lack access to the court; The NSA surveillance programs lack due process because the FISC presents no opportunity for a public hearing; The NSA surveillance programs lack user notification: those whose data is obtained do not know that their communications have been monitored and hence they cannot appeal the decision nor get legal representation to defend themselves; The NSA surveillance programs lack the required transparency and public oversight, because they operate in secret and rely on gag orders against the entities from whom the data are obtained, along with secret, if any, court proceedings; The NSA surveillance programs damage the integrity of communication systems by undermining security systems, such as encryption, requiring the insertion of surveillance back doors in communications technologies, including the installation of fiber optic splitters in transmission hubs; and The US surveillance framework is illegitimate because it applies less favorable standards to non-US persons than its own citizens; this discrimination places it in violation of the International Covenant on Civil and Political Rights (ICCPR).

More broadly, the United States justifies the lawfulness of its communications surveillance by reference to distinctions that, considering modern communications technology, are irrelevant to truly protecting privacy in a modern society. The US relies on the outmoded distinction between "content" and "metadata," falsely contending that the latter does not reveal private facts about an individual. The US also contends that the collection of data is not surveillance—it argues, contrary to both international law and the Principles, that an individual's privacy rights are not infringed as long as her communications data are not analyzed by a human being. It's clear that the practice of digital surveillance by the United States has overrun the bounds of human rights standards. What our paper hopes to show is exactly where the country has crossed the line, and how its own politicians and the international community might rein it back.

DEMOCRACY

What's the argument?

One of the most critical repercussions of NSA mass surveillance is the negative effect it has on free speech and democratic participation. Multiple studies discuss the theory known as the “chilling effect”, where surveillance grants power to the watcher over the watched and discourages free exercise of civil liberties (Richards). In other words, citizens are so worried that the government will flag and persecute their actions, they self-censor and choose not to speak their mind. Most applicably on this topic, citizens avoid researching and pursuing certain subjects that could amount to government suspicion. Furthermore, the existence of a surveillance state empirically stifles free expression and breeds fear and conformity (Greenwals). In fact, a recent study showed 28% of writers curtailed activities because of the presence of a surveillance state (Desai).

More generally speaking, surveillance erodes trust in government and democratic participation. Citizens forego participating in protests, fear collective action, and even disengage from voting out of fear of government repression. Even for individuals that are not concerned about a lack of privacy, government surveillance generally brings with it more intrusive government and less political freedom. This makes it difficult for dissent to flourish and democracy to remain healthy (Goold).

Finally, metadata removes the need for citizens to be civically engaged in the first place. The pooling of metadata allows polling services and politicians to predict how voters will respond to certain initiatives, eliminating the need for voluntary democratic participation (Howard). This creates a self-serving government that no longer requires the consent of the governed.

Why does the argument matter?

State surveillance jeopardizes the very existence of a healthy, thriving democracy. By stifling free expression, free speech, and dissent, surveillance decreases democratic participation and makes it easier for minoritarian entities to gain power and thrive.

Main players

The US government, US citizens

Strategy Considerations

While the links are some of the strongest on the topic, this argument is especially hard to quantify. Measuring the impact of decreasing or increasing democracy occurs indirectly through metrics such as income inequality or poverty. However, eroded democracy links into con arguments on the topic and can be used to downplay the impacts. Having a strong, democratic government is often a prerequisite for good policy change to occur. Furthermore, the alternative form of government that is more autocratic can magnify other pro arguments that deal with privacy and create problems for con arguments that seek to stop autocrats and terrorist organizations.

Evidence for Democracy

Surveillance creates a chilling effect on exercising civil liberties

Richards, Neil. "The Dangers of Surveillance." *Washington University of Law*. 25 March 2013.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412

At the level of theory, I will explain when surveillance is particularly dangerous, and when it is not. Surveillance is harmful because it can chill the exercise of our civil liberties, and because it gives the watcher power over the watched. In terms of civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about their political and social beliefs. Such intellectual surveillance is particularly dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy." Intellectual privacy is the idea that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing, and that a meaningful guarantee of privacy – protection from surveillance or interference – is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.

State surveillance stifles free expression through self-censorship

Greenwald, Glenn. "New Study Shows Mass Surveillance Breeds Meekness, Fear, and Self-Censorship." *The Intercept*. 28 April 2016. <https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/>

A NEWLY PUBLISHED study from Oxford's Jon Penney provides empirical evidence for a key argument long made by privacy advocates: that the mere existence of a surveillance state breeds fear and conformity and stifles free expression. Reporting on the study, the Washington Post this morning described this phenomenon: "If we think that authorities are watching our online actions, we might stop visiting certain websites or not say certain things just to avoid seeming suspicious." The new study documents how, in the wake of the 2013 Snowden revelations (of which 87 percent of Americans were aware), there was "a 20 percent decline in page views on Wikipedia articles related to terrorism, including those that mentioned 'al Qaeda,' 'car bomb' or 'Taliban.'" People were afraid to read [those] articles about those topics because of fear that doing so would bring them under a cloud of suspicion. The dangers of that dynamic were expressed well by Penney: "If people are spooked or deterred from learning about important policy matters like terrorism and national security, this is a real threat to proper democratic debate." As the Post explains, several other studies have also demonstrated how mass surveillance crushes free expression and free thought. A 2015 study examined Google search data and demonstrated that, post-Snowden, "users were less likely to search using search terms that they believed might get them in trouble with the U.S. government" and that these "results suggest that there is a chilling effect on search behavior from government surveillance on the internet." The fear that causes self-censorship is well beyond the realm of theory. Ample evidence demonstrates that it's real – and rational. A study from PEN America writers found that 1 in 6 writers had curbed their content out of fear of surveillance and showed that writers are "not only overwhelmingly worried about government surveillance, but are engaging in self-censorship as a result."

Surveillance changes behaviors to encourage compliance with the state: One study found 28% of writers curtailed activities because of the surveillance

Desai, Decen R. "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding." *Notre Dame Law Review*. 1 December 2014.

<https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4581&context=ndlr>

The nonprofit PEN America has shown that the government's ability to gather information directly or from third parties has chilled associational activities of writers.²⁵⁹ The study found that: • 28% have curtailed or avoided social media activities, and another 12% have seriously considered

doing so; • 24% have deliberately avoided certain topics in phone or email conversations, and another 9% have seriously considered it;

• 16% have avoided writing or speaking about a particular topic, and another 11% have seriously considered it; • 16% have refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious, and another 12% have seriously considered it; • 13% have taken extra steps to disguise or cover their digital footprints, and another 11% have seriously considered it; • 3% have declined opportunities to meet (in person, or electronically) people who might be deemed security threats by the government, and another 4% have seriously considered it.²⁶⁰ As scholars of association might say, with surveillance the room to disagree about what the common good is diminishes.²⁶¹ One way to think of the problem is as the need for anonymity. Christopher Slobogin has explained that perspective: "Anonymity in public promotes freedom of action and an open society. Lack of public anonymity promotes conformity and an oppressive society."²⁶² He calls this problem "public privacy."²⁶³ That seeming oxymoron captures the need to be public, yet private from government oversight. It is anonymity to the government that matters. That anonymity may be based on protections from direct surveillance or protections from the government accessing third party, private sector records of recent and past communications and acts.

Julie Cohen has shown why that is so.²⁶⁴ Surveillance changes behaviors, because "the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior."²⁶⁵

Instead of robust, diverse, and challenging ideas, we will favor the "the bland and the mainstream."²⁶⁶ We end up with a diminished "capacity to act and to decide," which leads to "the highest possible degree of compliance with [what the state determines is] the model . . . citizen."²⁶⁷ This problem is a type of chilling effect.²⁶⁸

Surveillance destroys privacy, trust in government, and democratic participation

Goold, Benjamin J. "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy." *Peter A. Allard School of Law University of British Columbia*. 2010. https://commons.allard.ubc.ca/fac_pubs/150/

This is a powerful argument in favor of privacy, and crucially it is one that may be easier to sell to the general public. One of the problems that has faced privacy advocates and civil libertarians interested in privacy is that it is often very difficult to explain to the public at large why they should care about their privacy or the privacy of others. Compared with easily understood anti-privacy slogans such as "nothing to hide, nothing to fear", appeals to the value of dignity and personal autonomy often fall on deaf ears. But arguments that privacy is essential if we are to be able to enjoy our basic political rights – and to be in a position to keep state actors honest and hold them to account – are

much easier to understand. According to this argument, we should resist the spread of surveillance not because we have something to hide, but because it is indicative of a worrying expansion in state power and makes dissent more difficult. While individuals might not be concerned about the loss of autonomy that comes from being subjected to more and more state scrutiny, it is unlikely that many would be comfortable with the suggestion that more surveillance inevitably brings with it more intrusive government and less political freedom. Furthermore, without privacy, it is much harder for dissent to flourish or for

democracy to remain healthy and robust, and as such there must be a limit placed on the ability of the state to know things about us or to subject us to surveillance.⁶¹ Finally, given that a democratic state can only be legitimate and thrive in an atmosphere of mutual trust between government and governed, it follows that any surveillance measure that threatens to erode or destroy that trust must be resisted, or at the very least its potential costs and benefits carefully considered. As anyone who has lived in a state where the rule of law is not taken for granted – and where there is little in the way of institutional trust – will be able to tell you, confidence in the institutions of government is hard won and easily lost.⁶³ For this reason, the presumption should be that any surveillance measure which is directed at the public at large – and which treats all citizens as potential threats or management challenges – has prima facie gone a step too far, and demands an extra-ordinary justification. According to this view, mass state surveillance should always be the exception and never the rule. In short, we will know when there is too much state surveillance when political rights and democratic participation are threatened, and it is at this point that the citizenry should demand that the state pulls back and accepts that there are times when it is better for the government to know less rather than more. Of course, some will say that we have already passed this point, that the current surveillance infrastructure already poses a serious threat to democracy and the rule of law.

Surveillance destroys the need for voluntary civil participation

Howard, Phillip. “Internet of Things World – Is the Internet of Things Your New Constitution?” *University of Oxford*. 11 September 2015.

https://www.imgigi.com/amp/Download_Documents_PDF_Free_amp2.php?Download_PDF_courses=870

The Internet of Things as a Mechanism of Political Participation The politics of the future will be guided by a new power paradigm. Whoever controls the largest device networks will get the most sensor data, and hence will manage the largest number of connections between and among people and devices. As more of the things we manufacture are powered and networked, “inanimate” objects will be replaced by devices that talk with our other devices. They will communicate with their original manufacturer, the information services we subscribe to, national security agencies, contractors, cloud computing services, and anyone else in the data stream. They will work the behavioral data they have assembled and with algorithms—the script of our new constitution—mete out capacities and constraints on our political lives. Subsequently, civic engagement will increasingly become involuntary. None of us will have the opportunity to opt-out of the behavioral data collection that generates public policy. The basis of a democracy is voluntary civic engagement. A person’s participation in setting government policy is intentional and a matter of choice. In democracies, citizens express their preference through activism and voting. Historically, governments and huge record-keeping projects like the census. Politicians have long tried to interpret citizen intent and manipulate it through rhetoric and campaign tricks. But pervasive device networks will change the rules, making voluntary conversations among elected politicians eager to interpret (and manipulate) citizen intent also relied on opinion polls, conversations with civic groups, social science research, a officials, political parties, lobbyists and civic groups less important than the plethora of near-perfect data generated by the objects around us. Activism and petition-signing will be overshadowed by volumes of behavioral information cleverly extracted from the Internet of Things.⁸ This information will be of incalculable value. It will inform firms of consumer habits, enlighten governments as to the needs of citizens, and reveal the whims of voters to politicians. Political lobbying isn’t a new sport, but the Internet of Things is going to be a game-changing resource for lobbyists. the more a lobbyist knows about the behavior of voters and donors, the easier it is to activate and organize those people on clients’ behalf. Furthermore, smart data mining will cost good money, which will place it out of the reach of many civic groups, scientists and journalists. Hence, society’s watchdogs [who] will not be able to

use this data to check on what big political players are doing with this megadata. It is also important to realize that governance systems don't just involve states: they appear whenever a powerful actor can set some rules and restrictions on people's behavior. For example, Uber has ordered its drivers to stay away from protests in China, and it has a way to enforce the rule: they will use drivers' cellphones to track car location and cancel the contracts of violators. Though Uber's policy is a business decision, this rule has the political implication of cutting off a transportation option for Chinese citizens who want to help reform their government.

CON ARGUMENTS

STOPPING TERRORISM

What's the argument?

One of the most common arguments made in favor of NSA surveillance, especially amongst intelligence officials, is that surveillance data is used to identify and prevent acts of terrorism. The reasoning behind this is relatively simple: terrorist operations typically spread throughout social networks, so if one individual begins displaying radical or extremist tendencies online, the NSA can quickly and easily identify any and all persons to whom this ideology may have spread (“Surveillance and interception of communications.”)

This logic has been somewhat substantiated by past instances where federal agencies were able to stop acts of terrorism (Hines). For example, NSA surveillance data was able to stop a Somali Al Shabab terrorist funding initiative based in San Diego (Sharma). Additionally, the NSA is believed to have stopped a New York City subway bombing plot in 2009, but officials say it is impossible to be fully transparent due to the need to keep operations covert (Whitesides and Cornwell).

Why does the argument matter?

Metadata collected by the NSA allows federal agencies to piece together an extensive network and outline every stage of planning a terrorist attack. This allows them to save lives before they're even endangered, intercepting and thwarting these plots as they are being planned. While the War on Terror is still being fought, because of US devotion to counterterrorism over the years, global deaths from terrorist attacks continue to fall and many organizations have been defeated (Tarallo).

Main Players

Domestic terrorists, counter-terrorism officials, American civilians

Strategy Considerations

In a topic characterized by more nebulous, philosophical impacts such as democracy and the social contract, terrorism has a very tangible, high-magnitude impact: human lives. This makes it easy to outweigh most opponents, even if they win their links. This also helps craft a strong narrative about the security imperative behind the NSA, especially if it's accompanied with a sense of urgency in light of rising tensions with Iran. However, teams must be able to prove that these attacks would've gone forward without NSA surveillance, and not thwarted through other means.

Evidence for Stopping Terrorism

Surveillance is useful to terrorism-fighting agencies

“Surveillance and interception of communications.” *The Doha Declaration: Promoting a Culture of Lawfulness*. July 2018. <https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/surveillance-and-interception.html>

Public authorities involved in the prevention and investigation of acts of terrorism and potential terrorist conspiracies have shown great interest in ensuring that the records generated by communications service providers (e.g., public and private companies providing

telecommunications and Internet services) are available to them for the prevention, investigation and prosecution of serious crime, including terrorism. An accompanying source of privacy related concern has been the growing

practice of some intelligence agencies to gather bulk information about their citizens using telephone and Internet networks as part of their counter-terrorism efforts (Council of Europe, Parliamentary Assembly, 2015(b), paras. 1-3). Such bulk information usually contains descriptive information about other data and is called 'metadata' (Council of Europe, Parliamentary Assembly, 2015(a), para. 18). An example of metadata is the Internet Protocol address associated with a computer from which an individual had sent an email (Council of Europe, Parliamentary Assembly, 2015(b), para.12). Other examples are a list of telephone numbers which an individual dialed on a

particular day, or a list of websites which an individual has visited. The fact that the causes of terrorism include psychological and sociological factors provide a partial explanation as to why intelligence services are often keen to collect metadata as part of their efforts to identify terrorist networks. It is known that

terrorists recruit through social networks and social media (Taylor, 2016). If one can monitor individuals who actively expand their networks and post violent ideological messages on social media then one could come closer to identifying individuals who might potentially be involved in recruiting for, or joining terrorist groups. Additionally, social groups use symbols to identify themselves and their

cause as part of disseminating propaganda, radicalizing and recruiting individuals around a cause. By gathering metadata associated with symbols associated with terrorist groups or their causes, intelligence agents could locate individuals who support a terrorist cause. Moreover, one can potentially learn about potential causes of social conflict, and drivers of violent extremism through collecting information about the types of Internet activities individuals engage in. Intelligence and law enforcement agencies could use this information to engage more effectively with local communities as part of broader terrorism prevention strategies.

NSA surveillance prevented over 50 potential terrorist attacks

Hines, Pierre. “Here’s how metadata on billions of phone calls predicts terrorist attacks.” *Quartz*. 19 June 2013. <https://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/>

Yesterday, when NSA Director General Keith Alexander testified before the House Committee on Intelligence, he declared that the

NSA’s surveillance programs have provided “critical leads to help prevent over 50 potential terrorist events.” FBI Deputy Director Sean Boyce elaborated by describing four instances when the NSA’s surveillance programs have had an impact: (1) when an intercepted

email from a terrorist in Pakistan led to foiling a plan to bomb of the New York subway system; (2) when NSA’s programs helped prevent a plot to bomb the New York Stock Exchange; (3) when intelligence led to the arrest of a U.S. citizen who planned to bomb the Danish Newspaper office that published cartoon depictions of the Prophet Muhammad; and (4) when the NSA’s programs triggered reopening the 9/11 investigation. So what are the practical applications of internet and phone records gathered from two NSA programs? And how can “metadata” actually prevent terrorist attacks? Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted. Section 215 of the Patriot Act provides the legal authority to obtain “business records” from phone companies. Meanwhile, the NSA uses Section

702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases. One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists' planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat.

NSA surveillance prevented NYC subway bombing, but it's difficult to be transparent because most operations must be covert

Whitesides, John and Susan Cornwell. "NSA director says surveillance helped stop 'dozens' of attacks." *Reuters*. 12 June 2013. <https://www.reuters.com/article/us-usa-security/nsa-director-says-surveillance-helped-stop-dozens-of-attacks-idUSBRE95910O20130612>

"This is not us doing something under the covers," Alexander said. "We want to tell you what we're doing, and tell you that it's right, and let the American people see this." Alexander promised to make details of the thwarted attacks available to the public within the next week.

Officials said last week the email surveillance program played a role in foiling a 2009 Islamist militant plot to bomb the New York City subway system. Some members of Congress and

advocacy groups have pushed for tighter controls on the surveillance, which is subject to authorization by secret court orders. A bipartisan group of lawmakers asked on Wednesday for a probe of the programs by the Privacy and Civil Liberties Oversight Board, created after the September 11 attacks to oversee issues involving civil liberties. Alexander said the agency would cooperate with any board

investigation. Slideshow (5 images) "It's very, very difficult to have a transparent debate about secret programs, approved by a secret court issuing secret court orders based on secret interpretations of law," Democratic Senator Tom Udall of New Mexico said. Senators at the hearing wondered why Snowden, who had a spotty educational record and a relative lack of experience in the national security field, was able to gain a top-secret clearance and access to such sensitive information.

NSA surveillance convicted Somali Al Shabab terrorist funding initiative out of San Diego

Sharma, Amita. "NSA Surveillance Triggered 2010 Terror Case Against San Diego Men." *KBPS*. 18 June 2013. <https://www.kpbs.org/news/2013/jun/18/nsa-surveillance-spawned-somali-terror-financing-c/>

The case against four San Diego men convicted earlier this year of conspiring to send money to the Somali terrorist group al-Shabab was triggered by the National Security Agency's controversial surveillance program, said FBI Deputy Director Sean Joyce during a hearing Tuesday. Joyce told the House Intelligence Committee that the NSA spotted a San Diego phone number from its database of all domestic phone call logs because of its suspicious contacts outside the United States. He said the NSA gave the number to the FBI. Joyce said that after electronic surveillance was carried out in the case, officials learned the phone number belonged to a man planning to send money to a terrorist group in Somalia.

Joyce said co-conspirators were identified through the surveillance and the terrorist activity was disrupted. Federal officials in

San Diego confirmed the case was that of the four Somali immigrants arrested in 2010 and charged with providing financial support to al-Shabab in Somalia. They were convicted earlier this year. The government's case was primarily based on wiretaps of calls between the men and members of al-Shabab.

Terrorist fatalities continue to decrease, down more than 52%

Tarallo, Mark. "Fatalities from terror attacks continue to decrease." *Asia Online*. March 2020. <https://www.asionline.org/security-management-magazine/articles/2020/03/fatalities-from-terror-attacks-continue-to-decrease/>

For the fourth consecutive year, deaths from terrorism worldwide have declined, according to the latest edition of the Global Terrorism Index (GTI). **This means that total deaths from terrorism are now down more than 52 percent from their peak in 2014.** Nonetheless, terror's tentacles still have a grip on countless countries around the world, according to the GTI, which is produced by the Institute for Economics and Peace and based on data from the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database. In 2018, the last full year for which data was available, 103 countries recorded at least one terrorist incident, and 71 countries suffered at least one fatality from a terror attack. This marks the second worst year on record for the number of countries suffering at least one death. "Although the intensity of terrorism has diminished, its breadth has not," the report authors write. "It highlights the need for continued assertive international action to combat terrorism." Bombings and armed assaults have remained the most common types of terrorist attack over the past two decades, according to the report. In sum, the GTI sketches out global trends in terrorism in the last 50 years, with an emphasis on trends since 2014—the year which some say marked the beginning of the fall of the Islamic State (ISIS).

DISCOVERING ESPIONAGE

What's the argument?

One critical function of the NSA's program of mass surveillance is identifying espionage, both foreign and domestic. As the US' role in global affairs continues to increase, foreign governments have taken to paying government officials to funnel sensitive data overseas (Kramer). This increases the United States' vulnerability to espionage because normal, law-abiding citizens can easily give way to financial incentives at corruption.

Luckily, because they process 75% of all US internet traffic, the NSA has been able to identify many bad actors through their surveillance. This process allows for the identification of both victims and perpetrators of espionage (Gorman). The NSA's existence also deters citizens from turning to espionage since they know it's very easy for them to get caught and prosecuted. In fact, in 2018, the NSA identified over 17 thousand victims of foreign espionage (Harris). In one particular instance, they were able to catch a Russian email hacking group (Barnes).

Why does the argument matter?

Espionage amounts to much more than just a violation of privacy. One impact of particular relevance is the potential for espionage to delay or hamper the efforts to produce a COVID-19 vaccine (Roberts). Beyond just this pandemic, though, espionage has serious costs to the economy - \$445 billion annually, to be precise (Nakashima). Countries and international corporations lose trust in the credibility and reliability of US companies and therefore are less inclined to purchase their goods. This problem is most prevalent within the tech sector.

Furthermore, espionage threatens US national security. If adversarial governments like Russia and China are able to receive sensitive US intelligence or new military technology, it loses the United States their military advantage and diplomatic standing when responding to global conflicts.

Main Players

Foreign governments, American citizens, American corporations, low-level government officials

Strategy Considerations

Teams seeking to run this argument on con must be prepared to quickly respond to the predictable pro retort: ending surveillance on American citizens won't impact our ability to detect foreign espionage. While this response doesn't interact with the specific warranting, it will likely be an instinctual response and, without a clear explanation from con as to why it is not accurate, judges could be persuaded. This argument is also more heavily supported than instances of the NSA stopping domestic terror. The only way to truly uncover planted spies is to monitor all communications, so the argument is incredibly unique especially when compared to pro privacy arguments or even other con arguments.

Evidence for Discovering Espionage

Vulnerability to Espionage

US is vulnerable to insider espionage

Kramer, Lisa and Richards Heuer. "America's Increased Vulnerability to Insider Espionage." *International Journal of Intelligence and Counterintelligence*. 2007. <https://noir4usa.org/wp-content/uploads/2014/02/Americas-Increased-Vulnerability-to-Insider-Espionage.pdf>

Because espionage is a secret activity, it is not possible to know how many spies are currently active in American organizations or exactly what the future will bring in terms of discovered espionage cases. Nevertheless, it is possible to explore U.S. vulnerability to the crime of insider espionage by examining known factors that, on the basis of past experience, can serve to make insider espionage more or less likely to occur. A recent study has identified technological, social, and economic trends that are serving to increase the opportunity and motivation for insider espionage. Opportunity for espionage consists of access to classified or proprietary information that can be exchanged for money or other benefits, access to foreign entities interested in obtaining this information, and means for transferring this information to foreign recipients. Motivation, broadly defined, is a feeling or state of mind that influences an individual's choices and actions. While motivation for espionage results from a complex interaction between personality characteristics and situational factors, the focus here is primarily on the latter. If more insiders are encountering situations that provide motivation and opportunity for espionage, the

logical conclusion is that United States vulnerability to this crime is increasing. Technological advances in information storage and retrieval are making it increasingly difficult to control access to classified and proprietary information. The same characteristics of information technology (IT) systems that improve employee productivity also enhance employee capacity to gather information for the purposes of espionage. Two specific technological advances have particularly dramatic implications for spying: the development of large, networked databases with automated search functions and the miniaturization of data-storage devices. The increasing dependence upon networked databases exponentially increases the amount of information a single malicious insider can access. Automated search functions make it possible for insider spies to locate specific kinds of data—for example, information that is of particular value to foreign buyers. American spies who exploited large organizational databases include Aldrich Ames, Harold Nicholson, Brian Regan, and Robert Hanssen. In addition to improved ability to locate specific types of information, rapid advances in the miniaturization of data storage devices make it easier for an insider to remove large quantities of information from an organization without being detected. The physical size and cost of memory sticks and flash drives are decreasing, yet the data storage capacities of these devices are expanding. As the miniaturization of storage hardware continues, the emergence of nanoscale devices—devices with structural features in the range of 1 to 100 nanometers—is likely. Potential future applications of nanoscale electronics include tiny data storage devices with capacities that are 1,000 times greater than those of today. Numerous products now available do not look like data storage devices but hold substantial sums of material. For example, the USB Memory Watch appears to be a normal timekeeping device, but it has a USB cable hidden in the band and the capacity to store up to 1 megabyte of data—around 22,000 pages of text. As a result of America's status as a

dominant political, economic, and military force, and the increasingly competitive global economy, foreign demand for protected U.S. information is increasing. American insiders now have access to more types of protected information that can be sold for profit and can sell information to a broader range of private and government-sponsored entities than ever before. Insiders working within American biotechnology, aerospace, telecommunications, computer software and hardware, advanced transportation, manufacturing, energy research, pharmaceutical, and semiconductor industries have access to proprietary information that foreign businesses and intelligence collectors will pay substantial sums of money to obtain. Increasing demand for American proprietary information supplements an ongoing demand for classified information pertaining to information systems, sensors and lasers, electronics, aeronautics, armaments, energetic materials, marine and space systems, guidance systems, navigation and vehicle systems, signature control systems, space systems, nuclear systems technologies, chemical-biological systems, weapons effects and countermeasures, ground systems, and directed and kinetic energy systems.⁵ In addition to foreign government representatives, American employees can now sell protected information to foreign and multinational corporations, foreign research and science institutions, freelance agents (some of whom are former intelligence officers), terrorist organizations, revolutionary groups, extremist ethnic or religious organizations, drug syndicates, and organized crime groups. As more allied and friendly

countries pursue U.S. technological information, some insiders may find it easier to rationalize committing espionage. Other individuals who consider it reprehensible to sell American technology or military secrets to an avowed enemy of the United States may be less reluctant to sell this information to individuals or organizations in countries that are viewed as friendly to U.S. interests. The globalization of business and scientific research is expanding the opportunity for espionage by increasing the frequency with which insiders are able to establish and maintain contact with foreigners interested in exploiting

their knowledge. Relationships established through participation in joint research and business projects and attendant activities provide opportunities for Americans to share or sell classified information and make it easier for foreign entities to identify and recruit Americans with exploitable weaknesses. The frequency and nature of foreign scientific and business relationships also makes it more difficult for security and counterintelligence personnel to distinguish relationships that present a significant security risk from those which do not. Participation in joint business ventures creates an environment that may be particularly conducive to espionage. According to Deputy Assistant Secretary of Defense Linton Wells, the inclination of those involved in multinational trade to regard the unauthorized transfer of information or technology as a business matter rather than an act of national betrayal or treason may be growing. Foreign business relationships commonly involve discussions in which sellers and buyers bargain over price, quantity, and quality. Providing sensitive information or working as a “technical consultant” can be a bargaining chip in these negotiations. Collaboration on scientific research projects, by its very nature, involves the approved exchange of scientific and technical information. Some insiders participating in these exchanges have access to protected information that should not be shared, yet may find it difficult to determine exactly which information is protected and which is public. Some scientists believe that, in the spirit of furthering scientific discovery, research findings must be divulged. Available data suggests that greater numbers of insiders routinely participate in collaborative international scientific and commercial endeavors, and that the number of international science and technology agreements being forged between the U.S. government and foreign counterparts is increasing over time. The percentage of papers authored by U.S. scientists in conjunction with foreign scientists has been increasing steadily for decades. Scientific collaboration between the United States and other countries is occurring more often in the private sector as well. The increasingly multinational nature of research and development is illustrated by the growing establishment of international research facilities. Finally, the number of American organizations involved in the exportation of goods and services to foreign countries, and the value of these goods and services, have gone up dramatically in the last twenty years. Increasing Frequency of International Travel Americans are making more visits abroad, and citizens of other nations are visiting the United States more often. Increased frequency of international travel results in increased opportunity for the transfer of classified and other protected information to foreign entities. American insiders with access to valuable information are better able to establish contact with foreign buyers, and foreign nationals have more opportunity to spot, assess, and recruit American personnel. At the same time, while it is becoming easier for American sellers of information and foreign buyers to contact each other, security and counterintelligence personnel are experiencing greater difficulty in distinguishing between foreign travel and contacts that are of security concern.

NSA Identifies Instances of Foreign Espionage

Identified nearly 17 thousand US victims of foreign espionage

Harris, Shane. “NSA Unmasked More US Identities, Likely to Warn Victims of Foreign Spying, new report suggests.” *Washington Post*. 30 April 2019.

https://www.washingtonpost.com/world/national-security/nsa-unmasked-more-us-identities-likely-to-warn-victims-of-foreign-spying-new-report-suggests/2019/04/30/35739e80-6b50-11e9-9d56-1c0cf2c7ac04_story.html

The National Security Agency revealed the identities of many more citizens, permanent residents and corporations who were mentioned in intelligence reports last year, in a process

known as “unmasking” that has been a source of controversy for President Trump and his allies in Congress. But **the statistics**,

released Tuesday in an annual report, may **reflect an increase in the number of people or American**

businesses being victimized by a foreign government, including through computer hacks, and **whose identities were revealed to warn them**, a U.S. official said. In 2018, the NSA, which conducts legally authorized

surveillance of communications overseas, unmasked the identities of 16,721 “U.S. persons,” a term that includes corporations, in response to a request from another government agency, according to the report from the Office of the Director of National Intelligence. That was a more than 7,000-person increase from 2017. In the course of monitoring communications abroad, the agency routinely picks up the communications of U.S. persons, whose identities are “masked” in reports that are circulated among government agencies, to protect their privacy. When the recipient of a report — for instance, an official at the CIA — can demonstrate a “need to know” that U.S. person’s identity, to assess the information in the report and its importance, officials and lawyers who review the matter can unmask it and show a name or other piece of identifying information. It wasn’t immediately clear how the administration or lawmakers would react to the sharp increase in unmaskings under the Trump administration. Alex Joel, who oversees civil liberties and transparency issues for the Director of National Intelligence, attributed the spike in part to **foreign intelligence services that are trying to monitor U.S. individuals and companies. Foreign computer hackers have aggressively stepped up their efforts in recent years to steal private communications or pilfer trade secrets from U.S. companies.** In recent years, **the FBI has made an effort to warn Americans when a foreign**

government is trying to spy on U.S. persons or steal their communications, according to U.S. officials involved in the practice who spoke on the condition of anonymity to discuss the process. Law enforcement officials often find out who is being targeted based on information collected overseas, including by the NSA. The new report emphasized that a single report from the agency could contain “multiple U.S. person identities, masked and/or openly named. For example, a single report could include a large number of U.S. identities that a foreign intelligence target is seeking to victimize; each of those identifiers would be counted.” The term “identity” also encompasses an email address or an Internet protocol address, the unique number that identifies a particular computer. So, the larger number of unmasked identities could consist of that information, in addition to names. The report also took stock of a range of other authorized surveillance activities that the intelligence community conducts under the Foreign Intelligence Surveillance Act, but it didn’t disclose many dramatic changes. The total number of orders issued by the surveillance court in 2018, for instance, was around 1,100, a drop of about 250 orders from the previous year. But the estimated number of “targets” of those orders, which could be a person’s communications or a physical place, went up by about 37 percent, to just over 1,800. About 12.7 percent of those targets are estimated to be U.S. persons, according to the report. The figure includes surveillance that is conducted overseas and within the United States. It can be difficult to discern the reason that figures fluctuate from year to year, Joel said. The report notes that changes in world events, the priorities of a particular agency, new technical capabilities and changes in behavior by those who are being surveilled are all contributing factors. “These reasons often cannot be explored in detail in an unclassified setting without divulging information necessary to protect national security,” the report says. “Moreover, there may be no relationship between a decrease in the use of one authority and an increase in another.” Overall, Joel said that the report shows that the government is conducting surveillance in ways that “can be expected” given what the law allows. In cases where the numbers changed, it wasn’t because those legal authorities had changed, he said.

NSA caught Russian email hackers

Barnes, Julian and David Sanger. “US Accuses Russian Military Hackers of Attack on Email Servers.” *New York Times*. 28 May 2020.

<https://www.nytimes.com/2020/05/28/us/politics/nsa-russian-hack.html>

The National Security Agency publicly accused Russian government hackers of targeting email servers around the world in an unusual announcement on Thursday, showing that the agency is becoming more aggressive in calling out Moscow’s action as the presidential election approaches. While the Trump administration has publicly attributed cyberattacks to Russia before – including for its 2016 election hack and for paralyzing Ukraine in 2017, which damaged the operations of the shippers Maersk and FedEx – this allegation was unusually specific. It singled out Russia’s military intelligence unit, widely known as the G.R.U., demonstrating intelligence agencies’ concern that Russia intends to interfere in the election only a little more than five months away. But it also comes as President Trump has renewed his baseless claims that the investigation into Russia’s activities was part of a “hoax” intended by Democrats to paralyze him. He has publicly questioned Russia’s culpability in the election hacking and appeared to accept President Vladimir V. Putin’s argument that Russia was so good at cyberoperations that it would never have been caught. “There has been a reluctance to be critical of Russia because of echoes of investigations,” said retired Gen. Martin E. Dempsey, the former chairman of the Joint Chiefs of Staff. “For the N.S.A. to do that, in this climate, they must have absolutely incontrovertible evidence.” The “Sandworm Team,” a group of G.R.U. hackers, tried to use a vulnerability in computer networks to gain access to them, the National Security Agency said. It did not say which networks were compromised. But the software targeted by the hackers, Exim, is a commonly used email transfer program, used by some Unix computers. Exim was developed at Cambridge University and is frequently used in Britain. The vulnerability allowed attackers to execute commands and run their own code on compromised networks, a National Security Agency official said. It was, the agency said in its announcement, “pretty much any attacker’s dream access.” The Russian Embassy in Washington did not respond to a request for comment. Since before the 2018 midterm elections, the National Security Agency and its sister agency, United States Cyber Command, have stepped up efforts to identify and deter Russian interference. They have taken down internet networks used to spread divisive messages, warned the people behind troll farms against spreading disinformation and carried out other undisclosed operations. They also began an operation to put malware in the Russian electrical grid, as a warning about what kind of retaliation could happen if Moscow tried to attack the American grid. The G.R.U.’s continued malicious activity shows that the American counterattacks have had only a modest effect, even as the National Security Agency persists in pressuring Russia. “When you are looking at some of the actions that have been done, they haven’t quite made their mark,” Scott Jasper, a lecturer at the U.S. Naval Postgraduate School and the author of a new book, “Russian Cyber Operations,” said at a Cato Institute event on Thursday. Hackers from the G.R.U. were behind both the theft of documents on the Democratic National Committee’s servers and the hack of Hillary Clinton’s campaign in 2016. Russia publicly released those documents in an attempt to promote the election of Donald J. Trump, the United States government concluded. The ability to exploit the software was first identified publicly in June 2019, and the G.R.U. team began using it two months later, targeting unpatched systems, according to the National Security Agency. The agency urged companies using the Exim software to update it to remove the vulnerability. In February, the State Department called out the G.R.U. and the Sandworm Team, accusing them of conducting electronic attacks on the republic of Georgia in 2019 that defaced government websites and interrupted television broadcasts. For the agency to accuse a Russian intelligence agency is a sign that, at least for now, it can operate outside of direct

political pressure from Mr. Trump, former officials said. National Security Agency officials have insisted that their agency is able to operate apolitically, without political influence changing their intelligence judgments. But that often involves acting against Russia without first seeking explicit permission from the president. Under a presidential order issued in 2018, Gen. Paul M. Nakasone, the head of the agency and the commander of the United States Cyber Command, can operate on his own authority in operations short of war, including the kind that involve pushing back on Moscow.

NSA goes through 75% of US internet traffic

Gorman, Siobhan and Jennifer Valentino-Devries. "New Details Show Broader NSA Surveillance Reach." *Washington Post*. 20 August 2013.

<https://www.wsj.com/articles/SB10001424127887324108204579022874091732470>

The National Security Agency—which possesses only limited legal authority to spy on U.S. citizens—has built a surveillance network that covers more Americans' Internet communications than officials have publicly disclosed, current and former officials say. **The system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence**, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say. The NSA's filtering, carried out with telecom companies, is designed to look for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the U.S. But officials say the system's broad reach makes it more likely that purely domestic communications will be incidentally intercepted and collected in the hunt for foreign ones.

Impacts of Foreign Espionage

Could delay / hamper COVID-19 vaccine production

Roberts, Nicole. "COVID Crimes: Espionage, Hackers, and Why America is Vulnerable."

Forbes. 28 July 2020. <https://www.forbes.com/sites/nicolefisher/2020/07/28/covid-crimes-espionage-hackers-and-why-america-is-vulnerable/?sh=1d868bae5873>

In recent years, cybercrimes and hacks have increased dramatically. Every few weeks, we hear of another data breach, phishing scam or social media hack impacting millions of people. It is estimated that a cybercrime is committed every 39 seconds somewhere in the world to the tune of an estimated \$6 trillion by 2021. And those assessments were done before tens of millions of people were abruptly compelled to work from home with no time for proper cybersecurity planning. But the cybercrime risks faced by Americans working from home are just the tip of a very dangerous cyberattack iceberg. Strong evidence indicates that **Russia, China and potentially other adversaries have been attempting to hack universities and research institution's databases to steal potentially lifesaving Covid-19-related intellectual property**. Pharmaceutical companies too have seen a barrage of hacking attempts. And just days ago, the European Union's top court ruled that U.S. privacy protections are inadequate for sharing personal and other sensitive information – potentially threatening our ability to work with E.U. countries on vaccines and treatments. With millions of lives and trillions of dollars at stake, **the U.S. is in a dangerous place when it comes to vulnerabilities associated with the pandemic** – one of which is cybersecurity. To

understand just what we're facing, I asked Bryan Cunningham, long-time cybersecurity and privacy lawyer and Founding Executive Director of the University of California, Irvine Cybersecurity Policy & Research Institute, exactly what's going on, what the focus should be, and what precautions Americans should be taking. Nicole F. Roberts: While the world is focused on the health and economic threats posed by Covid-19, cybercriminals around the world are capitalizing on this crisis. Most people don't know all the ways cybersecurity can be threatened, nor what the implications are. So how can (or are) cybercriminals using the pandemic to their advantage? Bryan Cunningham: Much like politicians, bad cyber actors never let a crisis go to waste. Within days of Johns Hopkins posting their widely-cited Covid-19 statistics map, cyber attackers had posted a near replica that – if clicked on – would launch a cyber attack against your device. In addition to the plethora of phony tests and cures being peddled on the internet (a tale as old as time), professional nation-state hackers, particularly in Russia and China, are launching massive attacks against Covid-19 researchers in the West, trying to steal IP that can accelerate treatments, vaccines and the like. Roberts: That sounds like espionage. Is that what we're really talking about? We hear so much about Russia and China hacking U.S. data. But how does that play out in the science and medical communities? Cunningham: The U.S. Director of National Intelligence a few years ago testified before Congress that Chinese IP theft against the United States amounted to the greatest transfer of wealth in

human history. Even in normal times, the People's Republic of China, the Russian Federation, and other nation states concentrate massive intelligence resources on stealing western intellectual property, whether related to medical, defense, or other advanced technologies. Recent reports have – predictably – validated significant efforts, particularly by Russian intelligence, to steal any and all research being conducted in the west targeted towards vaccines or treatments for Covid-19. Hopefully the U.S. and allied governments are taking measures to combat these significant threats, but academics, public-health scientists, and other researchers also must be vigilant by: not clicking on links they are not certain are from trusted colleagues; using multifactor authentication, Virtual Private Networks (VPN), and strong passwords; and using common sense before sharing information with anyone. Roberts: Let's talk more about international issues. What's going on in Europe with this Schrems II decision? My understanding is that is says American data and privacy protections don't meet

European standards. So, essentially, without significant intelligence, surveillance, and privacy reform in the United States, we could lose access to the health and science data coming out of Europe that might help us fight

coronavirus? Cunningham: The Court of Justice of the European Union (CJEU) this week struck down the "Privacy Shield" agreement between the U.S. and Europe that had enabled U.S. companies to transfer personal data of E.U. citizens to the United States, holding that U.S. privacy protections are inadequate under applicable European law. As with its prior decision striking down the U.S. "Safe Harbor" agreement, the Court found that American intelligence and surveillance laws do not provide adequate privacy protections to non-U.S. Persons and that they discriminate against non-Americans. The Privacy Shield agreement made possible transatlantic data transfers by more than 5,000 U.S. and E.U. companies, enabling approximately 1/3rd of all global trade flows. Unlike the U.S., the European Union has comprehensive privacy protections for its citizens, enshrined in the E.U. Charter of Fundamental Rights and the recently enacted General Data Protection Regulation (GDPR). These protections include limitations on government surveillance and meaningful mechanisms for redress for individuals improperly surveilled. In 2015, the CJEU invalidated the prior "Safe Harbor" agreement with the U.S. which enabled US companies to transfer protected data of E.U. citizens to the U.S. despite the fact that the E.U. does not consider U.S. privacy protections adequate. The Court was particularly troubled by the lack of a legal mechanism for E.U. citizens to determine if they have been surveilled by U.S. authorities and gain meaningful redress for any unlawful invasions of their privacy. Roberts: So, what does that mean for health care and Covid-19?

Espionage costs \$445 billion annually

Nakashima, Ellen and Andrea Peterson. "Report: Cybercrime and espionage costs \$445 billion annually." *Washington Post*. 9 June 2014.

https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

A Washington think tank has estimated the likely annual cost of cybercrime and economic espionage to the world economy at more than \$445 billion – or almost 1 percent of global income. The estimate by the Center for Strategic and International Studies is lower than the eye-popping \$1 trillion figure cited by President Obama, but it nonetheless puts cybercrime in the ranks of drug trafficking in terms of worldwide economic harm.

"This is a global problem and we aren't doing enough to manage risk," said James A. Lewis, CSIS senior fellow and co-author of the report, released Monday. The report, funded by the security firm McAfee, which is part of Intel Security, represents one of the first efforts to analyze the costs, drawing on a variety of data. "Cybercrime costs are big, and they're growing," said Stewart A. Baker, a former Department of Homeland Security policy official and a co-author of the report. "The more that governments understand what those costs are, the more likely they are to bring their laws and policies into line with preventing those sorts of losses. According to the report, the most advanced economies suffered the greatest losses. The United States, Germany and China together accounted for about \$200 billion of the total in 2013. Much of that was due to theft of intellectual property by foreign governments. Though the report does not break out a figure for that, or name countries behind such theft, the U.S. government has publicly named China as the major perpetrator of cyber economic espionage against the United States. The Chinese government has accused the United States of being one of the biggest perpetrators of cyber-espionage, but the U.S. government has always objected that it does not steal intellectual property and hand it to its own industries to give them a competitive advantage. CSIS estimated that the United States lost about \$100 billion. Germany was second with \$60 billion, and China followed with \$45 billion. In both the United States and China, the losses represent about 0.6 percent of their economies, while Germany's loss is 1.6 percent. Japan, the world's fourth largest economy, reported losses of \$1 billion, which researchers said was extremely low and not credible. Valuing intellectual property is an art form, based on estimating future revenues the intellectual property will produce or the value the market places on it, the report said. Putting a price tag on it is difficult but not impossible, it said. Intellectual-property theft lessens companies' abilities to gain a full return on their inventions, and so they turn to other activities to make a profit, the report states. That depresses overall global rates of innovation, it said. The report stated that countries appear to tolerate cybercrime losses as long as they stay at less than 2 percent of their national income. If losses rise above 2 percent, "we assume it would prompt much stronger calls for action as companies and societies find the burden unacceptable," it said. The report breaks the harm into three categories, without giving figures. The largest, it said, is intellectual property theft. The second is financial crime, or the theft of credit

card and other types of data largely by criminal rings. The third is theft of confidential business information to gain an advantage in commercial negotiations or business deals. CSIS used several methods to arrive at a range of estimates, from \$375 billion to as much as \$575 billion. Researchers looked for published data from governments around the world. They interviewed officials in 17 major countries. And they came up with a predictive model based on a CSIS report last year that estimated the cost of cybercrime to the U.S. economy. Their figures also included the cost of recovering from cyberattacks. The main assumption they used was that the cost of cybercrime is a constant share of national income — at least in countries with similar levels of development. In less developed countries, that cost is about 0.2 percent of gross domestic product, and in advanced economies it is almost 1 percent. In 2009, McAfee issued a news release that pegged global economic losses at more than \$1 trillion. The figure was cited by the White House and then-National Security Agency director Gen. Keith B. Alexander. But this year's CSIS report concluded that it was unlikely that cybercrime cost more than \$600 billion, which is the cost of the global drug trade. The researchers said cybercrime and economic espionage require a response on par with global efforts to reduce drug trafficking. Besides better cybersecurity technologies, they said, governments need to devote resources to building defenses and to commit to observing existing international commitments to protect intellectual property.

CYBER ATTACKS

What's the argument?

Offensive cyber operations are increasingly being used by nations as a means of modern warfare. The NSA has helped spearhead the pivot to cyberwarfare by creating ransomware and programs to conduct these attacks. Furthermore, NSA surveillance of citizens plays an active role in discovering cyberterrorists and hackers that reside within the United States (Goldsmith). Overall, NSA surveillance is critical to both cyber offensive operations and defensive cybersecurity. Without the ability to discover these hacks and leaks, there would be significantly more cybercrime and vulnerability in the United States' cyber infrastructure.

Why does the argument matter?

Cyberattacks come with very probable and very dangerous impacts. Economically, personal data breaches and attacks on small businesses compromise innovation and destroy jobs. Overall, the total impact of cyberattacks on the US economy are an estimated \$243 billion rising up to \$1 trillion in the most extreme cases (Bolt). As such, it comes as no surprise that economic experts think the next global financial crisis will be triggered by a cyberattack (Pisani). If it is at all similar to 2008, this could put hundreds of millions into extreme poverty.

Cyberattacks also have a potential high magnitude impact when targeting critical infrastructure. While this scenario is less likely, experts argue that a planned-out grid attack could result in mass injury and a death toll similar to that of a nuclear weapon (Straub). Because this impact is so severe, any effort that the NSA can make to help stop cyberattacks is of extreme importance.

Main Players

North Korea, Russia, Chinese, independent hackers, US cybersecurity, small businesses, stock markets

Strategy Considerations

Cyberattacks have extremely terminal impacts that have been calculated and researched by scholars. These impacts are also very likely to manifest given that several small businesses are hacked every day and there are substantial threats to critical infrastructure as well. While the economic ramifications are not as high magnitude as other impacts on this topic, it is definitely ahead when it comes to the strength of its relevance to the topic as well as the probability that it will occur.

Evidence for Cyber Attacks

NSA prevents cyber-intrusions and prevents large losses of international property

Goldsmith, Jack. "We Need an Invasive NSA." *The New Republic*. 10 October 2013.

<https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>

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. 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.

Cyberattacks on business cost \$243 billion to more than \$1 trillion to the US economy

Bolt, Tom. "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid." *Center for Risk Studies University of Cambridge*. 2015.

<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf>

Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain. The total impact to the US economy is estimated at \$243bn, rising to more than \$1trn in the most extreme version of the scenario. The report also analyses the implications of these direct and indirect consequences on insurance losses. The total of claims paid by the insurance industry is estimated at \$21.4bn, rising to \$71.1bn in the most extreme version of the scenario. One of the important considerations identified by this report for insurers is the wide range of claims that could be triggered by an attack on the US power grid, revealed in the matrix in Figure 4 at page 40.

A cyberattack could trigger the next US financial crisis that could go global

Pisana, Bob. "A cyberattack could trigger the next financial crisis, new report says." *CNBC*. 13 September 2018. <https://www.cnbc.com/2018/09/13/a-cyberattack-could-trigger-the-next-financial-crisis.html>

A cyberattack could trigger the next financial crisis, a new report suggests. Imagine this hypothetical scenario: A criminal gang or a state actor hacks into a central bank, a custodial bank or a clearing firm that settles daily stock, bond and derivative trades. There are not many of these firms, so they are "systemically important." Say this hack disrupts the operations of one or more of these firms to the point that their services shut down and key data is damaged or destroyed. It's difficult to replicate all the services these firms provide, so the effects ripple across other financial services firms. For example, Iran hacked banks and last year, crediting company Equifax was hacked and sent ripples through the market. When it comes to a financial crisis, everyone seems to agree that the next one will not come in the same form as the one that hit 10 years ago this week, which was tied to a housing bubble and shoddy mortgage lending practices. "We tend to fight the last war," former Treasury Secretary Hank Paulson said in an interview Wednesday with *CNBC's* Andrew Ross Sorkin at the Brookings Institution. But determining what the next crisis will look like is a lot like talking to a bunch of blind people who are petting an elephant. Their impression of the elephant depends on what part of the elephant they are touching.

Cyberattack could have the death toll of a nuclear bomb

Straub, Jeremy. "Hackers Could Kill More People Than a Nuclear Weapon." *Live Science*. 27 August 2019. <https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html>

As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon. Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths. This might sound alarmist, but look at what has been happening in recent years, in the U.S. and around the world. In early 2016, hackers took control of a U.S. treatment plant for drinking water, and changed the chemical mixture used to purify the water. If changes had been made — and gone unnoticed — this could have led to poisonings, an unusable water supply and a lack of water. In 2016 and 2017, hackers shut down major sections of the power grid in Ukraine. This attack was milder than it could have been, as no equipment was destroyed during it, despite the ability to do so. Officials think it was designed to send a message. In 2018, unknown cybercriminals gained access throughout the United Kingdom's electricity system; in 2019 a similar incursion may have penetrated the U.S. grid.

ELECTION SECURITY

What's the argument?

For the past several years, and especially in the past few months, the national conversation surrounding election security has increased significantly. While this conversation has largely centered around foreign threats, recent information indicates that much of the threat of misinformation and interruption emerges from within our own borders (Myre and Bond).

As a result, the NSA's Election Security Group has expanded their focus to include ransomware attacks against the election. The built-up defense works to combat the possibility that malicious actors could seize this moment, which would result in more distrust in election results (Vavra).

Critically, compromised election security places our entire democracy in jeopardy (Henry). When people distrust the results of an election, the very institution upon which our government relies is endangered.

Why does the argument matter?

Jeopardizing election security decreases faith in our political system, creating populist backlash movements and decreasing the legitimacy of the US as a country. A reduction in democratic strength within the United States could lead to lower human capital, higher inflation, higher political instability, and lower levels of economic freedom. This means that even if we don't go into complete institutional collapse, we could see scalar harms that alter the way of life in the United States due to erosion of democracy.

Election misinformation also has a disproportionate impact on low-income communities and people of color. Hackers target them to suppress their vote and disenfranchise them in the process, perpetuating the negative impacts of systemic racism and income inequality and inhibiting change from easily occurring (Vandewalker).

Main players

Political candidates, election officials, anti-democratic actors

Strategy Considerations

While critical, democracy impacts are often difficult to explain in the context of a debate round. It is impossible to quantify a “decrease in democracy”, so teams must rely on other related quantifications such as inflation. Conversely, though, democracy can trump many other impacts on the affirmative side as it forms the foundation upon which every other institution rests. If the pro is making arguments about trust in government and privacy, how can individuals have trust in government and a democratic institution when the integrity of elections is compromised? The integrity of our elections is also a relevant, a hot-button issue in the wake of the 2016 and 2020 elections. Given the fact that election infrastructure is frequently targeted, the probability of this impact is also high when compared to other arguments on the topic, making it a good choice for a contention.

Evidence for Election Security

The United States is currently very prone to misinformation and interruptions to the election

Myre, Greg and Shannon Bond. "Russia Doesn't Have to Make Fake News': Biggest Election Threat is Closer to Home." *NPR*. 29 September 2020.

<https://www.npr.org/2020/09/29/917725209/russia-doesn-t-have-to-make-fake-news-biggest-election-threat-is-closer-to-home>

Q. What are the biggest concerns at this point about domestic disinformation? Shannon Bond: Security experts are warning that the atmosphere is ripe for disinformation, and there are a lot of false claims and rumors already circulating. That includes "everything from Qanon [a baseless conspiracy theory] to mobilizations to protest, COVID-19 conspiracies and then ultimately mail-in ballots and voter fraud," said Clint Watts, a former FBI special agent who tracks online security threats at the Foreign Policy Research Institute. Researchers and social media platforms say bad actors are capitalizing on the uncertainty created by the pandemic to confuse people about how to vote, undermine confidence in the election results and even threaten violence. In some cases, they say, would-be foreign meddlers need only amplify falsehoods being spread by U.S. social media users. "Russia doesn't have to make fake news. They just repeat what conspiracies are coming out of the White House and the administration," Watts said. Election watchers are particularly concerned about efforts to undermine confidence in voting – as President Trump has done repeatedly, with his tweets and Facebook posts claiming, falsely, that mail-in ballots are vulnerable to fraud.

The threat of ransomware attacks, specifically to the election, is very pressing

Varva, Shannon. "Election Interference Efforts Have Shifted, NSA and Cyber Command Election Threats Leads Say." *Cyberscoop*. 7 August 2020.

<https://www.cyberscoop.com/election-interference-2020-presidential-elections-nsa-cyber-command-russia-china/>

Bill Evanina, Director of the National Counterintelligence and Security Center, revealed Russia wants to "primarily denigrate ... Biden," while China "prefers that President Trump ... does not win reelection." The intelligence community has assessed "that Iran seeks to undermine ... President Trump, and to divide," Evanina added. Threats to U.S. elections don't stop with nation-state actors' social media operations.

Threats to U.S. elections don't stop with nation-state actors' social media operations. Ransomware threats to U.S. elections are so great, for instance, that the Election Security Group in recent months has expanded their focus to include those types of attacks, a U.S. government official told CyberScoop. Imbordino noted Friday he is concerned about ransomware, indicating that ransomware actors could – wittingly or unwittingly – contribute to possible election interference operations. "I think ransomware is one of those wild cards out there that could be wielded by anyone, criminal actors, etc.," Imbordino said. In the case that a ransomware attack does target any election infrastructure or networks, Imbordino expressed concern that malicious actors could seize the moment to make people distrust the election results. Imbordino said he is worried bad actors might spread disinformation suggesting that a ransomware attack could impact the tally of people's votes, even if that's not the case. "You can have a ransomware in a local network that actually doesn't even impact the election's counting," Imbordino said. "But someone could then spin an influence campaign from that and report it to make you think there has been an impact and then not trust the results." Moving forward, the NSA is continuing to monitor China's

threats to the election, primarily due to both the scope and depth of their capability, Imbordino said.

Election interference severely hinders democracy within the US

Henry, Shawn. "Election Security: Thwarting Disinformation and Interference in 2020." *Federal News Network*. 2 October 2020.

<https://federalnewsnetwork.com/commentary/2020/10/election-security-thwarting-disinformation-and-interference-in-2020/>

The upcoming U.S. presidential election cycle falls at a very unique time in our history. We knew coming into 2020 that we'd likely be facing adversaries attempting to influence our campaigns, elections and democracy as they did four years ago. I don't think anyone realized we'd also be dealing with a global pandemic or highly emotional protests on top of that. As troubling as this year has been for people around the world, and Americans in particular, it's pure gold for the enemy. Not only are they preying on our emotions and vulnerability during an especially difficult and unprecedented time, but they're also working in overdrive on ways to corrupt, undermine and remotely disrupt our daily lives. Information operations are nothing new. Disinformation, propaganda and attempts to manipulate public perception have been documented since some of the earliest records exist, morphing as new methods of communication emerged. First campaigns leveraged paintings, then cartoons, posters, pamphlets, films, radio and TV shows, and now they use the full global reach and impact of modern digital communications. In information warfare, nation states continue to deliver on the same goals as they did when dropping pamphlets by plane on soldiers during wartime – but with the anonymity, speed and scale now enabled by modern social media tools and the far-reach of the internet. What is new is the weaponization of content in an attempt to achieve the broadest societal impact via online influence operations, leaks and extortion. While cyber espionage has traditionally had a tremendous and negative impact on the global economy through the drain of intellectual property, the attacks we've witnessed on the election process and infrastructure further amplify those risks. These threats cut through the heart of the modern democratic process. As a former FBI official, I witnessed attacks as far back as 2008 on both the Obama and McCain presidential campaigns. It was espionage, plain and simple, to collect intelligence on the candidates' strategies and policies. The upcoming U.S. presidential election cycle falls at a very unique time in our history. We knew coming into 2020 that we'd likely be facing adversaries attempting to influence our campaigns, elections and democracy as they did four years ago. I don't think anyone realized we'd also be dealing with a global pandemic or highly emotional protests on top of that. As troubling as this year has been for people around the world, and Americans in particular, it's pure gold for the enemy. Not only are they preying on our emotions and vulnerability during an especially difficult and unprecedented time, but they're also working in overdrive on ways to corrupt, undermine and remotely disrupt our daily lives. Information operations are nothing new. Disinformation, propaganda and attempts to manipulate public perception have been documented since some of the earliest records exist, morphing as new methods of communication emerged. First campaigns leveraged paintings, then cartoons, posters, pamphlets, films, radio and TV shows, and now they use the full global reach and impact of modern digital communications. In information warfare, nation states continue to deliver on the same goals as they did when dropping pamphlets by plane on soldiers during wartime – but with the anonymity, speed and scale now enabled by modern social media tools and the far-reach of the internet. What is new is the weaponization of content in an attempt to achieve the broadest societal impact via online influence operations, leaks and extortion. While cyber espionage has traditionally had a tremendous and negative impact on the global economy through the drain of intellectual property, the attacks we've witnessed on the election process and infrastructure further amplify those risks. These threats cut through the heart of the modern democratic process. As a former FBI official, I witnessed attacks as far back as 2008 on both the Obama and McCain presidential campaigns. It was espionage, plain and simple, to collect intelligence on the candidates' strategies and policies. Insight by

Blackboard: Learn how the Coast Guard accelerated its approach to training and technology modernization due to the pandemic in this free webinar. Although adversary interventions during the 2018 midterm cycle appeared more muted than in the 2016 race, we should not assume that they will sit on the sidelines in 2020 and beyond. Election security leading up to November is key – a vital pillar to the health of the democratic process. Similarly, one of the main components of any reasonable cybersecurity program is the health of the system. Adversaries are looking to collect intelligence that will help them understand candidates in terms of policies, economic values and the like. And the security posture of the various electoral systems will determine the adversaries’ success. They will always use the path of least resistance to conduct a breach. They are patient, thorough, and take the time to learn and exploit vulnerabilities. We need to ask the most basic, albeit incredibly important, questions. How are electoral assets secured? How are the systems configured? What is the breakdown of access control? Is software and hardware patched? Are existing vulnerabilities identified and secured such that they can't be exploited? How is DNS traffic being filtered? How are campaigns preventing phishing operations among their staffers? The list of questions is simply too long to cover comprehensively here. Fortunately, it's promising that people now seem to recognize more than in prior years just how widely dispersed our electoral system and infrastructure is. But it is critical to execute on that knowledge and mitigate the risk – awareness must translate to action. I would argue that with the success of previous election interference events, there will be other nation states that use this vector as part of their toolset and electoral officials need to be cognizant of that. They have taken on the responsibility of administering the election system and must take that responsibility seriously. Their failure to protect the infrastructure could result in a failure in democracy. On a larger scale, it's also noteworthy that the U.S. is not the only country under attack by interference and disinformation campaigns. The reconnaissance and theft of intelligence related to electoral processes is a global issue against the majority of Western democratic operations. The growing threat that we first saw against our systems has now been replicated throughout the world in Taiwan, India, Finland, France, Israel, Germany, Ukraine and others. Globally, information and intelligence sharing on emerging threats, new technologies and fresh techniques is critical. We must look from country to country to determine adversary actions and attempt to stop them in their tracks. We know through CrowdStrike intelligence reporting that various state and federal agencies, educational institutions, and critical infrastructure sectors are actively being targeted by Russia-based adversaries, not unlike those that disrupted the 2016 election cycle. Through spear phishing, intrusion and password-spraying attacks, they're gaining access to systems vital to our daily lives. On top of this, the FBI is warning of malign foreign influence, defined as “operations by foreign powers to influence US policy, distort political sentiment and public discourse, or undermine confidence in democratic processes and values to achieve strategic geopolitical objectives.” This includes cyberattacks on election infrastructure and systems, campaigns, political parties, and acting public officials; subversive influence campaigns to either assist or harm a particular candidate or party; and overt disinformation operations and efforts to manipulate public opinion, sow discord and disrupt government processes and policies. I often use the age-old government mantra “one team, one fight.” It's never been more prevalent than now in this time of global cyber warfare. We have to unite against the adversary, protect our infrastructure, and be cognizant of who is reporting what we believe online. We cannot let our 2020 election cycle be the next cybercrime statistic and strip us of a fair and uncompromised voting experience that will determine the next four years of our history. Every second counts in defending our democracy.

The impact of decreased democracy

Doucouliaos, Hristos and Ulubasoglu, Mehmet Ali. “Democracy and Economic Growth: A Meta-Analysis.” *MPSA*. January 2008. <https://www.jstor.org/stable/25193797>

Despite a sizeable theoretical and empirical literature, no firm conclusions have been drawn regarding the impact of political democracy on economic growth. This article challenges the consensus of an inconclusive relationship through a quantitative assessment of the democracy-growth literature. It applies meta-regression analysis to the population of 483 estimates derived from 84 studies on democracy and growth. Using traditional meta-analysis estimators, the bootstrap, and Fixed and Random Effects meta-regression models, it derives several robust conclusions. Taking all the available published evidence together, it concludes that democracy does not have a direct impact on economic growth. However, democracy has robust, significant, and positive indirect effects through higher human capital, lower inflation, lower political instability, and higher levels of economic freedom. Democracies may also be associated with larger governments and less free international trade. There also appear to be country- and region-specific democracy-growth effects. Overall, democracy's net effect on the economy does not seem to be detrimental.

Hacking Primarily Targets Poor Communities of Color and Leads to Disenfranchisement

Vandewalker, Ian. “Digital Disinformation and Vote Suppression.” *Brennan Center for Justice*. 2 September 2020. <https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression>

There is a multitude of stories about attempts to trick certain people out of voting. These deceptive practices have often involved the use of flyers, mailers, and robocalls. For example, during Texas’s Super Tuesday primary in March 2020, robocalls falsely told voters that they could vote “tomorrow.” Similarly, in 2004, flyers distributed in Franklin County, Ohio, falsely told voters that Republicans should vote on Tuesday and Democrats on Wednesday due to high levels of voter registration. A related tactic is to intimidate voters with false reports of law enforcement presence, immigration enforcement actions, or election monitoring by armed individuals. These voter suppression tactics frequently target historically disenfranchised communities, including communities of color, low-income communities, and immigrant communities. For example, during Alabama’s U.S. Senate special election in 2017, residents of Jefferson County — where the largest city, Birmingham, is predominantly African American — received text messages with false information about polling site changes. And on Election Day in 2010, Maryland gubernatorial candidate Bob Ehrlich’s campaign manager targeted African American households with robocalls claiming that Governor Martin O’Malley had already been reelected, implying that his supporters could stay home instead of voting. Deceptive election practices are most commonly used in the last days before an election because they are presumably most effective if spread without time for rebuttal before voting begins. As a result, the scale and scope of voter suppression tactics for the 2020 election remain unknown, although recent history suggests disinformation will be a significant problem.

STOPPING IP THEFT

What's the argument?

One critical function of the NSA's mass surveillance is the identification and protection of US intellectual property. Intellectual property refers to intangible creations of the human intellect such as copyrights, patents, trademarks, and trade secrets. Corporations need intellectual property protected in order to have ownership over a product and security in their business. The NSA protects this property from hackers and more likely the Chinese government by monitoring vulnerabilities and suspicious activity. (Goldsmith).

This function is especially important because, in its absence, each cyber-attack could compound in its damage. In other words, each time a bad actor stole US intellectual property, they could steal ransomware that would allow them to inflict even more damage next time. Absent NSA protection, US businesses and innovation could be at the mercy of foreign governments.

Why does the argument matter?

IP theft inflicts an extraordinary amount of damage upon the US economy. Chinese theft alone costs the United States up to \$600 billion annually, with the average company losing \$101.9 million annually (Pham; Casey). Compounded over multiple years, this damage is a major hindrance on long term economic growth.

Main Players

US tech companies, foreign governments

Strategy Considerations

This argument, on paper, is one of the strongest on the negative side. It has straightforward warrants, tangible impacts, and intuitive logic. This makes it especially strategic for teams to lean heavily upon for their narrative in-round. The economic impacts function as the clearest, most straightforward path to the ballot when

compared to typical affirmative impacts like democracy and privacy. However, there are limited examples of the NSA actually being successful at preventing IP theft, which con teams will likely be quick to point out. Teams running this argument must be prepared to explain why that is and why it matters regardless.

Evidence for Stopping IP Theft

Surveillance necessary to prevent theft

Surveillance critical to preventing malware, intrusion, and theft

Goldsmith, Jack. "We Need an Invasive NSA." *The New Republic*. 10 October 2013.

<https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>

Such cyber-intrusions threaten corporate America and the U.S. government every day. "Relentless assaults on America's computer networks by China and other foreign governments, hackers and criminals have created an urgent need for safeguards to protect these vital systems," the Times editorial page noted last year while supporting legislation encouraging the private sector to share cybersecurity information with the government. It cited General Keith Alexander, the director of the NSA, who had noted a 17-fold increase in cyber-intrusions on critical infrastructure from 2009 to 2011 and who described the losses in the United States from cyber-theft as "the greatest transfer of wealth in history." If a "catastrophic cyber-attack occurs," the Times concluded, "Americans will be justified in asking why their lawmakers ... failed to protect them." The Times editorial board is quite right about the seriousness of the cyber- threat and the federal government's responsibility to redress it. What it does not appear to realize is the connection between the domestic NSA surveillance it

detests and the governmental assistance with cybersecurity it cherishes. To keep our computer and telecommunication networks secure, the government will eventually need to monitor and collect intelligence on those networks using techniques similar to ones the Times and many others find reprehensible when done for counterterrorism ends. The fate of domestic

surveillance is today being fought around the topic of whether it is needed to stop Al Qaeda from blowing things up. But the fight tomorrow, and the more important fight, will be about whether it is necessary to protect our ways of life embedded in computer networks. Anyone anywhere with a connection to the Internet can engage in cyber-operations within the United States. Most truly harmful cyber-operations, however, require group effort and significant skill. The attacking group or nation must have clever hackers, significant computing power, and the sophisticated software—known as "malware"—that enables the monitoring, exfiltration, or destruction of information inside a computer. The supply of all of these resources has been growing fast for many

years—in governmental labs devoted to developing these tools and on sprawling black markets on the Internet. Telecommunication networks are the channels through which malware typically travels, often anonymized or encrypted, and buried in the billions of communications that traverse the globe each day. The targets are the communications networks themselves as well as the computers they connect—things like the Times' servers, the computer systems that monitor nuclear plants, classified documents on computers in the Pentagon, the nasdaq exchange, your local bank, and your social-network providers. To keep these computers and

networks secure, the government needs powerful intelligence capabilities abroad so that it can learn about planned cyber-intrusions. It also needs to raise defenses at home. An

important first step is to correct the market failures that plague cybersecurity. Through law or regulation, the government must improve incentives for individuals to use security software, for private firms to harden their defenses and share information with one another, and for Internet service providers to crack down on the botnets—networks of compromised zombie computers—that underlie many cyber-attacks. More, too, must be done to prevent insider threats like Edward Snowden's, and to control the stealth introduction of vulnerabilities during the manufacture of computer components—vulnerabilities that can later be used as windows for cyber-attacks. And yet that's still not enough. The U.S. government can fully monitor air, space, and sea for potential attacks from abroad. But it has limited access to the channels of cyber-attack and cyber-theft, because they are owned by private telecommunication firms, and because Congress strictly limits government access to private communications. "I can't defend the country until I'm into all the networks," General Alexander reportedly told senior government officials a few months ago. For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation. It will also allow it to discern patterns of malicious activity in the swarm of communications, even when it doesn't possess the malware's signature. And it will better enable the government to trace back an attack's trajectory so that it can discover the identity and geographical origin of the threat. 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.

Impacts of IP Theft

IP theft by China costs the US hundreds of billions of dollars a year

Pham, Cherisse. "How Much Has the US lost from China's IP Theft?" *CNN*. 23 March 2018.
<https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html>

So just how much damage has it done? The United States Trade Representative, which led the seven-month investigation into China's intellectual property theft and made recommendations to the Trump administration, found that "Chinese theft of American IP currently costs between \$225 billion and \$600 billion annually." Those numbers are in line with a 2017 report from the Commission on the Theft of American Intellectual Property. Chinese officials have said that protecting foreign companies' intellectual property rights is important to China. But many of its companies appear to have missed that memo. "China has sought to acquire US technology by any means, licit or illicit," James Andrew Lewis, senior vice president at the Center for Strategic and International Studies in Washington, wrote in a blog post Thursday. "Espionage and theft were part of this, but so were forced technology transfers or mandatory joint ventures as a condition for doing business in China," he wrote. One of the most recent high profile examples of theft of US intellectual property happened earlier this year. In January, a Beijing-based wind turbine company was found guilty in the US of stealing trade secrets, using secretly downloaded source code stolen from a Massachusetts company. Forced technology transfer is also a growing concern for US companies, especially tech firms. To get an idea of how much forced technology transfer costs the US, some experts say to look at the costs associated with the theft of trade secrets. Total theft of US trade secrets accounts for anywhere from \$180 billion to \$540 billion per year, according to the Commission on the Theft of American Intellectual Property -- as "the world's principal IP infringer," China accounts for the most of that theft. Those numbers are likely to go up, as China doubles down on policies that could lead to acquisition of foreign technology and information -- like the controversial new cybersecurity law that went into effect last year. One of the most contentious parts of the law involves measures that allow China to conduct security reviews of technology products and services that could affect national security. Critics slammed the plans as intrusive and trade-inhibiting, and industry organizations, including the US Chamber of Commerce, say they are concerned over unfair advantages for Chinese companies and trade barriers. Beijing says the new law is meant to strengthen the protection of personal information and combat online fraud.

IP theft costs individual companies millions of dollars

Casey, Bob. "The Impact of Intellectual Property Theft on the Economy." *Report by the US Congress Joint Economic Committee Chairman's Staff*. August 2012.
https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf

Businesses often experience lost revenue and ultimately lower profits when sales are diverted from authentic goods to counterfeit ones. In addition to lower sales, profits are also adversely affected by the additional costs required to protect the firm from future episodes of intellectual property infringement. 8 One estimate found that the average company lost \$101.9 million in revenues and

incurred costs of \$1.4 million in identification and enforcement of intellectual property rights, leading to an average decline in profits of \$46.3 million.⁹

Recent government data help to shed light on the magnitude of foreign infringement. In 2011, the U.S. Customs and Border Protection seized 24,792 counterfeit or pirated goods, a 24.2 percent increase over the amount of goods seized in 2010.¹⁰ These seized goods represented more than \$1.1 billion in lost sales.¹¹ Availability of a counterfeit good can also put downward pressure on the price of the authentic product, causing a further decline in a firm's revenue. Additionally, a company's brand may be damaged when consumers who are unaware they have purchased a counterfeit good blame the maker of the genuine product for the poor-quality counterfeit they have bought.

A2 PRO

A2 BIG DATA COLLECTION

NSA surveillance is able to isolate previous hacking groups and bring them to justice to patch flaws and stop cybercriminals. For example, they warned of a serious flaw in an email software that was being exploited by Russian hackers and uncovered who was beyond the infamous Not Petya global cyber attack

Gazis, Olivia. "NSA warns of new cyberattacks by Russian military hackers." *CBS News*. 28 May 2020. <https://www.cbsnews.com/news/national-security-agency-cyberattack-sandworm-russia-hackers/>

A notorious hacking team backed by the Russian government has been exploiting a serious flaw in commonly used email software, the National Security Agency (NSA) warned Thursday, issuing a rare advisory that publicly attributed attempts to utilize the software flaw to a nation-state actor. The NSA's Cybersecurity Directorate said a group of cyber actors known as "Sandworm team" from the GRU, Russia's military intelligence agency, had identified and exploited a vulnerability in the popular email software Exim Mail Transfer Agent (MTA) since at least August 2019. "The Russian actors ... have used this exploit to add privileged users, disable network security settings, execute additional scripts for further network exploitation; pretty much any attacker's dream access – as long as that network is using an unpatched version of Exim MTA," the advisory said. The agency advised users to immediately update the software and warned that any outdated versions would likely remain vulnerable to attack. "When the patch was released last year, Exim urged its users to update to the latest version. NSA adds its encouragement to immediately patch to mitigate against this still current threat," it said. Sandworm is known to have operated for at least a decade and has been linked to large-scale cyberattacks on government, energy and telecommunications sectors in Ukraine and Poland, as well as on NATO and the European Union. The group was determined to be behind the devastating 2017 NotPetya attacks, which caused billions of dollars of damage across Europe, the United States and Asia. In February, the State Department publicly blamed Sandworm for a widespread cyberattack on government and private websites in the country of Georgia.

NSA surveillance and intelligence capabilities are necessary to prevent cyber intrusions that steal intellectual property and innovation from corporations. They work to build up cybersecurity.

Goldsmith, Jack. "We Need an Invasive NSA." *The New Republic*. 10 October 2013. <https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>

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. 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.

A2 INTELLECTUAL PROPERTY AND INNOVATION

NSA surveillance techniques create new programs and cyber security advances that become high-tech innovation. They have more than 70 technologies in their portfolio that they open to the private sector.

Polit, Kate. "NSA Opens More of its 'Hot Tech' to the Private Sector." *MeriTalk*. 21 March 2019. <https://www.meritalk.com/articles/nsa-opens-more-of-its-hot-tech-to-private-sector/>

The National Security Agency is broadening the menu of technologies it wants to help the private sector develop. The agency's Technology Transfer Program (TTP) recently added several new patents to its TTP portfolio, through which industry and entrepreneurs can license the patents for further innovation. But this year, NSA is framing its offering as a list of "hot technologies" available for licensing, in an apparent effort to spur further participation. Licensing a TTP patent can help a company attract funding, hire new people, and look to increase its market share. The NSA, for its part, gets its piece of the licensing pie while allowing private-sector innovation to improve on the technologies. NSA now has more than 70 technologies listed in its portfolio, broken down under the categories of Data Science, Cyber, Internet of Things and Mobile. The vast majority of them have a heavy national security element, which you would expect from the agency known (if not in great detail) for its covert work in cybersecurity, encryption, and signals intelligence. But the agency has said it tries to be proactive in recognizing opportunities for industry to develop new products. The agency since 2005 (when it released Security Enhanced Linux) also has been sharing open-source software via its GitHub page. Quite a few of the portfolio technologies reflect ongoing projects the Intelligence Community and the Department of Defense have been working on in other projects as well. One of several involving translation, for instance, focuses on recognizing speech in any language through a technology that currently converts the phonetic sounds of speech in about 15 languages into text. The Intelligence Advanced Research Projects Activity (IARPA) in early 2018 launched a multi-year project to develop a similar universal translator project, though with the idea of converting text in any language to English. Some of the other technologies on the list include digital camera fingerprinting, analyzing similarities in datasets, rapid biometric authentication, face recognition, wideband signal geolocation, antenna designs, and technologies that detect tampering with such things as courier bags and even manhole covers—the latter being a way to help protect access to telecom and utility services, and defend against infrastructure attacks. All of them have national security implications, of course, but could be applied as well in the commercial sector. Many of them, such as face recognition, already are in wide use but have plenty of room for improvement. NSA's patents plus an infusion of private sector innovation could move the ball forward.

The NSA helps protect corporations from IP theft by exposing weaknesses in software. For example, they recently discovered and

released a major flaw in Microsoft's operating system to close potential backdoors for hackers.

Nakashima, Ellen. "NSA found a dangerous Microsoft software flaw and alerted the firm – rather than weaponize it." *Washington Post*. 14 January 2020.

https://www.washingtonpost.com/national-security/nsa-found-a-dangerous-microsoft-software-flaw-and-alerted-the-firm--rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html

The National Security Agency recently discovered a major flaw in Microsoft's Windows operating system – one that could potentially expose computer users to significant breaches or surveillance, and alerted the firm to the problem rather than turn it into a hacking weapon, according to people familiar with the matter. The disclosure represents a major shift in the NSA's approach, choosing to put computer security ahead of building up its arsenal of hacking tools that allow the agency to spy on adversaries' networks, according to the people familiar with the matter who spoke on condition of anonymity because of the sensitivity of the matter. . "Big kudos to NSA for voluntarily disclosing to Microsoft," said computer security expert Dmitri Alperovitch in a tweet Tuesday morning. "This is the type of [vulnerability] I am sure the [NSA hackers] would have loved to use for years to come." The vulnerability – essentially a mistake in the computer code – affects the Windows 10 operating system, which is the most widely used today, according to the people who were briefed on the matter. The discovery has been likened to a slightly less severe version of the Microsoft flaw that the NSA once weaponized by creating a hacking tool dubbed EternalBlue, which one former agency hacker said was like "fishing with dynamite." The NSA used EternalBlue for more than five years, but when it learned that the tool had been obtained by others, it alerted Microsoft, which issued a patch in early 2017. About a month later, Shadow Brokers, a suspected Russian hacking group, released the NSA tool online.

Corporations have been encrypting their data to protect their property – they are solving the problem themselves.

Shackford, Scott. "Big Corporations Band Together to Fight the Government's Secrecy in Collecting Citizen." *Reason Magazine*. 6 September 2016.

<https://reason.com/blog/2016/09/06/big-corporations-band-together-to-fight/print>
Microsoft filed suit against the Department of Justice in April, arguing that gags prohibiting them from telling customers they've had their data taken by government officials are unconstitutional, violating both the Fourth Amendment rights of their customers and the First Amendment rights of Microsoft. But they're not fighting alone. A whole bunch of corporations from across the spectrum have just announced their support. It's not just tech companies and tech privacy activists, as we've seen in some cases (like the Apple encryption fight). As Reuters notes, we're talking about a wide-ranging group of companies that includes the Washington Post, Delta Air Lines, pharmaceutical company Eli Lilly, the U.S. Chamber of Commerce, and Fox News. There are even five

former federal law enforcement officials supporting Microsoft's position.

A2 SOFT POWER / INTERNATIONAL RELATIONS

Our soft power is already on the decline from other, more notable reasons than the NSA

Handley, Lucy. "The US is the world's top 'soft' power – but Trump has damaged its reputation, survey says." *CNBC*. 25 February 2020. <https://www.cnn.com/2020/02/25/the-us-is-the-worlds-top-soft-power-but-trump-has-damaged-its-reputation.html>

The U.S. is seen as a global force in terms of its "soft power" and influence, despite controversy around President Trump's administration, which has damaged the country's reputation, according to new research. The Global Soft Power Index, by consultancy Brand Finance, surveyed more than 50,000 consumers in 87 countries to rank countries in terms of their familiarity, reputation and influence, among other measures. The U.S. came in top, with Germany, the U.K., Japan and China following. France, Canada, Switzerland, Sweden and Russia make up the rest of the top 10. The term "soft power" was coined by political scientist Joseph Nye in the late 1980s and relates to a nation's ability to attract or persuade other nations, rather than coerce using military or economic means. But while the U.S. was ranked highly by respondents in terms of its influence in entertainment, media, sport and science, its reputation, governance and political stability are seen less positively by people around the world. "The mixed international reception of controversies surrounding President Trump's administration is likely to be the reason behind relatively low ratings for reputation," the report authors noted. The U.S. came 13th for reputation, 13th for ethical standards, 19th for political standards and 44th for relations with other countries. People also ranked it low for climate action (28th) and trustworthiness (23rd), according to the study, published Tuesday. "This is perhaps understandable given America's decisions to unilaterally pull out of the Paris Agreement on climate change and the Joint Comprehensive Plan of Action on Iranian nuclear policy, undermining the nation's reliability as a partner on the world stage," the report stated. Trump's impeachment trial also had an impact, according to David Haigh, chair and CEO of Brand Finance, but other measures helped it to the top spot. "Soft power cannot be rapidly achieved, nor lost. The United States has shown that ultimately, despite the reputational challenges of impeachment and unpredictable foreign policy, its position as the rule-maker in the international system ... is unrivalled," Haigh said in a release. A spokesperson for the White House was not immediately available for comment when contacted by *CNBC*. Like the U.S., China and Russia rank higher for influence than for reputation. China is ranked as the world's second-most influential country but comes in at 24th for reputation. Russia ranks 7th for influence and 26th for reputation. "China and Russia are the nexus of change for global political, economic, and social world order. Western democracies can no longer rely on the end-of-history assumption that liberal values have won globally and have to adapt to a world shared with these new colossal soft power players," the report states. Despite leaving the European Union, the U.K.'s reputation appears undented, due in part to the importance of Queen Elizabeth II, its standing in media (which the report attributes to the BBC's reputation) and culture. Peter Fisk, professor of leadership and strategy at Madrid's IE Business School, said that soft power is likely to continue to have an impact on nations, describing it as "meta power." "Meta power is not about having the largest army, it is about having the best story," he stated in the report.

The NSA and other US surveillance organizations help other countries with anti-terrorism efforts which means other countries do not hate it entirely

“The Use of the Internet for Terrorist Purposes.” *The United Nations*. September 2012.

https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.

For example, a “honey pot” jihadist website reportedly was designed by the [Central Intelligence Agency] and Saudi Arabian Government to attract and monitor terrorist activities. The information collected from the site was used by

intelligence analysts to track the operational plans of jihadists, leading to arrests before the planned attacks could be executed. However, the website also was reportedly being used to transmit operational

plans for jihadists entering Iraq to conduct attacks on U.S. troops. Debates between representatives of the [National Security Agency, Central Intelligence Agency, Department of Defense, Office of the Director of National Intelligence and National Security Council] led to a determination that the threat to troops in theater was greater than the intelligence value gained from monitoring the website, and a computer network team from the [Joint Task Force- Global Network Operations] ultimately dismantled it.¹³² As illustrated in the above case, coordination between agencies is an important factor in successfully responding to identified threats.²²⁹ Other Member States, such as the United Kingdom, have indicated that significant emphasis has been

placed on developing working relationships and entering into memorandums of understanding between the prosecution and law enforcement or intelligence agencies, with positive results. Similarly, in Colombia, the Integrated Centre of Intelligence and Investigation (Centro Integrado de Inteligencia e Investigación, or CI3) is the domestic agency that coordinates investigations into suspected terrorist activities using a strategy based on six pillars. This approach involves a high-ranking official from the national police assuming overall command and control of different phases of the investigation, which include the gathering, verification and analysis of evidence and a judicial phase in which police collect information on parties and places associated with the commission of any crimes.¹³³

US diplomacy is not as much of a function of the signals we send without domestic policy and more so deals with leverage and coercion. This comes from the Pentagon and the US military standing, and, in part, the NSA itself

Rubin, Michael. “Why was John Kerry such a bad Secretary of State?” *AEI*. 29 December

2016. <https://www.aei.org/publication/yes-mr-president-there-is-an-alternative-to-the-iran-deal/>

Rather than exploit Iran’s desperation, Kerry worked to alleviate it: The Obama administration offered Iran billions of dollars just to come to the table. Nor did Kerry (or Obama) once enunciate what the best alternative to a negotiated agreement was, leading his Iranian counterparts to conclude correctly that they had the upper hand in talks. After all, if Obama and Kerry castigated their critics as warmongers, then how likely were they to join their critics if they believed war the only alternate? Can Kerry alone be blamed? No: US strategy has been incoherent across administrations. Secretaries of State might opine but if there is no unity of effort to ensure that their diplomacy is set up to succeed, then it won’t be successful. The State Department cannot alone build leverage –

that is the job of the Pentagon and perhaps Central Intelligence Agency and should be coordinated by the National Security Council. Kerry’s problem was ego: Perhaps it was his decades immersed in the culture of the Senate,

but he seems to have come to believe that his own good faith and rhetoric could substitute for the hard work of crafting coherent strategy. Essentially, his tenure was one giant short-cut. He worked hard, but not effectively. Staff and close advisors who might have offered him a reality check instead recognized that their path to recognition and promotion was to affirm whatever Kerry thought, no matter how destructive or, in some case, factually challenged it could be. Kerry, himself, has always been handicapped by his credulity: He believes what he is told. His adversaries understand that personal charm can lead Kerry to dismiss the accumulated wisdom of those more experienced or knowledgeable than he. Diplomacy that diverges from reality is seldom successful. Kerry did not live in the real world. Nor does

diplomacy absent leverage ever work with adversaries or rogue regimes. It is a lesson Kerry never learned, and history will condemn him for it. He has left the United States and its allies in a far worse position than had he done nothing.

There is no impact to a decrease in soft power. Other countries are so heavily dependent on the US, for example with trade, that they will always continue to work with us

United States Trade Representative. "Countries and Regions." *Executive Office of the President*. 2020. <https://ustr.gov/countries-regions>

The United States is the world's largest trading nation, with over \$5.6 trillion in exports and imports of goods and services in 2019. The U.S. has trade relations with more than 200 countries, territories, and regional associations around the globe. Goods Exports

The United States is the 2nd largest goods exporter in the world. U.S. goods exports to the world totaled \$1.6 trillion in 2019, down 1.4 percent (\$22.5 billion) from 2018.

Canada was the largest purchaser of U.S. goods exports in 2019, accounting for 17.8 percent of total U.S. goods exports. The top five purchasers of U.S. goods exports in 2019 were: Canada (\$292.6 billion), Mexico (\$256.6 billion), China (\$106.4 billion), Japan (\$74.4 billion), and the United Kingdom (\$69.1 billion). U.S. goods exports to the European Union 27 were \$267.6 billion. Goods Imports The United States is the largest goods importer in the world. U.S. goods imports from the world totaled \$2.5 trillion in 2019, down 1.6 percent (\$40.2 billion) from 2018. China was the top supplier of goods to the United States, accounting for 18 percent of total goods imports. The top five suppliers of U.S. goods imports in 2019 were: China (\$452 billion), Mexico (\$358 billion), Canada (\$319 billion), Japan (\$144 billion), and Germany (\$128 billion). U.S. goods imports from the European Union 27 were \$515 billion. Services Exports The United States is the largest services exporter in the world. In 2019, U.S. exports of services were \$875.8 billion, up 1.6 percent (\$13 billion) from 2018. U.S. exports of services account for 35 percent of overall U.S. exports in 2019. The United Kingdom was the largest purchaser of U.S. services exports in 2019 accounting for nearly 9 percent of total U.S. services exports. The top five purchasers of U.S. services exports in 2019 were: the United Kingdom (\$78.3 billion), Canada (\$67.7 billion), Ireland (\$57.5 billion), China (\$56.5 billion), and Japan (\$50.0 billion). U.S. services exports to the European Union 27 were \$200.3 billion. Services Imports The United States is the largest services importer in the world. In 2019, U.S. imports of services were \$588.4 billion, up 4.7 percent (\$26.3 billion) from 2018. The United Kingdom was the largest supplier of services, accounting for 11 percent of total U.S. service imports in 2019. The top five suppliers of U.S. services imports in 2019 were: the United Kingdom (\$62.3 billion), Canada (\$38.5 billion), Japan (\$35.8 billion), Germany (\$34.9 billion), and Mexico (\$29.8 billion). U.S. services imports from the European Union 27 were \$145.9 billion

A2 HUMAN RIGHTS / PRIVACY

The real data privacy concern stems from big technology giants, not government surveillance programs, because regardless data privacy remains a large problem

Mahida, Om. "It's 2020 and we still have a data privacy problem." *The Next Web*. 25 January 2020. <https://thenextweb.com/podium/2020/01/25/its-2020-and-we-still-have-a-data-privacy-problem/>

Today, as consumers in the US, we do not have any right to own or manage our data. Companies whose products or services we use on a daily basis use our data and sell it to advertisers. This data can include anything from your full name and address to who you are friends with as well as your full Google search history. There's even evidence that DMVs in the US sell information such as addresses and age to advertisers. All of this without our explicit permission. Over the past two decades, our data has become a gold mine for corporations. When corporations have to choose between protecting user data and maximizing profits, they'll choose profits every time (they have to – it's their duty to shareholders!). It is only through external pressures that a change can be enacted. There are few citizens in the community that are taking a proactive approach towards data privacy, while others continue to try and exploit consumer data. The current legal framework does not sufficiently protect consumer rights at an institutional level, instead relying on individual behavior to 'opt-in' or not. Even when signing up for a service and given the chance to read the terms and conditions, there is no plausible way to limit the exposure of personal data. In reality, the only way to keep your data to yourself is to avoid operating in mainstream society, something that is nearly impossible today.

Corporations and individuals fight back against NSA surveillance by filing lawsuits, encrypting data, and creating barriers so the government cannot access it

Shackford, Scott. "Big Corporations Band Together to Fight the Government's Secrecy in Collecting Citizen." *Reason Magazine*. 6 September 2016.

<https://reason.com/blog/2016/09/06/big-corporations-band-together-to-fight/print>
Microsoft filed suit against the Department of Justice in April, arguing that gags prohibiting them from telling customers they've had their data taken by government officials are unconstitutional, violating both the Fourth Amendment rights of their customers and the First Amendment rights of Microsoft. But they're not fighting alone. A whole bunch of corporations from across the spectrum have just announced their support. It's not just tech companies and tech privacy activists, as we've seen in some cases (like the Apple encryption fight). As Reuters notes, we're talking about a wide-ranging group of companies that includes the Washington Post, Delta Air Lines, pharmaceutical company Eli Lilly, the U.S. Chamber of Commerce, and Fox News. There are even five former federal law enforcement officials supporting Microsoft's position.

Courts have already restricted the NSA's surveillance that infringes on individual privacy as unconstitutional, so it is not that much of an issue

Holmes, Aaron. "The NSA phone-spying program exposed by Edward Snowden didn't stop a single terrorist attack, federal judge finds." *Business Insider*. 2 September 2020.

<https://www.businessinsider.com/nsa-phone-snooping-illegal-court-finds-2020-9>

The National Security Administration's sweeping program to snoop on Americans' phone records was illegal and possibly unconstitutional – and there's no evidence it led to the arrests of any terrorism suspects – a federal appeals court ruled Wednesday.

In its ruling, the 9th Circuit Court of Appeals said the NSA broke the law by collecting "phone metadata," or bulk records of Americans' phone-call history. The court upheld the convictions of four Somali immigrants who were charged with fundraising for terrorists, however, concluding that the NSA's phone-record collection was ultimately not relevant to their convictions. The NSA's program to collect phone records was first brought to light by the former NSA contractor Edward Snowden in 2013. Amid public outrage following the revelation, the agency defended the program by claiming it had helped thwart terrorist attacks.

Even if individual privacy is violated, there has been no tangible harm to citizens since the NSA's inception, so there is no real impact to these operations

Hertzberg, Hendrik. "The N.S.A., the 'Encroaching Police State,' and the System." *The New Yorker*. 9 July 2013.

<https://www.newyorker.com/news/daily-comment/the-n-s-a-the-encroaching-police-state-and-the-system>

Yes, I did say that the N.S.A.'s data-collection-and-mining program appears to have been conducted lawfully, i.e., within the letter of the law. Whether I'm right or wrong on that point, I probably should have mentioned Kinsley's Law of Scandals: "The scandal isn't what's illegal.

The scandal is what's legal." **But I truly don't think we're living under an encroaching police state. I still don't know of a single instance where the N.S.A. data program has encroached on or repressed any particular person's or group's freedom of expression or association in a**

tangible way. Nor have I come across a clear explanation of exactly how the program could be put to such a purpose. But even if the program could be misused in that way, for it to happen you would have to have a malevolent government—or, at least, a government with a malevolent, out-of-control component or powerful official or officials. You would have to have a Nixon or a J. Edgar Hoover. But when you have a government or a powerful government official bent on repression and willing to out the law, there are always plenty of tools at hand. Nixon and Hoover didn't need data mining to do their mischief—and, again, I haven't seen an explanation of how data mining would have helped them do worse than they did.

A2 DEMOCRACY

Instead of a chilling effect, the NSA leaks in 2013 created significant backlash and a movement that strengthened data privacy. In 2014, the US passed the Freedom Act to trim back the NSA and it gave rise to outspoken groups like QAnon that are anything but silent

Johnson, Lock, Richard Aldrich, and Christopher Moran. “An INS Special Forum: Implications on the Snowden Leaks.” *Intelligence and National Security*. 2014.

<https://doi.org/10.1080/02684527.2014.946242>

In 2013, the National Security Agency (NSA) in the United States became embroiled in controversy – again. Its questionable use of wiretaps (Operation MINARET) and its improper reading of international cables sent and received by Americans over decades (Operation SHAMROCK) had been revealed by the Church Committee in 1976; and in 2005 the New York Times disclosed that the NSA had been wiretapping selected American citizens without a warrant, contrary to the Foreign Intelligence Surveillance Act of 1978. Central to

the debate stood the question of whether or not Snowden was a patriot for disclosing to the public a questionable intelligence program or a traitor for his unauthorized

disclosure of classified information – much of it going beyond the metadata program that he claimed had justified his

actions. The retiring NSA Director, General Keith B. Alexander, called the Snowden leaks ‘the greatest damage to our combined nations’ intelligence systems that we have ever suffered’. In contrast, his replacement in 2014, Admiral Michael S. Rogers, deplored the leaks but downplayed their damage, saying that there was no indication ‘the sky is falling’.¹The Times had noted earlier that none of the secret

agencies had presented ‘the slightest proof that his disclosures really hurt the nation’s security’.² In June 2014, the US House

enacted legislation – the USA Freedom Act – to trim back on the breath of the NSA

metadata program, although not to ban it altogether. The Senate was expected to take up the measure in summer 2014. Shortly before the House passed the bill, the editors of *Intelligence and National Security* asked some members of its Editorial Board to comment on the implications of the Snowden leaks. I would like to take this opportunity to thank the participants for their thoughtful contributions, under a short deadline. Below, in alphabetical order, are their responses.

Gurman, Hannah. “QAnon is just the latest in a long line of right-wing conspiracy theories.”

Washington Post. 15 August 2018. <https://www.washingtonpost.com/news/made-by-history/wp/2018/08/15/qanon-is-just-the-latest-in-a-long-line-of-right-wing-conspiracy-theories/>

However, for followers of Q, collectively known as QAnon, he is a heroic truth teller. Q claims to have the highest level of security clearance in the Department of Energy, which means he has access to the deepest secrets of the state. In the interest of advancing the greater good, he discloses this information to the public. In short, he claims to be a whistleblower. In the popular imagination, national security whistleblowers are generally thought to be antiwar liberals – Daniel Ellsberg, the Rand analyst who exposed a top-secret historical study of U.S. policymaking in Vietnam (later dubbed the Pentagon Papers) and more recently,

Chelsea Manning and Edward Snowden, whose disclosures fueled a left-leaning

disenchantment with the national security state. Why? The history of whistleblowing on the far right is one in

which conspiracy theorists who advanced the agenda of the far right were celebrated as whistleblowers, while whistleblowers

who threatened that agenda were discredited as conspiracy theorists, effectively

blurring the lines between the two. This problem was exacerbated by the mainstream

press's refusal to take legitimate accusations against the national-security state seriously, leading it to focus instead on the backgrounds and personal foibles of whistleblowers. In this context, the rise of Q represents a perfectly logical next chapter in the longer story of right-wing whistleblowing: Why not just invent a deep-state whistleblower out of whole cloth? Why bother to ground his claims in any evidence? If history is any guide, the nonbelievers won't believe anyway. And the true believers will believe no matter what.

Big data hurts the democratic process more than NSA surveillance because the collection of behavioral metadata removes the need to use polls and surveys to determine public opinion, eliminating the voluntary civic participation needed for a strong democracy

Howard, Phillip. "Internet of Things World – Is the Internet of Things Your New Constitution?" *University of Oxford*. 11 September 2015.

https://www.imgigi.com/amp/Download_Documents_PDF_Free_amp2.php?Download_PDF_courses=870

The Internet of Things as a Mechanism of Political Participation The politics of the future will be guided by a new power paradigm. Whoever controls the largest device networks will get the most sensor data, and hence will manage the largest number of connections between and among

people and devices. As more of the things we manufacture are powered and networked, "inanimate" objects will be replaced by devices that talk with our other devices. They will communicate with their original manufacturer, the information services we subscribe to, national security agencies, contractors, cloud computing services, and anyone else in the data stream. They will work the behavioral data they have assembled and with algorithms—the script of our new constitution—mete out capacities and constraints on our political lives.

Subsequently, civic engagement will increasingly become involuntary. None of us will have the opportunity to opt-out of the behavioral data collection that generates public policy. The

basis of a democracy is voluntary civic engagement. A person's participation in setting government policy is intentional and a matter of choice. In democracies, citizens express their preference through activism and voting. Historically, governments and huge record-keeping projects like the census. Politicians have long tried to interpret citizen intent and manipulate it through rhetoric and campaign tricks. But pervasive device networks will change the rules, making voluntary conversations among elected politicians eager to interpret (and manipulate) citizen intent also relied on opinion polls, conversations with civic groups, social science research, a officials, political parties, lobbyists and civic groups less important than the plethora of near-perfect data generated by the objects around us. Activism and petition-signing will be overshadowed by volumes of behavioral information cleverly extracted from the Internet of Things. 8 This information will be of incalculable value. It will inform firms of consumer habits, enlighten governments as to the needs of citizens, and reveal the whims of voters to politicians. Political lobbying isn't a new sport, but the Internet of Things is going to be a game-changing resource for lobbyists. The more a lobbyist knows about the behavior of voters and donors, the easier it is to activate and organize those people on clients' behalf. Furthermore, smart data mining will cost good money, which will place it out of the reach of many civic groups, scientists and journalists. Hence, society's watchdogs [who] will not be able to use this data to check on what big political players are doing with this megadata. It is also

important to realize that governance systems don't just involve states: they appear whenever a powerful actor can set some rules and restrictions on people's behavior. For example, Uber has ordered its drivers to stay away from protests in China, and it has a way to enforce the rule: they will use drivers' cellphones to track car location and cancel the contracts of violators. Though Uber's policy is a business decision, this rule has the political implication of cutting off a transportation option for Chinese citizens who want to help reform their government.

The bigger problem destroying democratic participation in government is our unresponsive political machinery and lack of political efficacy, not government surveillance

Hertzberg, Henrik. "The N.S.A., the "Encroaching Police State," and the System." *The New Yorker*. 9 July 2013. <https://www.newyorker.com/news/daily-comment/the-n-s-a-the-encroaching-police-state-and-the-system>

More alarming than the reach of the N.S.A. program is the composition of the Foreign Intelligence Surveillance Court, the panel of federal judges that is supposed to oversee that program and which, the Times reported last week, "has quietly become almost a parallel Supreme Court." All eleven of the fisa court's members were chosen by John Roberts, the Chief Justice of the actual Supreme Court. Like Roberts himself, ten of the eleven are Republican, and conservative, appointees. The composition of both Supreme Courts, the actual and the parallel, is a direct consequence of the 5-4 decision in *Bush v. Gore*, the judicial coup d'état that installed George W. Bush as President thirteen years ago. The real danger to civic trust (and ultimately, perhaps, to our freedoms) is the calcification and unresponsiveness of our political and governmental machinery. The post-2000 Supreme Court is part of that long, sad story. So is the filibuster, which is a bigger threat to small-d democratic governance than the N.S.A., the C.I.A., and the I.R.S. put together. The same goes for the electoral-college status quo; the built-in, and increasing, malapportionment of the Senate; and the malapportionment of the House, both deliberate, via gerrymandering, and demographic, via population patterns. These structural horrors don't make us a police state, encroaching or otherwise. But they do enable minorities—usually conservative, mostly monied minorities—to systematically thwart the will of the majority. They don't necessarily require anybody to act in bad faith in order to do their damage. And they damage not just people's faith in democracy but democracy itself.

A2 CON

A2 STOPPING TERRORISM

The NSA cannot logistically sift through the vast amount of information to be able to track down domestic terrorists.

Adams, Nick. "Counterterrorism since 9/11: Evaluating the Efficacy of Controversial Tactics." *Breakthrough Institute*. Spring 2011. <https://thebreakthrough.org/articles/counterterrorism-since-9-11>

The expansion of investigative and surveillance powers after 9/11 appears to compound the challenges faced by security and intelligence agencies by increasing the amount of informational 'noise' they must filter out to detect terrorist 'signals.' Signal detection, not

intelligence-gathering, failed in the run-up to 9/11 and in the case of the would-be Christmas Day bomber. Policies allowing for easy surveillance of people who have little reason to be suspected of terrorism have flooded security agencies with informational noise and generated thousands of false leads that distract them from real threats. These signal detection failures are reflected in data on the numbers of cases the FBI has recommended for DOJ prosecution. Despite a several-fold increase in the use of expanded search and surveillance tools, the FBI is generating far fewer cases for prosecution than they did in 2002 and many more of them are being declined by the DOJ because they lack evidence of wrongdoing.

Finding terrorists via mass surveillance is a probabilistic impossibility.

Rudmin, Floyd.. "The Politics of Paranoia and Intimidation." *University of Tromso, Norway*. 26 May 2006. <https://www.lewrockwell.com/2006/05/floyd-rudmin/the-politics-of-paranoia-andintimidation/>

In addition, however, mass surveillance of an entire population cannot find terrorists. It is a probabilistic impossibility. It cannot work. What is the probability that people are terrorists given that NSA's mass surveillance identifies them as terrorists? If the probability is zero ($p=0.00$), then they certainly are not terrorists, and NSA was wasting resources and damaging the lives of innocent citizens. If the probability is one ($p=1.00$), then they definitely are terrorists, and NSA has saved the day. If the probability is fifty-fifty ($p=0.50$), that is the same as guessing the flip of a coin. The conditional probability that people are terrorists given that the NSA surveillance system says they are, that had better be very near to one ($p=1.00$) and very far from zero ($p=0.00$). To know if mass surveillance will work, Bayes' theorem requires three estimations: 1. The base-rate for terrorists, i.e. what proportion of the population are terrorists; 2. The accuracy rate, i.e., the probability that real terrorists will be identified by NSA; 3. The misidentification rate, i.e., the probability that innocent citizens will be misidentified by NSA as terrorists. No matter how sophisticated and super-duper are NSA's methods for identifying terrorists, no matter how big and fast are NSA's computers, NSA's accuracy rate will never be 100% and their misidentification rate will never be 0%. That fact, plus the extremely low base-rate for terrorists, means it is logically impossible for mass surveillance to be an effective way to find terrorists.

NSA Surveillance system is overloaded with false positives

Bialik, Carl. "Ethics Aside, Is NSA's Spy Tool Efficient?". *Wall Street Journal*. 14 June 2013. <https://www.wsj.com/articles/SB10001424127887324049504578543542258054884>

A Ph.D. candidate in computational ecology wrote on his blog last week that even a very accurate algorithm for identifying terrorist communications could produce about 10,000 false positives for every real "hit," creating a haystack of false leads to chase in order to find every needle.

Several media reports repeated the figure, and some experts agreed. "The false positives will kill you in this kind of system," said Bruce Schneier, a security technologist at U.K. telecommunications company BT Group PLC.

False positives distract attention and resources away from helpful counterterrorism efforts.

Adams, Nick. "Counterterrorism since 9/11: Evaluating the Efficacy of Controversial Tactics." *Breakthrough Institute*. Spring 2011. <https://thebreakthrough.org/articles/counterterrorism-since-9-11>

While unnecessary informational noise poses a challenge to the detection of genuine terrorist signals, false signals actually distract attention and resources away from helpful CT efforts. To prevent the pursuit of false leads, states – for centuries – have regulated the ability of law enforcement to conduct searches and surveillance. If evidentiary thresholds for attaining investigative warrants are set too low (or eliminated entirely), agents may, intentionally or not, pursue more weak leads than they would with stricter oversight. Expansive investigative powers threaten security and undermine state legitimacy if they distract the attention and resources of security agencies, encourage the harassment of innocents, or allow the guilty to go free. Our review of news accounts and government reports has uncovered evidence that expanded search and surveillance tools after 9/11 increased informational noise and the pursuit of false signals.

PATRIOT ACT provisions allowed the FBI to collect more and more information about people without demonstrating sufficient (or in many cases, any) cause for suspicion. Between the years 2000 and 2008, the issuance of National Security Letters (NSLs) – demands sent to companies to secretly gather financial and communications transactional information about individuals without their knowledge – increased over fivefold to 50,000 per year (Dept. of Justice 2007).¹⁴ The number of FISA warrants sought and approved also doubled over the period to 2,400 (Electronic Privacy Info. Center 2008). And, the number of Suspicious Activity Reports (SARs), which are secret reports to the Treasury Department made by U.S. banks about their customers, grew six-fold to 1,250,000 by 2007 (Dep. of Treasury 2008). (Meanwhile, the number of FBI agents working on terrorism only doubled.) With so much information being collected, one might think that the number of terrorism cases also increased dramatically over the period. However, the number of cases prosecuted by the DOJ dropped significantly from its post- 9/11 high of 355 in 2002, to 34 in 2008 (the latest year for which data were available at the time of printing). Those numbers may reflect prosecutorial overzealousness in 2002 and/or a steady decline in the number of individuals engaged in terrorist activity over the period. In any case, the enhanced information gathering powers of the FBI did not seem to result in higher quality case files for prosecution. While in 2001, DOJ prosecutors declined only 33 percent of the terrorism cases the FBI referred for prosecution, in 2002 that declination percentage rose to 54%. By 2006, the DOJ rejected 87% of the terrorism cases the FBI referred for prosecution (Transactional Records Access Clearinghouse 2006).

There is no credible evidence that the NSA has ever stopped a terrorist attack using mass surveillance information

van Dongen, Teun. "The NSA Isn't Foiling Terrorist Plots." Leiden University. 8 October 2013. <https://fpif.org/nsa-isnt-foiling-terrorist-plots/>

It might be tempting to give the NSA the benefit of the doubt, given that the organization speaks on the basis of information that we do not have. But such dubious claims about the effectiveness of the digital surveillance programs fit seamlessly into a pattern of misinformation and deceit. The U.S. government acknowledged the existence of PRISM only after Edward Snowden had leaked details about it to The Guardian. Moreover, when the news broke, President Obama and Director of National Intelligence James Clapper tried to downplay the scale of the digital data gathering, even though we know now that the NSA is essentially making a back-up of pretty much all conceivable forms of online communication. President Obama further promised that "nobody is listening to your phone calls," but it later became clear that the NSA can access the content of phone calls and emails if it so desires. Congressional oversight is poor, privacy rules are frequently broken, and the NSA liberally shares data with other intelligence agencies and foreign governments. Against this background of disputed or outright false government claims, the public is wise to be skeptical of the NSA's claims about the effectiveness of the digital surveillance programs. The recent revelations may be mind-boggling in their technological, legal, and procedural complexities, but the bottom line is

quite simple: The first credible piece of evidence that these programs are doing any good in the fight against terrorism has yet to surface. Until such evidence is provided, the Obama administration is only eroding the trust of the citizens it is claiming to protect.

Mass surveillance infrastructure tends to make terrorism worse off because it pushes terrorist groups to the dark web that push operations underground

Bershidsky, Leonid. "U.S. Surveillance is Not Aimed at Terrorists." *Bloomberg*. 23 June 2013. <http://www.bloomberg.com/news/2013-06-23/u-s-surveillance-is-not-aimed-at-terrorists.html>

"People who radicalise under the influence of jihadist websites often go through a number of stages," the Dutch report said. "Their virtual activities increasingly shift to the invisible Web, their security awareness increases and their activities become more conspiratorial."

Radicals who initially stand out on the "surface" Web quickly meet people, online or offline, who drag them deeper into the Web underground. "For many, finally finding the jihadist core forums feels like a warm bath after their virtual wanderings," the report said. When information filters to the surface Web from the core forums, it's often by accident. Organizations such as al-Qaeda use the forums to distribute propaganda videos, which careless participants or their friends might post on social networks or YouTube. The infrastructure set up by the National Security Agency, however, may only be good for gathering information on the stupidest, lowest-ranking of terrorists. The Prism surveillance program focuses on access to the servers of America's largest Internet companies, which support such popular services as Skype, Gmail and iCloud. These are not the services that truly dangerous elements typically use. Similarly, monitoring phone calls is hardly the way to catch terrorists. They're generally not dumb enough to use Verizon.

Granted, Russia's special services managed to kill Chechen separatist leader Dzhokhar Dudayev with a missile that homed in on his satellite-phone signal. That was in 1996. Modern-day terrorists are generally more aware of the available technology. At best, the recent revelations concerning Prism and telephone surveillance might deter potential recruits to terrorist causes from using the most visible parts of the Internet. Beyond that, the government's efforts are much more dangerous to civil liberties than they are to al-Qaeda and other organizations like it.

A2 DISCOVERING ESPIONAGE

The NSA makes espionage easier by making the internet less secure by installing backdoors in technological products

Zetter, Kim. "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA." *Wired Magazine*. 24 September 2013. <http://www.wired.com/threatlevel/2013/09/nsa-backdoored-and-stole-keys/>

These methods, part of a highly secret program codenamed Bullrun, have included pressuring vendors to install backdoors in their products to allow intelligence agencies to access data, and obtaining encryption keys by pressuring vendors to hand them over or hacking into systems and stealing them. Most surprising, however, is the revelation that the agency has worked to covertly undermine the encryption standards developers rely upon to build secure products. Undermining standards and installing backdoors don't just allow the government to spy on data but create fundamental insecurities in systems that would allow others to spy on the data as well. "The encryption technologies that the NSA has exploited to enable its secret dragnet surveillance are the same technologies that protect our most sensitive information, including medical records, financial transactions, and commercial secrets," Christopher Soghoian, principal technologist of the ACLU's Speech, Privacy and Technology Project, said in a statement about the revelations. "Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance. The NSA's efforts to secretly defeat encryption are recklessly shortsighted and will further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies."

The internet being insecure puts the public at risk and threatens our ability to conduct investigation in times of danger

Brewster, Tom. "Has the NSA's mass paying made life easier for digital criminals?" *The Guardian*. 7 March 2014. <https://www.theguardian.com/technology/2014/mar/07/nsa-spying-harmed-digital-crime-fight>

Cross-border data-sharing mechanisms - a critical part in both online and non-internet crime investigations - have come under threat since the Edward Snowden leaks. Even though information-sharing deals covering banking and airline passenger data just about survived calls to suspend them, the Snowden files have caused problems for collaboration between public and private bodies. The heightened tensions lie not between law enforcement agencies, but between police and other organisations that potentially hold valuable information for investigations. "The impact is more [with] third parties giving more consideration to sharing their data with agencies or other departments," said Charlie McMurdie, formerly the head of the defunct Metropolitan Police Central e-Crime Unit and now senior crime adviser at PricewaterhouseCoopers. "This can have a negative impact on law enforcement ability to respond to or progress investigations, but on the positive side [this] has also made third parties think more about where their data exists, security and sharing protocols, which isn't a

bad thing.” A recent European Commission report on trust between the US and the EU following the leaks last year said: “Information sharing is ... an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed.” Discussions are ongoing about an umbrella agreement covering law enforcement data sharing, with much talk of the need to ensure safeguards are in place, with “strict conditions”. The US government has already seen the impact. In response to a Guardian question on the effect of Snowden’s revelations on data sharing, Phyllis Schneck, the chief cybersecurity official at the US Department of Homeland Security, said the government body’s partners were “feeling it”. She said the data sharing environment had to be improved if the nation was to protect against people who wanted “to change and hurt our way of life”. “It’s so important to be able to combine what we know... We all have to make sure we get this right and we will, with full privacy and full civil rights,” Schneck said during a panel at the conference. Steven Chabinsky, former deputy assistant director for the FBI’s Cyber Division and now general counsel for offensive security firm Crowdstrike, said the information sharing problems that had emerged “have to be resolved”. Criminals learning from NSA Intelligence agency hacking techniques will also be adopted by criminals, according to security luminaries speaking with The Guardian. This has been seen in other nations in recent history. “The spear-phishing tricks we saw the Chinese secret police using against the Dalai Lama in 2008 were being used by Russian crooks to steal money from US companies by 2010. We predicted as much in ... 2009,” said Ross Anderson, professor of security engineering at the University of Cambridge. “A lot more people have become aware of what can be done.”

The US’ actions of spying on their citizens encourages countries like Russia and China to ramp up their efforts and do the same.

Wadhwa, Tarun. “NSA Surveillance May Have Dealt Major Blow To Global Internet Freedom Efforts.” Forbes. 13 June 2013.

<https://www.forbes.com/sites/tarunwadhwa/2013/06/13/with-nsa-surveillance-us-government-may-have-dealt-major-blow-to-global-internet-freedom-efforts/?sh=184846cf5ada>

The government has used peculiar interpretations of laws - that they are not even willing to discuss - to defend an invasive collection of personal data beyond anything even the paranoid among us would have thought was possible. And while President Obama “welcomes the debate” over an issue he has worked hard to keep secret, we are now starting to see the usual Washington tactics of political spin, feverish scapegoating, and patriotic grandstanding in lieu of a real discussion. **We should all be extremely concerned about the colossal surveillance infrastructure that is being built in the name of our safety.** In trying to reassure the public, our leaders have told us that these programs are not meant to target us, but instead, foreigners who may pose a threat to our security. But this is merely a decision on how the data is being used today - we are getting into very dangerous territory by hoping for the best intentions of whoever is in power in the future. American history holds many lessons for us here: circumstances can change, the perception of who is a threat can vary with whoever is in office, and we cannot predict what our political situation will look like decades, or even years, from now. **In the court of global public opinion, America may have tarnished its moral authority to question the surveillance practices of other nations - whether it be Russia on monitoring journalists, or China on conducting cyber espionage. Declarations by the State Department that were once statements of principle now ring hollow and hypocritical to some. No nation can rival the American surveillance state, but they no longer need support to build their own massive systems of espionage and oppression. The costs of surveillance and data storage technologies are plummeting -- these will no longer be prohibitive factors.** Diplomatic pressures and legal barriers that had also once served as major deterrents will soon fade away. The goal has been to promote internet freedom around the world, but we may have also potentially created a blueprint for how authoritarian governments can store, track, and mine their citizens’ digital lives.

A2 CYBER ATTACKS

NSA surveillance put backdoors of entry in technology for them to enter

Zetter, Kim. "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA." *Wired Magazine*. 24 September 2013. <http://www.wired.com/threatlevel/2013/09/nsa-backdoored-and-stole-keys/>

These methods, part of a highly secret program codenamed Bullrun, have included pressuring vendors to install backdoors in their products to allow intelligence agencies to access data, and obtaining encryption keys by pressuring vendors to hand them over or hacking into systems and stealing them. Most surprising, however, is the revelation that the agency has worked to covertly undermine the encryption standards developers rely upon to build secure products. Undermining standards and installing backdoors don't just allow the government to spy on data but create fundamental insecurities in systems that would allow others to spy on the data as well. "The encryption technologies that the NSA has exploited to enable its secret dragnet surveillance are the same technologies that protect our most sensitive information, including medical records, financial transactions, and commercial secrets," Christopher Soghoian, principal technologist of the ACLU's Speech, Privacy and Technology Project, said in a statement about the revelations. "Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance." The NSA's efforts to secretly defeat encryption are recklessly shortsighted and will further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies."

These backdoors make cyber attacks easier for criminals, terrorists, and foreign hackers because they can use those existing backdoors

Peha, Jon M. "The Dangerous Policy of Weakening Security to Facilitate Surveillance". *Carnegie Mellon University. Office of the US Director of National Intelligence*. 4 October 2013. http://users.ece.cmu.edu/~peha/Peha_on_weakened_security_for_surveillance.pdf

Individual computer users, large corporations, and government agencies all depend on the security features built into information technology products and services that they buy on the open market. If the security features of these widely available products and services are weak, everyone is in greater danger. There have recently been allegations that U.S. government agencies have engaged in a number of activities deliberately intended to weaken this widely available technology. Weakening commercial products and services does have the benefit that it becomes easier for U.S. intelligence agencies to conduct surveillance on targets who use the weakened technology, and if it is occurring, this is probably the motivation. However, this strategy also inevitably makes it easier for criminals, terrorists, and foreign powers to infiltrate these systems for their own purposes. Moreover, everyone who uses this technology is vulnerable, and not just the handful who may be surveillance targets for U.S. intelligence agencies. No government agency should act to reduce the security of a product or service sold on the open market without first conducting a careful risk assessment.¹ If the recent allegations in the press are correct, and no such risk assessment occurred, the White House should make sure that a thorough review is conducted now, and that policies are changed as needed based on this assessment.

NSA surveillance erodes trust and destroys public-private partnerships which is necessary to improve cyber security and prevent cyber attacks

Nakashima, Ellen. "NSA tries to regain industry's trust to work cooperatively against cyberthreats." *Washington Post*. 10 October 2013.

http://www.washingtonpost.com/world/national-security/nsa-tries-to-regain-industrys-trust-to-work-cooperatively-against-cyber-threats/2013/10/09/93015af0-2561-11e3-b3e9-d97fb087acd6_print.html

A drop in Americans' trust in the government is making the difficult task of public-private cooperation against cyber-threats even more difficult. And that has officials such as Gen. Keith B. Alexander, director of the National Security Agency, scrambling to shore up confidence in his agency, whose image has taken a beating in the wake of leaks about its surveillance programs by former NSA contractor Edward Snowden. At public hearings and in speeches, Alexander, who also heads the U.S. Cyber Command, is warning that cyberattacks on such critical and technology-dependent industries as energy, finance and transportation can be prevented only if those industries work with the government. But companies are wary of partnering with an agency that has been revealed to be conducting far-reaching domestic data collection in the name of thwarting terrorism. "Industry is critical to resolving our problems" in cybersecurity, Alexander said at the Billington Cybersecurity Summit last month at the National Press Club. The scale of the data collection stunned Americans, said Paul Tiao, former senior counselor to the FBI director who is a partner at Hunton & Williams. "I don't think a lot of people thought they had all that information. The NSA has been trying to overcome that ever since." Companies have long been sensitive to the implications of sharing data with the government, fearing harm to their reputations and potential lawsuits for privacy and other violations, Tiao said. "The Snowden disclosures have made companies more careful about what they might share with the government because they know that the public is that much more concerned about it." And restoring confidence, experts say, depends on how meaningful the government's surveillance reforms are.

The United States has an incredible advantage in cyberspace because we have some of the strongest cybersecurity to prevent attacks. The chance an attack creates even a marginal impact is extremely unlikely.

Lindsay, Jon R. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *University of California, San Diego*. 27 October 2015.

http://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf

The existence of high-reward targets in cyberspace is a large part of what makes the cyber threat narrative compelling. Critical infrastructure and command and control systems are increasingly interconnected and, in principle, they are vulnerable to attack. The prevalence of attacks against low-reward targets by well-disguised attackers makes these high-reward targets appear to be all the more vulnerable. Yet appearances are misleading. The reality is that, although the technical possibility of

attacks against high-reward targets can never be ruled out, the probability of a successful attack against a high-reward target is quite low. High-reward targets pose greater risks and costs to those that attack them. If the attacker cannot be sure that its anonymity is secure or the attacker has doubts that its malware will execute as intended (and without unwanted collateral damage or fratricide) or that its resources will not be wasted, then the benefits of attacking a target must be sharply discounted. The asymmetric actors featured in cybersecurity discourse—rogue states, lone hackers, criminals, and terrorists—will tend to focus on the low-risk, low-reward bonanza and avoid deception-dominant high-risk, high-reward operations. Advanced industrial states will also partake in low-risk, low-reward espionage and harassment in cyberspace. Capable countries will, however, employ risky computer network attacks against lucrative targets only when they are willing and able to follow them up or backstop them with conventional military power. Because intelligence is costly and its exploitation is complicated, wealthier and larger states tend to have more sophisticated, robust intelligence capacities. Only capable actors, such as major powers, are likely to be able to master the complex tango of deception and counter-deception necessary to execute high-intensity operations. Powerful actors have an operational advantage in cyberspace. Even then, the frequency of complex and risky action should still be relatively low. One type of cyber threat inflation, therefore, is the attempt to represent cyberspace as categorically offense dominant when there may in fact be relatively affordable defenses. Doomsday scenarios such as a “cyber Pearl Harbor” are useful in the pursuit of bureaucratic resources and autonomy. The potential for deception in cyberspace thus fosters a more politically motivated form of deception. Deception-prone environments increase the risk of threat inflation. A state that believes it is in an offense-dominant world may invest more in military and intelligence resources than is necessary or pursue capabilities of the wrong or suboptimal type. Yet if offense dominance does not apply to the most important targets—since they are protected by complexity and deception—then over-arming and sowing fear are wasteful and destabilizing. Resources that could be allocated elsewhere will instead be expended for unnecessary security measures. Such efforts might even interfere with economically productive aspects of the Internet. There is also the potential for tragedy if officials hastily resort to aggression in the mistaken belief that relations are fundamentally unstable. The disaster of 1914, when great powers rushed headlong into costly deadlock, reflected, in part, the impact of a mistaken “ideology of the offensive” applied inappropriately to what clearly turned out to be a defense-dominant reality.⁸⁸

A2 ELECTION SECURITY

Information uncovered by the NSA could be misused for malicious intent by government officials to manipulate elections.

Friedersdor, Connor. "The Surveillance State Puts U.S. Elections at Risk of Manipulation."

The Atlantic. 7 November 2013. <https://www.theatlantic.com/politics/archive/2013/11/the-surveillance-state-puts-us-elections-at-risk-of-manipulation/281232/>

Why do I doubt Romney was treated unfairly? Because I doubt Obama would have dared order it, and because the prospect of a Romney victory didn't threaten either the NSA nor a contractor like Booz Allen Hamilton nor the national-security state generally. There was reason to believe he'd have been friendlier to them than Obama! The scenario I worry about most isn't actually another Richard Nixon type in the Oval Office, though that could certainly happen. What I worry about actually more closely resembles Mark Felt, the retired FBI agent exposed 32 years after Watergate as Deep Throat **—that is, I worry more about people high up inside the

national-security state using their insider knowledge to help take down a politician. Is part of the deference they enjoy due to politicians worrying about that too? Imagine a very plausible 2016 presidential contest in which an anti-NSA candidate is threatening to win the nomination of one party or the other—say that Ron Wyden is challenging Hillary Clinton, or that Rand Paul might beat Chris Christie. Does anyone doubt where Keith Alexander or his successor as NSA director would stand in that race? Or in a general election where an anti-NSA candidate might win? What would an Alexander type do if he thought the victory of one candidate would significantly rein in the NSA with catastrophic effects on national security? Would he really do nothing to prevent their victory? I

don't know. But surely there is some plausible head of the NSA who'd be tempted to use his position to sink the political prospects of candidates antagonistic to the agency's

interests. And we needn't imagine something so risky and unthinkable as direct blackmail. Surveillance-state defenders will want to jump in here and insist that there are already internal safeguards and congressional oversight to prevent the abuses I am imagining. But I don't buy it. It isn't just that I can't help but think Alexander could find a way to dig up dirt on politicians if he wanted to without it ever getting out to overseers or the public. Forget about Alexander. Let's think about someone much lower in the surveillance state hierarchy:

Edward Snowden. As we know, Snowden broke protocol and violated his promise to keep classified information secret because his conscience demanded it: He believed that he was acting for the greater good; his critics have called him a

narcissist for taking it upon himself to violate rules and laws he'd agreed to obey. It isn't hard to imagine an alternative world in which the man in Snowden's position was bent not on reforming the NSA, but on thwarting its reformers—that he was willing to break the law in service of the surveillance state, fully believing that he was acting in the best interests of the American people. A conscience could

lead a man that way too. This Bizarro Edward Snowden wouldn't have to abscond to a foreign country with thousands of highly sensitive documents. He wouldn't have to risk his freedom. Affecting a U.S. presidential election would be as easy as quietly querying Rand Paul, or Ron Wyden, or one of their close associates, finding some piece of damaging information, figuring out how someone outside the surveillance state could plausibly happen upon that information, and then passing it off anonymously or with a pseudonym to Politico, or The New York Times, or Molly Ball. Raise your hand if you think that Snowden could've pulled that off. And if you were running for president, or senator, even today, might you think twice about mentioning even an opinion as establishment friendly as, "Hey, I'm all for NSA surveillance, but I don't trust a private contractor like Booz Allen Hamilton to do it"? Maybe safeguards put in place since the first Snowden leak would prevent a Bizarro Edward Snowden with strong Booz loyalties from targeting you. Maybe. Why risk it? In yet another

scenario, the NSA wouldn't go so far as to use information obtained through surveillance to affect an election. But they'd use it to their advantage to thwart the reform agenda of the candidate they didn't like if he or she won. And maybe the NSA would be as horrified by this sort of thing as I am. But maybe one of their contractors is on the payroll of a foreign government, and that person wants to affect a presidential election by exploiting the unprecedented amounts of data that the surveillance state has collected and stored on almost everyone. American democracy could be subverted in all sorts of hypothetical ways. Why worry about this one in particular? Here's the general standard I'd submit as the one that

should govern our thinking: If a powerful institutional actor within government has a strong incentive to do something bad, the means to do

it, and a high likelihood of being able to do it without getting caught, it will be done eventually. The NSA has the incentive. At least as recently as the Snowden leaks, an unknown number of its employees or contractors had the means. And many informed observers believe abuse undetected by overseers could be easily accomplished. If this particular abuse happened, it would be ruinous to self-government.

Let's fix this before it causes a scandal even bigger than Watergate—or permits behavior more scandalous than Watergate that is never uncovered, rectified or punished.

Violations have already begun, and it only is matter of time before they escalate

Nakashima, Ellen. “FBI and NSA violated surveillance law privacy rules, a federal judge found.” *The Washington Post*. 4 September 2020.

https://www.washingtonpost.com/national-security/fbi-and-nsa-violated-surveillance-law-or-privacy-rules-a-federal-judge-found/2020/09/04/b215cf88-eec3-11ea-b4bc-3a2098fc73d4_story.html

Two of the nation’s largest surveillance agencies repeatedly violated either the law or related court orders in incidents reported last year despite training on the procedures set up to protect the privacy of U.S. persons, a federal judge found. The FBI flouted the law and the National Security Agency ignored a rule to safeguard civil liberties when these agencies gathered or searched emails and other communications gathered from U.S. tech and phone companies, under a statute designed to produce foreign intelligence, ruled Judge James E. Boasberg, presiding judge of the Foreign Intelligence Surveillance Court, in a significant opinion made public Friday. “It should be unnecessary to state that government officials are not free to decide for themselves whether or to what extent they should comply with court orders.”

Boasberg wrote in the December 2019 opinion. The 83-page partially redacted ruling by Boasberg was released by the Office of the Director of National Intelligence. It focused on whether to approve a new set of rules enabling the FBI, NSA and CIA to continue collecting and searching millions of communications gathered from American companies under a law known as “Section 702” of the Foreign Intelligence Surveillance Act. Passed in 2008 and renewed in 2017, the law is the most potent power Congress has granted U.S. spy agencies to gather intelligence on everything from terrorism to nuclear proliferation to foreign adversaries’ plans and intentions. Because of its reach, and the potential to scoop up innocent Americans’ communications, Congress and the courts have imposed rules on how the government can collect and use the data.

A2 STOPPING IP THEFT

NSA surveillance makes the problem worse by indirectly giving cyber tools to US adversaries. China reverse engineered the NSA's hacking tools to conduct its cyberattacks on the United States and around the world, tapping millions of private communications

Perlroth, Nicole and David Sanger. "How Chinese Spies Got the NSA's Hacking Tools, and Used Them for Attacks." *New York Times*. 6 May 2019.

<https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html>

Chinese intelligence agents acquired National Security Agency hacking tools and repurposed them in 2016 to attack American allies and private companies in Europe and Asia, a leading cybersecurity firm has discovered. The episode is the latest evidence that the United States has

lost control of key parts of its cybersecurity arsenal. Based on the timing of the attacks and clues in the computer code, researchers with the firm Symantec believe the Chinese did not steal the code but captured it from an N.S.A. attack on their own computers — like a gunslinger who grabs an enemy's rifle and starts blasting away. The Chinese action shows how proliferating cyberconflict is creating a digital wild West with few rules or certainties, and how difficult it is for the United States to keep track of the malware it uses to break into foreign networks and attack adversaries' infrastructure. The losses have touched off a debate within the intelligence community

over whether the United States should continue to develop some of the world's most high-tech, stealthy cyberweapons if it is unable to keep them under lock and key. The

Chinese hacking group that co-opted the N.S.A.'s tools is considered by the agency's analysts to be among the most dangerous Chinese contractors it tracks, according to a classified agency memo reviewed by The New York Times. The group is responsible for numerous attacks on some of the most sensitive defense targets inside the United States, including space, satellite and nuclear propulsion technology makers. Now that nation-state cyberweapons have been leaked, hacked and repurposed by American adversaries, Mr. Chien added, it is high time that nation states "bake that into" their analysis of the risk of using cyberweapons — and the very real possibility they will be reassembled and shot back at the United States or its allies. In the latest case, Symantec researchers are not certain exactly how the

Chinese obtained the American-developed code. But they know that Chinese intelligence contractors used the repurposed American tools to carry out cyberintrusions in at least five countries or territories: Belgium, Luxembourg, Vietnam, the Philippines and Hong Kong. The targets included scientific research organizations, educational institutions and the computer networks of at least one American government ally. One attack on a major telecommunications network may have given Chinese intelligence officers access to hundreds of thousands or millions of private communications. Symantec said. Symantec did not

explicitly name China in its research. Instead, it identified the attackers as the Buckeye group, Symantec's own term for hackers that the Department of Justice and several other cybersecurity firms have identified as a Chinese Ministry of State Security contractor operating out of Guangzhou. Because cybersecurity companies operate globally, they often concoct their own nicknames for government intelligence agencies to avoid offending any government; Symantec and other firms refer to N.S.A. hackers as the Equation group. Buckeye is also referred to as APT3, for Advanced Persistent Threat, and other names.

The NSA's stealing of Chinese intellectual property ruined negotiations back in 2015 that would have stopped China from sponsoring US IP theft and ruined trust between the two powers

Eckert, Paul. "Snowden affair blunts US push for China to curb cyber theft." *Reuters*. 8 July 2013. <https://www.reuters.com/article/us-usa-china-cyber/snowden-affair-blunts-u-s-push-for-china-to-curb-cyber-theft-idUSBRE96713220130709>

Snowden's disclosures of American electronic surveillance around the world give China an argument to counter U.S. complaints that it steals private intellectual property (IP) from U.S. companies and research centers. Cyber security is at the center of high-level talks between the two countries in Washington that will show whether a positive tone struck by President Barack Obama and new Chinese President Xi Jinping at a summit last month can translate into cooperation on difficult issues.

Top U.S. officials, from Obama down, have long tried to convince China to recognize a clear line between the kind of cyber espionage by spy agencies revealed by Snowden and the theft of technology. "This Snowden thing has muddled the waters in a terrible way," said James McGregor, author of a book on China's authoritarian capitalism and industrial policy. Last week the U.S. Department of Justice charged Chinese wind turbine maker Sinovel Wind Group Co and two of its employees with stealing software source code from U.S.-based AMSC worth \$800 million. The U.S. Chamber of Commerce hopes "to see a clear indication that China recognizes thefts of trade secrets, whether by cyber or other means, is stealing property and will bring the full force of its laws to curb this," said Jeremie Waterman, the group's senior director for Greater China.

Beijing parries complaints about Chinese hacking into the computers of U.S. businesses by saying China is itself a major victim of cyber espionage. Chinese officials have dismissed as

unconvincing recent U.S. official and private-sector reports attributing large-scale hacking of American networks to China.

China's official Xinhua news agency said last month the Snowden case showed the United States was "the biggest villain in our age" and a hypocrite for complaining about Chinese cyber attacks. On Tuesday, the Communist Party's People's Daily attacked the United States for a hypocritical internet policy of defending hacking in the name of national security when it suited Washington's purposes. "Differentiating hacking attacks as 'good' and 'bad' is a double standard when it comes to internet security," the newspaper's overseas edition said in a front page comment.

China's stance seems to be stiffened by Snowden's revelations of widespread surveillance by the National Security Agency and his assertion that the agency hacked into critical network infrastructure at

universities in China and Hong Kong. Snowden fled to Hong Kong before his leaks to newspapers became public last month, and then went to Moscow, where he is believed to be holed up in the transit area of the Sheremetyevo airport, trying to find a country to give him sanctuary.

The best way to prevent intellectual property theft is to bridge the public-private divide among technology and security information,

Lyngas, Sean. "NSA official: Foreign hackers have 'pummeled' US by stealing IP."

Cyberscoop. 5 September 2018. <https://www.cyberscoop.com/george-barnes-nsa-us-china-ip-theft/>

The U.S. intelligence community has in recent weeks ratcheted up its public warnings that intellectual property theft is a risk to national security.

In July, the National Counterintelligence and Security Center released a report detailing persistent efforts by China, Iran, and Russia to steal U.S. trade secrets. NCSC Director William Evanina said then that China had not been honoring a 2015 agreement to refrain from economic espionage, pointing to multiple indictments of Chinese nationals in recent years. In addition to concerns over intellectual property, U.S. officials have sought to warn companies about what they say are the broader national security risks of doing business with Chinese telecom companies Huawei and ZTE, and Russian antivirus vendor Kaspersky Lab. U.S. officials worry Beijing and Moscow could leverage those companies to spy on Americans,

an allegation the companies deny. For Barnes, the key to better defending U.S. trade secrets from hackers is to share threat information across “the public-private divide.” “Our [threat] information is no good unless we can get it into the hands of critical infrastructure” as well as government personnel defending federal networks, he said.

The NSA drives private companies to encrypt data and prevent government cooperation

Whittaker, Zack and Danny Chrichton. “Should tech giants slam the encryption door on the government?” *TechCrunch Magazine*. 22 January 2020.

https://techcrunch.com/2020/01/22/should-tech-giants-slam-the-encryption-door-on-the-government/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMFdgayVVJDDIJZy4wBmr088npFi7a3EM37rmsxCQZD6ybATnl-8aLAylmH7IA4vSHBVfR9wxui--MKCYBMdb0U25KFdEQdmWyzd2hFe3GijX3EZupEUPFbpZyOQr7u0-EfYHSRjFbX4ygNt_RrElViwELRmMw4D3PXYprKPa6V

Zack: Tech companies are within their rights – both legally and morally – to protect their customers’ data from any and all adversaries, using any legal methods at their disposal. Apple is a great example of a company that doesn’t just sell products or services, but one that tries to sell you trust – trust in a device’s ability to keep your data private. Without that trust, companies cannot profit. Companies have found end-to-end encryption is one of the best, most efficient and most practical ways of ensuring that their customers’ data is secured from anyone, including the tech companies themselves, so that nobody other than the owner can access it. That means even if hackers break into Apple’s servers and steal a user’s data, all they have is an indecipherable cache of data that cannot be read. But the leaks from last decade which revealed the government’s vast surveillance access to their customers data prompted the tech companies to start seeing the government as an adversary – one that will use any and all means to acquire the data it wants. Companies are taking the utilitarian approach of giving their customers as much security as they can. That is how you build trust – by putting that trust directly in the hands of the customer.

INDICTS TO PRO EVIDENCE

A2 HOLMES AND KIRKPATRICK

“Freedom and Growth”, Higher Democratic Index Scores Increase GDP by 2%¹⁴

This study would be used to impact PRO arguments about government surveillance to the economy. While the warrant about whether or not NSA leaks hurt corporations, the stock market, or other economic aspects are up for debate, this study does not do a great job of establishing causality between democratic rankings and GDP. First of all, this study is from 1998 using data from 1980-1993, more than 30 years ago with completely different geopolitical environments. Nowadays, the US democratic index score has dropped to a flawed democracy all the while economic growth boomed during the early Trump administration¹⁵. Finally, this study concludes that democracies have 2% higher GDP rates when they compare entire democratic countries to authoritarian ones. Comparing two completely different countries' economies and saying the GDP difference is due to faith in democracy is baseless and unwarranted. To say perceptions of democracy have such severe economic trade-offs requires a lot more proof than this study offers.

Lynn-Jones, Sean M. “Why the United States Should Spread Democracy.” *Belfer Center*. March 1998. <https://www.belfercenter.org/publication/why-united-states-should-spread-democracy>

Why do democracies perform better than autocracies over the long run? Two reasons are particularly persuasive explanations. First, democracies-especially liberal democracies-are more likely to have market economies, and market economies tend to produce economic growth over the long run. Most of the world's leading economies thus tend to be market economies, including the United States, Japan, the “tiger” economies of Southeast Asia, and the members of the Organization for Economic Cooperation and Development. Two recent studies suggest that there is a direct connection between economic liberalization and economic performance. Freedom House conducted a World Survey of Economic Freedom for 1995-96, which evaluated 80 countries that account for 90% of the world's population and 99% of the world's wealth on the basis of criteria such as the right to own property, operate a business, or belong to a trade union. It found that the countries rated “free” generated 81% of the world's output even though they had only 17% of the world's population.³⁷ A second recent study confirms the connection between economic freedom and economic growth. The Heritage Foundation has constructed an Index of Economic Freedom that looks at 10 key areas: trade policy, taxation, government intervention, monetary policy, capital flows and foreign investment, banking policy, wage and price controls, property rights, regulation, and black market activity. **It has found that countries classified as “free” had annual 1980-1993 real per capita Gross Domestic Product (GDP) (expressed in terms of purchasing power parities) growth rates of 2.88%.** In “mostly free” countries the rate was 0.97%, in “mostly not free” ones -0.32%, and in “repressed” countries -1.44%.³⁸ Of course, some democracies do not adopt market economies and some autocracies do, but liberal democracies generally are more likely to pursue liberal economic policies.

¹⁴ Holme, Kim and Melanie Kirkpatrick. “Freedom and Growth.” *Wall Street Journal*. 16 December 1996. <https://www.wsj.com/articles/SB850499195576337000>

¹⁵ Rueckert, Phineas. “The United States is Now Considered a ‘Flawed Democracy’: Report.” *Global Citizens*. 26 January 2017. <https://www.globalcitizen.org/fr/content/the-us-is-now-a-flawed-democracy/>

A2 GOODWIN

Pen America, 1/6 Writers Self-Censor because of NSA surveillance¹⁶

This study is referenced in several others as one of the strongest pieces of evidence supporting the chilling effect. However, it is full of generalizations that are not as broad-based. First of all, the only writers that this study surveys are institutional PEN America writers that are disproportionately aware and concerned about government surveillance given that it is a free expression think tank. Secondly, the survey was taken directly after the Snowden leaks, so it is not immune to the response that the chilling effect has largely dissipated with the onset of social media and outspoken free speech movements. Thirdly, concluding that 1/6 self-censor is also a mischaracterization because the survey only ever indicated reluctance to write or search certain things, not the complete omission of subjects from literature. The full methodology can be found in the footnoted paper. Overall, the findings of this study are often overblown and don't really indicate any large-scale impact.

¹⁶ Goodwin, Peter. "Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor." *Pen America*. 12 November 2013. https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

A2 PENNY

UC Berkley, NSA's Chilling Effect on Online Activity¹⁷

This is a breakthrough study that offers many insights on NSA surveillance as well as the history of regulatory chilling effects in the United States. Even though Penney concludes a significant almost 20% drop in online activity after the Snowden leaks, the main problem with this study is the time frame that it looks at. It only analyzes Google and Wikipedia searches up until August of 2014, not at all close to a long-term trend. Internet activity picked up back to normal pace in a few months after the Snowden incident faded away from the public eye, which just goes to show how insignificant NSA surveillance really is when it comes to free speech.

Penney, Jonathon. "Chilling Effects: Online Surveillance and Wikipedia Use." *UC Berkeley Technology Law Journal*. 2016.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

Notwithstanding the significance of this case study's findings and their attendant implications, they have important limitations. First, the period of the study only extends until August 2014. This means that the persistence of any chilling effects beyond that point remains an open question. Though the findings here suggested a long-term, even permanent, chilling effect, this possibility cannot be confirmed or denied using existing data. Additional research using more recent data could shed some light on this aspect of the study. Second, a true experimental design, one with a true control group - randomly drawn from the identical subject pool or population - was not possible. Given the secrecy surrounding government surveillance practices and their potential wide scope, the research design could not be strengthened by comparing Wikipedia users affected by surveillance with a true control group that had not been exposed to online surveillance; the covert nature of the surveillance rendered it impossible to isolate or identify such a group of individuals. This is one of the challenges of studying chilling effects and the impact of surveillance more generally - much of the practices at issue are secret and thus difficult to study systematically.

Cushing, Tim. "The Chilling Effect of Mass Surveillance Quantified." *Tech Dirt Magazine*. 2 May 2016. <https://www.techdirt.com/articles/20160429/07512934314/chilling-effect-mass-surveillance-quantified.shtml>

There has been much talk about the chilling effect of mass surveillance. The problem isn't that anyone is actively watching everyone. The problem is that algorithms and search tools are doing the watching, meaning everything eventually receives some level of scrutiny if it's deemed suspicious by the filters. It's been mostly talk, though. Anecdotal evidence passed on by journalists, security researchers and others whose interests might clash with what the US government has deemed acceptable. Now, there's data. A study by Jonathon W. Penney shows searches for certain subject matter have declined in response to the NSA leaks. Penney cites earlier studies of Google traffic that showed a statistically significant decline of 5% in searches involving terms people might believe would be flagged as suspicious by mass surveillance software. He also notes that the dip was short-lived, corresponding roughly to the initial Snowden leaks before resuming at their normal pace after a few months.

¹⁷ Penney, Jonathon. "Chilling Effects: Online Surveillance and Wikipedia Use." *UC Berkeley Technology Law Journal*. 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

**INDICTS TO
CON EVIDENCE**

A2 NSA

NSA, Stopped a NYC Subway Bombing¹⁸

On face, this instance of stopping terror seems true. The NSA tipped off the FBI based on knowledge gathered from its surveillance and the FBI prevented the attack from occurring. However, shortly after the attack was prevented, the House Intelligence committee revealed that it was the foreign surveillance that stopped the subway attack, not NSA surveillance on US citizens. This means that in the affirmative world, attacks like this will continue to be prevented using standard surveillance tactics.

Hosenball, Mark. "US NSA Internet spying foiled plot to attack New York subways: sources." *Reuters*. 7 June 2013. <http://www.reuters.com/article/2013/06/07/us-usa-security-plot-idUSBRE95617120130607>

A secret U.S. intelligence program to collect emails that is at the heart of an uproar over government surveillance helped foil an Islamist militant plot to bomb the New York City subway system in 2009, U.S. government sources said on Friday. The sources said Representative Mike Rogers, chairman of the House of Representatives Intelligence Committee, was talking about a plot hatched by Najibullah Zazi, an Afghan-born U.S. resident, when he said on Thursday that such surveillance had helped thwart a significant terrorist plot in recent years. President Barack Obama's administration is facing controversy after revelations of details of massive programs run by the National Security Agency for collecting information from telephone and Internet companies. The surveillance program that halted the Zazi plot was one that collected email data on foreign intelligence suspects, a U.S. government source said.

¹⁸ Amira, Dan. "Did Controversial NSA Spy Programs Really Help Prevent an Attack on the Subway?" *New York Magazine*. 10 June 2013. <https://nymag.com/intelligencer/2013/06/nsa-prism-zazi-subway-feinstein-rogers-phone.html>

A2 NSA

NSA, Stopped a New York Stock Exchange Bombing¹⁹

Another example CON teams might use to prove the NSA has been foiling terrorist attacks is the plot to bomb the New York Stock Exchange. Unfortunately for them, this attack was also prevented using normal foreign surveillance and intelligence that has nothing to do with the data acquired by citizens. The NSA monitored a known extremist in Yemen who contacted plants in the United States. Court documents and FBI reports later undercut NSA claims touting that their surveillance programs stopped Al Qaeda's plot.

Shiffman, John and Mark Hosenball. "US says surveillance thwarted NYSE attack, Somali funding." *Reuters*. 18 June 2013. <https://www.reuters.com/article/usa-security-nyse/u-s-says-surveillance-thwarted-nyse-attack-somali-funding-idINDEE95H0CF20130618>

In the NYSE case, Deputy FBI Director Sean Joyce told Congress that as the NSA monitored a "known extremist in Yemen," the agency learned that the suspect was contacting Khalid Ouazzani, a Kansas City used-auto parts businessman. Joyce did not cite dates, but court records place the time between 2008 and 2010. With that information, Joyce said, the FBI obtained a more tightly targeted Foreign Intelligence Surveillance Act warrant and was "able to detect a nascent plot to bomb the New York Stock Exchange." Joyce added that Ouazzani "had been providing information and support to this plot" but provided no further details.

Ross, Brian. "NSA Claim of Thwarted NYSE Plot Contradicted by Court Documents." *ABC News*. 19 June 2013. <https://abcnews.go.com/Blotter/nsa-claim-thwarted-nyse-plot-contradicted-court-documents/story?id=19436557>

Court documents and FBI field reports reviewed by ABC News undercut and contradict the dramatic testimony from senior counter-terrorism officials that the National Security Agency's surveillance programs thwarted an attack by al Qaeda on the New York Stock Exchange. According to an FBI interview with an imprisoned al Qaeda figure involved in the plot, "there was no further operational planning of that target" after surveillance found the four streets around the exchange building "were blocked off from vehicular traffic." The FBI document was filed last month in federal court in New York as part of the government sentencing memorandum for one of the alleged plotters, Sabirhan Hasanoff, who is to be sentenced next week. But the FBI deputy director, Sean Joyce, provided Congress with a different version of events Tuesday as he cited the stock exchange plot as one of more than 50 "terror events" that had been disrupted with the help of the NSA's secret surveillance programs. "We went up on the electronic surveillance and identified his co-conspirators and this was the plot that was in the very initial stages of plotting to bomb the New York Stock Exchange," Joyce testified.

¹⁹ McClam, Eric. "Plot to Bomb NYSE Foiled by Surveillance Program: FBI." *NBC News*. 18 June 2013. <https://www.cnbc.com/id/100802908>

A2 WHITESIDES

Reuters, Surveillance Stopped 50 Attacks²⁰

This evidence, and several instances where the NSA has claimed to have used surveillance information to prevent terrorist attacks, all come from the same place: The NSA. On top of this source being clearly biased to make their own agency look good, most of these “incidents” either did not exist or were stopped through other existing channels. General Keith Alexander, the one who argued that 54 terrorist attacks were stopped by surveillance, ended up being discredited after countless independent reporter investigations. Any unbiased source comes to the conclusion that there is zero evidence that NSA surveillance stopped a single terrorist attack.

Holmes, Aaron. “The NSA phone-spying program exposed by Edward Snowden didn’t stop a single terrorist attack, federal judge finds.” *Business Insider*. 2 September 2020.

<https://www.businessinsider.com/nsa-phone-snooping-illegal-court-finds-2020-9>

The NSA’s program to collect phone records was first brought to light by the former NSA contractor Edward Snowden in 2013. Amid public outrage following the revelation, the agency defended the program by claiming it had helped thwart terrorist attacks. But the NSA could point to only one example: the case of Basaalay Moalin. On Wednesday, the appeals court ruled that not only was the collection of Moalin’s phone records illegal, but it was ultimately irrelevant to the conviction. In other words, **there is zero evidence the NSA’s phone-records program stopped a terrorist attack, contradicting the public statements of US intelligence officials following Snowden’s revelation**. Judge Marsha Berzon said in the ruling. “To the extent the public statements of government officials created a contrary impression, that impression is inconsistent with the contents of the classified record,” she wrote. An NSA representative declined to comment when reached by Business Insider. The NSA’s program of collecting bulk metadata was discontinued in 2015 when Congress passed the USA Freedom Act. Under the law, bulk phone records would still be kept by private phone companies but could be obtained by investigators only with a judge’s permission. The NSA reportedly stopped pursuing phone metadata entirely by 2018.

Lind, Dara. “Everyone’s heard of the Patriot Act. Here’s what it actually does.” *VOX News*. 2 June 2015. <https://www.vox.com/2015/6/2/8701499/patriot-act-explain>

The Obama administration says that Section 215, in particular, has been extremely helpful in terrorism investigations. But **when the government’s Privacy and Civil Liberties Oversight Board reviewed the program in January 2014, that is ... not what it found (emphasis added)**: Where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways. The first is by offering additional leads regarding the contacts of terrorism suspects already known to investigators, which can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. But our review suggests that the Section 215 program offers little unique value here, instead largely duplicating the FBI’s own information-gathering efforts. The second is by demonstrating that known foreign terrorism suspects do not have U.S. contacts or that known terrorist plots do not have a U.S. nexus. [...] We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, **we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack**. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. In that case, moreover, the suspect was not involved in planning a terrorist attack and there

²⁰ Whitesides, John. “NSA director says surveillance helped stop ‘dozens’ of attacks.” *Reuters*. 12 June 2013. <https://www.reuters.com/article/us-usa-security/nsa-director-says-surveillance-helped-stop-dozens-of-attacks-idUSBRE95910O20130612>

is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.