victory briefs

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

January 2021 PF Brief*

*Published by Victory Briefs, PO Box 803338 #40503, Chicago, IL 60680-3338. Edited by Lawrence Zhou. Written by Inko Bovenzi, Siva Sambasivam, Yukiho Semimoto, and Anik Sen. Evidence cut by Ty Rossow and Lawrence Zhou. For customer support, please email help@victorybriefs.com.

Contents

1 Topic Analysis by Inko Bovenzi **6**
1.1 What is NSA Surveillance? 6
1.2 Aff Arguments 9
1.2.1 ICE..... 9
1.2.2 Overwhelming Quantity Information 10
1.2.3 Privacy 11
1.3 Neg Arguments 12
1.3.1 Security Benefits: Preventing Terrorism 12
1.3.2 Security Benefits: Other Crimes 13
1.3.3 Companies Improve Security 14

2 Topic Analysis by Yukiho Semimoto **16**
2.0.1 Introduction 16
2.1 Background 17
2.1.1 What is the NSA 17
2.1.2 History of NSA 19
2.1.3 Conclusion 20
2.2 Pro Arguments 20
2.2.1 Privacy 21
2.2.2 Racism 22
2.2.3 Inefficiencies/Tradeoff 23
2.2.4 Weighing/Framing 23
2.3 Con Arguments 24
2.3.1 Terrorism 24
2.3.2 Cybersecurity 25
2.3.3 Weighing/Framing 26
2.4 Conclusion 26

3 Topic Analysis by Anik Sen **27**
3.1 Introduction 27
3.1.1 Background 27
3.2 Aff Arguments 28
3.2.1 Privacy 29
3.2.2 Racism 30
3.2.3 Internet Fracturing 31
3.2.4 Cyber Security 32
3.2.5 AT: Terrorism 33
3.3 Neg Arguments 35
3.3.1 Terrorism 35
3.3.2 A2 Privacy 36
3.4 Conclusion 37

4 Topic Analysis by Siva Sambasivam **38**
4.1 Background 38
4.1.1 Introduction 38
4.1.2 History of NSA Surveillance 39
4.1.3 Topic-Related Considerations 40
4.2 Affirmative Arguments 41
4.2.1 Information Overload 41
4.2.2 Tech Competitiveness 45
4.3 Negative Arguments 48
4.3.1 Terrorism 48
4.3.2 Foreign Shift 50
4.4 Concluding Thoughts 52

5 Pro Evidence **53**
5.1 Metadata 53
5.1.1 Mass Surveillance 53
5.1.2 AT: Metadata Anonymous 55
5.1.3 Warrantless 57
5.2 PRISM 58
5.2.1 Secrecy 58
5.2.2 AT: Foreign Targets 60
5.2.3 Executive Power 61

5.3 AT: National Security 62
5.3.1 Already Out of Use 62
5.3.2 Costs 63
5.3.3 Encryption 64
5.3.4 Err Pro 65
5.3.5 Intelligence Shift 68
5.3.6 No Evidence 69
5.3.7 Not Worth It 70
5.3.8 AT: Any Risk of Terrorism 72
5.3.9 AT: Future Use 74
5.3.10 AT: Covid-19 76
5.4 AT: Political Controversy 77
5.4.1 Bipartisan 77
5.5 Rights 78
5.5.1 Abolish the NSA 78
5.5.2 Right to Privacy 81
5.5.3 Right to Privacy – Democracy Impact 82
5.5.4 Right to Privacy – Social Progress Impact 85
5.5.5 Abuse 87
5.5.6 1st Amendment 89
5.5.7 AT: Squo Reforms Solve 92
5.6 Social Control 95
5.6.1 Anti-Capitalism 95
5.6.2 Chilling Effect 96
5.6.3 Surveillance Capitalism 97

6 Con Evidence **99**
6.1 NSA Action Fails 99
6.1.1 Congress Key 99
6.1.2 EO12333..... 101
6.1.3 EO 1233 – AT: Not Domestic 103
6.1.4 Voluntary Actions Fail 105
6.1.5 Other Agencies 106
6.2 Outsourcing 107
6.2.1 Five Eyes 107
6.2.2 Backdoors 109

6.2.3 XKeyscore 110
6.2.4 Legal Checks 112
6.3 Covid-19 113
6.3.1 Tracking Infections 113
6.3.2 AT: Privacy Spillovers 115
6.4 National Security 117
6.4.1 Metadata 117
6.4.2 Metadata – AT: NSA Scrapped It 119
6.4.3 White Nationalism 120
6.4.4 White Nationalism – Empirics 122
6.4.5 White Nationalism – Impact 124
6.4.6 AT: No Evidence 126
6.4.7 AT: Out of Use 128
6.5 Political Controversy 129
6.5.1 Trump 129
6.6 AT: Privacy 131
6.6.1 Alternate Causes 131
6.6.2 Not Invasive 133
6.6.3 Protections Now 134
6.6.4 AT: Metadata 135
6.6.5 AT: Unconstitutional 137

1 Topic Analysis by Inko Bovenzi

Inko Bovenzi debated for Hunter High School in New York City. He qualified to the Tournament of Champions twice and reached outrounds in his junior year. He has reached late elimination rounds in several varsity tournaments, including finals at Yale, quarterfinals at UK and semifinals at Scarsdale. In addition, he was 8th speaker at Harvard, 3rd speaker at UK, and 7th speaker at Scarsdale. He was invited to compete at the Harvard Round Robin twice, and during his senior year, he was ranked first in the country. He was an instructor at the Victory Briefs Institute this summer.

1.1 What is NSA Surveillance?

The National Security Agency, or NSA, conducts regular surveillance of both Americans and foreign people, especially focusing on communication between Americans and for-eigners. The full extent of its surveillance is unknown, and much of what the NSA has done or is doing is illegal:

> Secret government documents, published by the media in 2013, confirm the NSA obtains full copies of everything that is carried along major domestic fiber optic cable networks. In June 2013, the media, led by the Guardian and Washington Post started publishing a series of articles, along with full government documents, that have confirmed much of what was reported in 2005 and 2006 and then some. The reports showed-and the government later admitted—that the government is mass collecting phone metadata of all US customers under the guise of the Patriot Act. Moreover, the media re-ports confirm that the government is collecting and analyzing the content of communications of foreigners talking to persons inside the United States, as well as collecting much more, without a probable cause warrant. Finally, the

> media reports confirm the "upstream" collection off of the fiberoptic cables that Mr. Klein first revealed in 2006.[1]
>
> News reports in December 2005 first revealed that the National Security Agency (NSA) has been intercepting Americans' phone calls and Internet communications. Those news reports, combined with a USA Today story in May 2006 and the statements of several members of Congress, revealed that the NSA is also receiving wholesale copies of American's telephone and other communications records. All of these surveillance activities are in vio-lation of the privacy safeguards established by Congress and the US Consti-tution.

Right off the bat, this illegal activity represents an important point for this topic: this topic is *not* legislative. The resolution is that the NSA should end all of this activity, not that Congress should pass a bill banning it. The distinction is important because perhaps if Congress banned surveillance of American nationals and lawful permanent residents, the NSA might ignore this. Such arguments, however, are not topical for the wording of this topic.

It is also possible that in the near future, courts may force the NSA to end this unlawful surveillance, which might significantly affect aff or neg ground on the topic. You should be prepared with evidence for why it is likely for the surveillance to end soon or not, as if this surveillance will disappear during the Biden administration, that could take out a lot of arguments on the topic, perhaps even your own. There are many lawsuits against current surveillance, for example the one below:

> EFF is fighting these illegal activities in the courts. Currently, EFF is repre-senting victims of the illegal surveillance program in Jewel v. NSA, a law-suit filed in September 2008 seeking to stop the warrantless wiretapping and hold the government and government officials behind the program account-able. In July 2013, a federal judge ruled that the government could not rely on the controversial "state secrets" privilege to block our challenge to the constitutionality of the program. On February 10, 2015, however, the court granted summary judgment to the government on the Plaintiffs' allegations of Fourth Amendment violations based on the NSA's copying of Internet traffic from the Internet backbone. The court ruled that the publicly avail-able information did not paint a complete picture of how the NSA collects

[1]EFF, "NSA Spying," Electronic Frontier Foundation, https://www.eff.org/nsa-spying

> Internet traffic, so the court could not rule on the program without looking at information that could constitute "state secrets." The court did not rule that the NSA's activities are legal, nor did it rule on the other claims in Jewel, and the case will go forward on those claims. This case is being heard in conjunction with Shubert v. Obama, which raises similar claims.[2]

To understand how it's possible for the United States to have a body of its government that engages in such activity, it's important to understand how the legal ambiguity that allows for mass-surveillance came to be. The Patriot Act, written into law by large ma-jorities of Congress following 9-11, explains what actions are legal and which are illegal for the NSA and other government bodies:

> The Patriot Act allows investigators to use the tools that were already avail-able to investigate organized crime and drug trafficking. Many of the tools the Act provides to law enforcement to fight terrorism have been used for decades to fight organized crime and drug dealers, and have been reviewed and approved by the courts. As Sen. Joe Biden (D-DE) explained during the floor debate about the Act, "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists." (Cong. Rec., 10/25/01)
>
> The Patriot Act allows law enforcement to use surveillance against more crimes of terror. Before the Patriot Act, courts could permit law enforce-ment to conduct electronic surveillance to investigate many ordinary, non-terrorism crimes, such as drug crimes, mail fraud, and passport fraud. Agents also could obtain wiretaps to investigate some, but not all, of the crimes that terrorists often commit. The Act enabled investigators to gather information when looking into the full range of terrorism-related crimes, including: chemical-weapons offenses, the use of weapons of mass destruction, killing Americans abroad, and terrorism financing.[3]

The vagueness of the Patriot Act allows the NSA to essentially wiretap any American. Because wiretapping everyone is technically "investigating terrorism," a very generous reading of the Patriot Act led to the current situation of mass surveillance.

Now that we understand the major points of what the NSA does, whether or not it's

[2]EFF, "NSA Spying," Electronic Frontier Foundation, https://www.eff.org/nsa-spying
[3]"What is the USA Patriot Web," https://www.justice.gov/archive/ll/highlights.htm

illegal, and whether or not that might change, let's look into some potential arguments.

1.2 Aff Arguments

1.2.1 ICE

ICE, or Immigrations and Customs Enforcement, is an agency of the United States gov-ernment that enforces laws relating to immigration. While ICE is best known for its deportations of undocumented immigrants, crimes related to human trafficking and other similar issues also fall under its jurisdiction. While there is no solid proof that ICE is able to deploy NSA data to help target undocumented immigrants who have not broken any laws, documents obtained by *The Daily Beast* strongly suggest that this is the case:

> …that may not sound like a big deal. But it indicates that NSA surveillance is relevant to the immigration agency's work.
>
> "FISA allows for the retention and dissemination of information that is evi-dence of a crime and is being retained or disseminated for law enforcement purposes," the handbook says.
>
> A paragraph on the uses of foreign intelligence information is redacted, as is an entire section titled "FISA Authority vs. Court-Overseen Criminal In-vestigatory Surveillance Techniques."
>
> A significant portion of a section about surveilling people suspected of being "lone wolf" terrorists.
>
> "The document strongly suggests that private information obtained using the government's secret spying tools is bleeding into certain ICE investiga-tions," Toomey said. "These tools were designed for foreign intelligence investigations, not immigration purposes. We need to know far more about how DHS agents use this sensitive information, what consequences it has for people living here in the United States, and when the government believes it must tell individuals that it has used FISA surveillance in immigration matters."[4]

[4]"Exclusive: Read the ICE Agents' Guide to NSA Surveillance," Daily Beast, https://www.thedailybeast.com/exclusive-read-the-ice-agents-guide-to-nsa-surveillance

The core of the issue is the following: while the NSA certainly can legally monitor so called "lone wolf attackers" under the Patriot Act, in doing this very broad surveillance it can uncover human traffickers, but also undocumented immigrants. The evidence suggests that the NSA then shares some of this information to ICE. The impact of this argument would be that such surveillance allows ICE to target undocumented immi-grants with far greater ease, leading to more deportations which can have deadly con-sequences. While I suppose that there might be a neg version of this argument (NSA surveillance helps ICE target human trafficking), I think this argument will be tougher to contextualize and weigh than the aff version.

You may be wondering how this argument can be topical when the resolution is ex-plicitly talking about the NSA ending its surveillance of lawful residents of the United States. The key is that the NSA generally does not know who is undocumented and who isn't before it begins its surveillance. That means that in order to find, say 10 undocu-mented immigrants, it must first wiretap at least dozens of lawful residents. Without wiretapping these residents first through mass surveillance, the NSA cannot find undoc-umented immigrants with any efficiency, or at least without any more efficiency than ICE already has.

1.2.2 Overwhelming Quantity Information

Because the NSA has such a large surveillance network, it's likely that there is such an overwhelming quantity of information that the NSA cannot focus on what's important to stopping terrorist attacks. With less broad searches, in theory the NSA should be more efficient overall:

> A second limitation on the potential of using surveillance to initiate real-time intervention is the sheer volume of information produced by existing surveillance systems. It can now be almost impossible to integrate and make timely sense of the reams of images and information being recorded. Given the enormous volumes of information coursing through some surveillance systems, officials tend to rely on practical shortcuts to help them select out particular actions, communications or individuals as "suspicious." Increas-ingly, such cognitive shortcuts are being formalized in technological struc-tures. One of the more controversial of these efforts is the U.S. National Security Agency' s ECHELON system which aims to capture all satellite, microwave, cellular and fiber-optic communications. Rather than attempt

> to analyze all of these communications, the ECHELON system processes this information through massive computers which search for key words or phrases, thereby drawing out particular individuals and messages for spe-cial attention.

These systems can also, whether intentionally or not, be designed in a potentially racist or at least stereotypical manner. Because algorithms are designed based on past terrorist attacks, they tend to discriminate towards (i.e. drawing suspicious towards) "stereotyp-ical terrorists," with limited success. In some instances, these biases in the systems can directly lead to racial and other profiling, where people are more likely to be put under investigation for factors ranging from their race and appearance to what they bought at an airport gift shop. This is clearly not the best way to do surveillance.

A somewhat suspect, but still reasonable statistical analysis of the NSA's efficiency found that the agency flags 475,500 innocent Americans for every terrorist it discov-ers, with a price tag of up to $14 billion for each discovered terrorist (once you add the NSA's budget with the costs of every false positive).[5] Because there are so few terrorists living in the United States (300 million people and maybe one large terrorist attack per year?), it simply is inefficient to wiretap everyone to find them, as the author concludes:

> The NSA's screening of the general population to find terrorists is analogous to the medical profession's screening for cancer, the methodology used in this article. Using the medical profession's insights and equations, we can see that the NSA is foisting a poor screening tool on Americans. Even putting concomitant costs and the huge loss of privacy aside, the NSA's electronic spying costs substantially more than it is worth and, on cost/benefit grounds, should be terminated.

1.2.3 Privacy

Because the NSA accumulates so much information on Americans for use by the gov-ernment, there is clearly a huge risk to Americans' personal privacy:

> One of the most problematic elements of this surveillance is the govern-ment's use of "backdoor searches" to investigate individual Americans. Although the government says PRISM is targeted at foreigners who lack Fourth Amendment privacy rights, it systematically combs through its

[5] https://www.econlib.org/library/Columns/y2014/Hoopersurveillance.html

> PRISM databases for the emails and messages of Americans. Indeed, FBI agents around the country routinely search for the communications of specific Americans using their names or email addresses — including at the earliest stages of domestic criminal investigations.
>
> The result is an end-run around the Fourth Amendment. Investigators have easy access to a trove of Americans' private emails, calls, and messages, with-out ever seeking individualized approval from any judge, as the Constitu-tion requires.
>
> This surveillance leaves far too much unchecked power in the hands of ex-ecutive branch officials. Today, that includes President Trump, who as a candidate called for expanded spying on Americans… Now the courts must do their part to ensure that Americans' online communications receive the full protection of the Fourth Amendment.[6]

The trouble with this sort of mass surveillance is that it gives the government access to almost all of the communications of each and every American. That can lead to a large number of potential problems. First, it makes it very easy for officials investigating an American for one crime to discover evidence of another in their surveillance, leading to much more criminalization of Americans, many of whom may lack the resources to defend themselves in court. Secondly, and perhaps more importantly, this allows for the executive branch to investigate any person until they find a crime or evidence of one in the surveillance data. Even if a crime was never communicated, just the investigation can be very damaging for a politician (for example Hillary Clinton's emails or the inves-tigations around Hunter Biden). Thus, surveillance gives the president and Attorney General a lot of power to attack political opponents, or anyone else whom they choose.

1.3 Neg Arguments

1.3.1 Security Benefits: Preventing Terrorism

Surveillance can help prevent terrorist attacks in three major ways:

[6]Patrick Toomey, 8-22-2018, "The NSA Continues to Violate Americans' Internet Privacy Rights," Amer-ican Civil Liberties Union, https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy

> The impetus behind the current embrace of surveillance relies on the assumption that more surveillance will provide greater security where the existing surveillance infrastructure has failed. Anti-terrorist surveillance is therefore justified in three ways. First, surveillance can provide information that can be retrospectively analyzed to provide insights about terrorists and their operations. Second, surveillance can deter future terrorist attacks. Finally, surveillance will allow the authorities to intervene in real-time to thwart terrorist acts before they occur.[7]

While data on how many terrorist attacks the NSA prevents may be classified and/or impossible to produce, there is no doubt that there is *some* positive effect here. The weakest of these three arguments is likely that of deterrence. Because most terrorists aren't worried about being imprisoned or dying for their "cause," it is exceptionally difficult to deter them. However, once can easily imagine a scenario where the NSA has accumulated a host of data about a group of suspects who then launch a series of attacks, where that data is useful to stopping the attacks as they unfold and apprehending the suspects. However, there are few, if any examples of this actually happening, though it is unclear if this is because this has never happened or when it has happened it was classified.

1.3.2 Security Benefits: Other Crimes

Insights of criminals in the United States is key to catching and arresting both ter-rorists and more common criminals such as murderers. Many potential criminals share the same behavior characteristics as ones who have been apprehended and mass-surveillance can help detect these individuals and investigate them to prevent future crimes. In fact, while such use of surveillance is possibly illegal, the FBI is the largest user of NSA data, which it uses to investigate domestic crimes that need not be related to terror:

> The declassified FISA court ruling revealed that the FBI is the most prolific miner of data about "U.S. persons," a legal term that means any U.S. citizen or foreign national legally in the country. Queries of this data are known as "backdoor searches." In 2017, the FBI ran approximately 3.1 million searches related to U.S. persons, compared to 7,500 combined searches by the CIA and NSA during the same year. Many of the FBI's searches were not legally

[7]https://www.jstor.org/stable/pdf/4146129.pdf?refreqid=excelsior%3Af49dcafe81e17e616d0757b9bce72c2e

> justified because they did not involve a predicated criminal investigation or other proper justification for the search, as required by law, according to Boasberg's FISA court ruling.[8]

This argument can possibly be compared with privacy arguments by arguing that surveillance is only ever an issue for a person if they have broken the law, in which case it usually is a positive thing if they are caught and prosecuted for it. It is very difficult to find negative impacts to lower privacy, and the benefits of increased security are clear.

1.3.3 Companies Improve Security

While this argument does not have a ton of evidence supporting it (few arguments on this topic have it, anyway), one interesting neg argument to research is the idea that companies, in an attempt to avoid NSA surveillance, will update their security systems in ways that will make them more robust in general:

> Most of us would agree that the NSA has spread its nets too far and cut deeply into our personal privacy. Ultimately, and perhaps ironically, I am hopeful this transgression will leave us with better protection for our per-sonal communication than ever before.
>
> I predict that more and more communications service providers will provide strongly encrypted communications by default. They'll also do so in such a way that outside, unauthorized parties (the NSA, law enforcement, and so on) will not be able to get the plaintext access to data they currently enjoy – at least not as easily as they do today…
>
> How might cloud providers protect customer data? For example, a public cloud provider might turn on default encryption in such a way that no one except the customer has access to the private keys. The data might be stored in a public cloud but appear as gobbledygook to anyone but the client. The NSA or other law enforcement agents would have no incentive to ask for the data, warranted or unwarranted (in the legal sense) because all they'd get is encrypted data. Several of these services already exist, and it's my strong

[8] Trevor Aaronson, 10-10-2019, "Court Ruling Shows How FBI Abused NSA Mass Surveillance," Intercept, https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/

personal belief that this model will become the norm.[9]

Better encryption of sensitive data and information, as well as stronger security, may benefit companies and civilians alike in the long term by reducing the frequency of successful, outside attacks on intellectual property or other valuable information. While the link of this argument is a bit fuzzy, the impact is certainly quite large, as these attacks already significantly damage our economy, and will get worse and worse every year without stronger security.

[9]Roger A. Grimes, 11-19-2013, "NSA spying will ultimately benefit us all," CSO Online, https://www.csoonline.com/article/2609882/nsa-spying-will-ultimately-benefit-us-all.html

2 Topic Analysis by Yukiho Semimoto

Yukiho Semimoto is a current freshman at Georgetown University studying Inter-national Politics. She debated for five years at Edgemont High School in Scarsdale, New York, serving as the captain of her team. In her competitive career, she qualified to the TOC twice and reached late elims like quarterfinals at Harvard and Emory, and amassed several speaker awards including 3rd at Emory, 2nd at Scarsdale, 6th at Lexington, and top speaker at Lakeland. As a coach, her students have finaled tour-naments like Glenbrooks and championed several others, and have amassed more than 10 gold bids. She was also an instructor at VBI this summer.

2.0.1 Introduction

Hi everyone! Welcome to the January topic: "Resolved: The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents." Tournament-wise, January topics have historically always been a favorite of mine. National tournaments like Blake that occur in December have always used the January topic, and so while it is the first topic of the year that has a one-month span instead of the two-month topics that we have gotten used to by this point in the year, the January topic definitely starts out earlier and has enough time to develop a topic meta within the literature of the topic.

While the nature of online-debate has made judge pools a lot more random, adapta-tion on this topic will definitely be very important! January's notorious for having a range of national tournaments like Emory (historically has been very flow), Columbia, Lexington, Sunvite, ASU, and more. Wherever you choose to debate this month, keep in mind the types of strategies and arguments that might work better in front of spe-cific judge pools. This topic is definitely one that could and should see the rise of more complex framing arguments, especially as there will be further debates about not just traditional "PF" impacts (e.g. recessions, conflicts), but instead also arguments about privacy, democracy, and marginalization of communities.

Lastly, while the VBI topic analysis will definitely cover a lot of the background of the topic and the potential arguments to be run in the next month, if you feel a need to read more from past debaters' thoughts on this topic, feel free to go to the Policy Wiki to learn more from their 2015 topic. Their 2015 topic, "Resolved: The US Federal Govern-ment should substantially curtail its domestic surveillance", has very similar ground topic-wise and while it is has different arguments regarding what is topical and what isn't, considering that our current topic is more specific to the NSA, there will definitely be a lot of literature that you can learn from. Keep in mind that while backfiles from past topics are a cool way to learn of ways to potentially think about topics, they should never be the end-all be-all for your topic research for the month especially for one that is rapidly changing like this topic. There will always be new things to account for, bet-ter evidence and literature out there considering that it has been 5 years since the last topic. This also will apply for any literature that you might use from the OCO topic last November, considering that there might be some literature overlap in arguments about counterterrorism and cyber-attacks. Always aim to find more recent evidence and literature, as literature changes and/or improves over time.

With that in mind, good luck in the research process, and hope you learn a little more about this exciting topic!

2.1 Background

This topic is honestly a really cool one in terms of topicality. But before we dive deeper into what's topical and the ground behind both the affirmative/pro and negative/con arguments, let's break down the actors and the historical context behind the topic.

2.1.1 What is the NSA

The National Security Agency, or the NSA, is an intelligence agency that is part of the Department of Defense within the US government. It's good to think of intelligence gathering within the US government as a result of a collection of agencies and offices; in fact, there are more than 17 combined intelligence gathering agencies, like the FBI, CIA, the DIA, and the Department of Homeland Security.[1]

[1] https://www.latimes.com/nation/la-na-17-intelligence-agencies-20170112-story.html

It's important to know the difference between some of these agencies, as teams defi-nitely might try to pass off evidence about general surveillance as evidence specifically about the NSA. The questions you should ask to guide your research are: *what type of intelligence would we be losing in the affirmative world? Is that intelligence somewhat better than the intelligence that the other agencies are gathering, and if the NSA were to curtail do-mestic surveillance, would a similar level of effective intelligence be possibly acquired by other agencies?* The affirmative world should argue that it is possible-- and potentially that other agencies could acquire it in even better methods, and the negative world should contest that and argue for the unique nature of NSA domestic surveillance.

And yes, the literature points to the NSA being of unique nature compared to the other intelligence gathering agencies and offices. As the LA Times sums it up:

> "Once so secret it was referred to as"No Such Agency," the NSA is the largest and perhaps most technologically sophisticated of all the intelligence agen-cies. It focuses on signals intelligence — monitoring, collecting and process-ing communications and other electronic information — and cracking secret codes. It also protects U.S. information systems from outside penetration."[2]

Agencies like the FBI work domestically, and the CIA functions differently than the NSA as it utilizes human-oriented ways to gather data. Overarchingly, the other intelligence agencies have different areas of responsibilities within intelligence gathering.[3]

The NSA is also well known for its process of using what is called metadata:

> "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 on-line chat began and how long the communication lasted.[4]

The mass metadata that the NSA acquires becomes an important part of the rest of the intelligence that the US gathers, as not only can they act as starting points for other intelligence agencies, data from specific intelligence agencies work as pieces of a puzzle that function together to counter threats.[5] Indeed, NSA data is used by other agencies

[2]https://www.latimes.com/nation/la-na-17-intelligence-agencies-20170112-story.html
[3]https://angelialevy.com/2011/05/11/an-overview-of-the-major-u-s-intelligence-agencies-what-is-the-difference-between-the-dia-nsa-cia-and-fbi/
[4]https://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/
[5]https://www.tandfonline.com/doi/full/10.1080/01972243.2017.1414721

like the FBI.[6]

2.1.2 History of NSA

The NSA has a deep history of potential violations of privacy through intelligence gath-ering. The topic of intelligence gathering has been an ongoing struggle for decades, especially due to the counterterror efforts after the attacks of 9/11. Having a general un-derstanding of the historical timeline behind this topic will be very important in terms of uniqueness claims, as because this is a rapidly evolving topic, some pieces of evidence that teams may read about specific policies may no longer be relevant.

The first Patriot Act was signed by President Bush six weeks after 9/11, increasing the capacity of the NSA and their surveillance. Overtime, the surveillance snowballed and led to not only the tracking of millions of phone calls and monitoring of the internet and phone traffic by the NSA, but also further policy that allowed for increased warrantless surveillance under particular circumstances.[7]

By 2013, Edward Snowden became known as one of the most well-known whistleblow-ers in American history by revealing to the public of the extensive nature of NSA surveil-lance. In fact:

> "Edward Snowden's explosive revelations about NSA's telephone metadata collection program triggered an uproar at home and abroad, culminating in the 2015 passage of the USA Freedom Act—legislation that supporters claimed would"end" the kind of mass surveillance Snowden had exposed to the world."[8]

However, the status quo is one where the NSA is still allowed to domestically surveil their citizens--thus the existence of this resolution.

> "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

[6]https://arstechnica.com/tech-policy/2017/01/obama-administration-relaxes-rules-on-nsa-intelligence-sharing/
[7]https://www.motherjones.com/politics/2013/09/nsa-timeline-surveillance/
[8]https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

> 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 Intelli-gence Surveillance Court to agree that there is"reasonable, articulable suspi-cion" that the seed target is linked to terrorism."[9]

While we saw the expiration of the USA Freedom Act in the end of 2019, there still exists domestic surveillance power by the NSA that "remains untouched".[10]

2.1.3 Conclusion

It will definitely be very important on this topic to ask the question about what is topi-cal as teams read arguments about surveillance. Ask the questions of what surveillance that the NSA obtains in the status quo remains, and what surveillance counts as domes-tic. For example-- is data about emails that are transferred between a foreigner and a domestic person domestic surveillance or foreign surveillance? I do believe these ques-tions are up for debate, even if it may not be as relevant in specific arguments on this topic.

Much like the OCO topic in November of 2019, there are definitely a lot of theoretical arguments in this topic due to the uncertainty of what the NSA actually accomplishes and has accomplished through intelligence gathering. For the sake of national security, there are things that an average citizen will never know about. For example- the infor-mation released by Snowden, these classified documents are arguments that we may have never known about. This might be somewhat important in arguments in the af-firmative world about the slippery slope that the violating nature of surveillance may cause as we may never truly know the extent of the privacy violations, and is also impor-tant to keep in mind in terms of how to terminalize or argue for theoretical arguments on this topic.

2.2 Pro Arguments

Now that we've established some familiarity with the background of the topic, let's dive into the affirmative/pro arguments!

[9]https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html
[10]https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

2.2.1 Privacy

Privacy is a core of the affirmative ground on this topic. To put it in the simplest terms, the domestic surveillance that the NSA pursues is (or is arguably) an immense violation of our privacies.

This is a pretty good link-level argument in the sense that yes, in order for the NSA to find data even if there are restrictions on it, there inherently exists some sort of privacy violation -- even if it may be argued that said violation is not inherently harmful.

Thus, I think the more nuanced part of this argument isn't at the link-level but how teams might choose to terminalize a vague concept like privacy. There's a couple ways I can see teams doing this.

First, teams can argue that the erosion of privacy is an impact in and of itself. Privacy is a core human right, and acts as a prerequisite or a necessity to enjoy all other aspects of our being. It's important to consider the psychological effects of the erosion of privacy, and potential impacts that may stem from it like distrust in government. However-- the impact of "privacy" is still considerably hard to terminalize in a PF world, so if you want to run a pure-privacy impact with this argument I would aim to be more comfortable executing the weighing in terms of why privacy is of inherent value, and more valuable than life-based or econ-based arguments that the negative might read. I would guess that a neg strategy against an argument like privacy would be to read arguments about why impacts that lead to better security outcomes are more important than privacy, as safety could be a prerequisite to privacy. Without the assurance of safety, humans don't have the ability to worry about something as secondary as privacy.

Second, teams can argue about constitutional harms and the erosion of legal institutions. The worse the privacy violations, the increased likelihood for further constitutional vi-olations of privacy as those violations become normalized over time. This could be an impact in and of itself I suppose, but I think it's more of an impact magnifier to the first argument, as it just leads to further privacy violations and falls traps to the same problems of debaters having to articulate why privacy is of inherent value.

Third, stemming from the first two arguments, the erosion of privacy can lead to demo-cratic harms, or the erosion of democracy. This argument might be a little more tangible in nature, but also requires a further explanation of why democracy even matters and how much democracy would be gained in the affirmative world anyways.

Fourth, it is definitely possible to run some sort of US global influence argument when

it comes to the erosion of privacy, democracy, and constitutional protections. I would be careful running this sort of argument unless you are sure that you can pinpoint the US to be what pushes other countries incentive-wise in being aggressive in their domes-tic/international surveillance. There are indeed countless other actors pursuing things like AI surveillance, and countries like China who lead the globe in that type of surveil-lance.[11]

2.2.2 Racism

Racial profiling has historically been quite a relavant part of the NSA, as the history of terrorist attacks have led to agencies surveilling Muslim-Americans "revealing a culture of racial profiling and a broad latitude for spying on U.S. citizens.[12]

Importantly, literature generally points to this racial profiling with surveillance not just being isolated to Muslim communities:

> "Today, law enforcement spends substantial resources monitoring the on-line conversations, activities, and networks of young Black and Latino men, looking for evidence of crimes, sometimes before any crime or real threat has occurred."[13]

It's important to note that a lot of the literature talks about broad surveillance being bad both for Muslim and Black communities, and is not always NSA specific, even if other agencies may use the aid of NSA data-- thus in order to run this argument effectively you have to specifically isolate the NSA's role in the institutionalized racism.

Impact wise, more data and more surveillance available especially when there are tar-gets means further incarceration of specific communities, and a loss of privacy for them which in and of itself should be an impact as institutionalized racism should be rejected on face.

Overarchingly, running this argument would require proper articulation of why remov-ing these systems that are racist in nature would be important and how removing do-mestic surveillance under the NSA would be beneficial for that.

[11]https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
[12]https://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance
[13]https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/

2.2.3 Inefficiencies/Tradeoff

This is an argument that points to the ineffectiveness of mass data collection from the NSA. It is something that takes up resources, and can be pointed to as more ineffective compared to other forms of intelligence gathering. The argument would be that a loss of domestic surveillance would incentive better ways to accomplish the goals that may be inhibited by this resolution. I believe that this argument would function better as a delink or turn in rebuttal, as it would be a reasonable narrative to read against negative arguments that claim that the NSA intelligence is what is critical to US intelligence gath-ering. If you do choose to proceed this way, make sure to not double turn yourself and read an impact turn about intelligence gathering being bad (e.g. it is racist), unless you distinguish why the tradeoff would be better on that front.

2.2.4 Weighing/Framing

Weighing is important. Tell your judge which aff impacts matter more. You can choose to do that through framing too -- for example, if I said "xyz impact comes first in the round," that would be an example of framing instead of arguing that "xyz argument is more important than my opponent's" (that's weighing).

I would say that my familiarity with PF weighing is definitely on a less literature-oriented level, and that yours does not necessarily need to divulge beyond that level of understanding unless you want to. While there could be teams that decide to read pure framing influenced by LD or policy backfiles, PF tends to see that the meta of these topics never usually develop that far especially because these arguments need to be articulated in front of everyday judges.

I saw a lot of teams run arguments about racism on the Medicare-for-all topic, but very rarely heard comparative analysis as to why racism impacts are inherently more violent (or more important) than other types of arguments, just that racism is inherently violent and more important. While the latter is an argument that you should be making, if you are attempting to run an argument about racism or privacy you should also take the effort to explain why that form of violence should be prioritized over any other forms. You can make arguments about how historically ignored impacts should come first, and that makes a lot of sense warrant-wise. To further warrant it out, one could read comparative weighing like this: problems that are flashier and aligned with white-policy maker's incentives always have a higher probability of being solved anyways

(e.g. terrorism, economic harms), whereas problems that concerns marginalized folk or something as taken for granted as privacy will always have a lower probability of being solved due to the lack of policy focus or a lack of perception by governments that those are an imminent form of violence-- which means prioritize the latter because the former would have forms of solvency anyways. That type of weighing would function well as it uses the probability metric to prioritize affirmative impacts.

2.3 Con Arguments

2.3.1 Terrorism

There's a convincing argument on Neg ground that data from NSA surveillance is crit-ical to counter-terrorist operations, with the NSA claim in 2013 that their surveillance programs have stopped more than 50 potential terrorist events.[14] On a detection level, the NSA's type of intelligence, called metadata, is uniquely important.

> According the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority [from the NSA] contributed in over 90% of the 50 cases [of stopped terrorist events]. One of major benefits of meta-data is that it provides hindsight—it gives intelligence analysts a retrospec-tive 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 impor-tant 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.[15]

The NSA surveillance doesn't solely act as a detection method for terrorism, it also acts to deter forms of attacks as people might be less incentivized to plan events if they knew that there exists intelligence data that can pinpoint their involvement into events. This would have to be a scalar argument, considering that there also exists other forms of surveillance through other agencies, along with the NSA's capacity to surveil in foreign

[14]https://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/
[15]https://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/

grounds in the affirmative world, and that should also be somewhat of a deterrence in terms of terrorist activity.

The impact of counter terror would need to be terminalized correctly on this topic, as it definitely is a little unclear on the magnitude of the impact especially as we don't know what specific terrorist attacks the NSA has prevented. According to the NSA, threats in the current world range from terrorists attempting to acquire weapons of mass destruction, to drug trafficking, and cyberspace terrorism.[16]

It is definitely also possible to argue that in the long-term the type of intelligence that the NSA gathers will be helpful in aiding the fight against right-wing extremism, as that is often considered a form of terrorism. This would be a response to the affirmative advantage about curtailing forms of racism. However, the questions to ask are: h*ow often is the NSA engaging in "terrorist" breaking behavior for right-wing extremists in the status quo? Are white supremacists even under the jurisdiction of terrorism? Is this a long-term argument to make, considering that our administration is turning more blue as a consequence of swing states turning more blue?*

2.3.2 Cybersecurity

This neg argument, like many others, is very closely related to the above argument about terrorism but also has further implications beyond it.

The NSA explains that:

> The newest threats we face, and perhaps the fastest growing, are those in cyberspace. Cyber threats to U.S. national and economic security increase each year in frequency, scope and severity of impact. Cyber criminals, hack-ers and foreign adversaries are becoming more sophisticated and capable every day in their ability to use the Internet for nefarious purposes…. Some
> of these bad actors are criminals motivated by profit, particularly in the ar-eas of identity theft and other forms of financial cybercrime. The cost of cybercrime – already in the billions of dollars – rises each year. But cyber threats also come from nation states and other actors who seek to exploit information to gain an advantage over the United States. They might seek an economic advantage, or to gain insight into our military or foreign policy. Denial of service attacks disrupt business and undermine confidence.[17]

[16]https://www.nsa.gov/what-we-do/understanding-the-threat/
[17]https://www.nsa.gov/what-we-do/understanding-the-threat/

The NSA currently plays an important role in cybersecurity, as it oversees the responsi-bility of working with both the public and private industry to protect our cyberspace.[18] Thus, the NSA surveillance becomes somewhat important in the role of detecting these threats through their intelligence-- and these threats range anywhere from IP theft and financial impacts to cyber threats that are more serious in nature for our national secu-rity.

Again-- the important aspect of this resolution will be to what extent domestic surveil-lance of our citizens will help with the NSA's economic and security goals in cyberspace, but as the nature of the negative's interpretation of intelligence would go, the more in-telligence exists the easier it will be to detect threats.

2.3.3 Weighing/Framing

Weighing on the negative side will be a lot more similar to other topics in the sense that the impacts are generally more "tangible".

However, it may seem difficult to weigh arguments that relate to things like the economy and compare it with affirmative arguments.

My advice on this front would be to think earlier on in the topic of what impacts on the negative side help solve back for affirmative arguments, or how to outweigh the consequences of the affirmative arguments. Like mentioned previously, security can be argued to be a prerequisite to privacy. Economic arguments can have a larger magni-tude in terms of the amount of people it affects, meaning that the impact might be more important in the long run. Coming up with a coherent strategy on the weighing on the neg will definitely help you in this topic, considering the predictability of affirmative ground.

2.4 Conclusion

Last piece of advice-- if you choose to compete early for this tournament (like at Blake), make sure to have some sort of coherent narrative or strategy going into this topic. This topic is one where the arguments are somewhat predictable, and pre-planning a strategy to beat back the core arguments and impacts of this topic will definitely put you ahead in the topic. Other than that, read on, and enjoy the topic!

[18]https://online.uttyler.edu/articles/what-is-the-nsas-role-in-cyber-security.aspx

3 Topic Analysis by Anik Sen

Anik Sen debated for The Quarry Lane School in Dublin, California. He served as Public Forum Captain his junior year and Team Captain his senior year. He has reached late out rounds at MineApple, Alta, ASU, Emory, and Berkeley. His career on the national circuit spanned all four years of high school, graduating with 10 career bids. Anik currently attends Duke University as a freshman.

3.1 Introduction

Hey everyone! The January topic, Resolved: The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents.

3.1.1 Background

Mass surveillance has existed in the United States from the times of the First and Second World Wars. While they were initially created to crack codes and monitor telegraphic data that was entering and exiting the country, these programs quickly evolved to mon-itor political dissent in the country soon after government programs like the FBI, CIA, and NSA were created. Moreover, these surveillance programs were used during the Civil Rights Era to keep a watch over individuals suspected to be supportive of commu-nism.

The mass surveillance in the United States combined with 4 other large countries to form the UKUSA surveillance agreement of 1946, now known as the ECHELON collab-oration or the Five Eyes. Australia, Canada, New Zealand, United Kingdom and the United States formed this collaboration with the focus on the interception of electronic communications along with increases to their own domestic surveillance capabilities.[1]

[1] "Unmasking the Five Eyes' global surveillance practices - GISWatch". *giswatch.org*. Retrieved 7 Decem-ber 2020.

Massive expansions to both domestic and international surveillance capabilities came after the September 11, 2001 attacks. The largest response to these attacks came in the passage of the Patriot Act. It was written to strengthen US national security in relation to terrorism and had three main functions: to expand law enforcements ability so surveil through tapping of domestic and international phones, stronger interagency commu-nication to fight counterterrorism, and stronger punishments and an expanded list of activities that qualify as terrorism. The legislation was later amended to disallow the NSA from continuing its mass phone data collection program.[2]

In June of 2013, America's mass surveillance program started to have leaks appear. Ed-ward Snowden, a former CIA and NSA system analyst, gave a cache of over 15,000 in-ternal documents that became the largest news leak in the modern history of the United States. He revealed top secret documents from NSA servers in an effort to protect "basic liberties for people around the world".[3] His leaks sparked a national debate over the assault on privacy and liberty that many citizens think these programs are, while gov-ernment officials are quick to justify these programs as essential to stopping terrorism and a key part of our general National security.

As more information is released about the governmental programs that watch over the United States, the general public is learning more about the actual effectiveness of these programs and the broad extent to which our government can surveil us.

3.2 Aff Arguments

This topic, at first glance, seems to be aff heavy. The idea of being surveilled without consent is one that many US citizens are not inclined to like. With the Fourth Amend-ment right that protects people from unreasonable searches and seizures by the govern-ment, the idea of privacy and other rights that should be protected becomes a strong argument for any aff team. The issue with these types of arguments is providing a sub-stantial impact. It is not enough in most rounds to say that the idea of privacy being infringed upon is significant or clear enough for a judge to vote for you. Thus, while this brief will give you many argument areas to consider, it is important to find strong and specific impacts for any contention.

[2]Kelly, Erin (June 2, 2015). "Senate approves USA Freedom Act". *USA Today*. Retrieved 7 December 2020.

[3]*"Ex-CIA employee source of leak on PRISM program". France 24. 9 June 2013. Retrieved 7 December 2020.*

3.2.1 Privacy

Privacy is something that is directly taken away with mass surveillance programs. The right to privacy is the freedom of interference which, government programs that spy on their citizens without their knowledge, prevent citizens from obtaining.

> Congressional panels, journalists, and citizens have been told that fusion centers raise few privacy concerns and that their information gathering is focused and valuable. Contrary to these assurances, critics have argued that fusion centers erode civil liberties without concomitant gains for security. A recent Congressional report backs these concerns, demonstrating that fusion centers have amounted to a waste of resources.[4]

Not only are these programs eroding our right to privacy, mass surveillance is uniquely bad as it is used by totalitarianism regimes to control their population.

> Totalitarian regimes in Germany made widespread use of mass surveillance in order to dominate freedom and carry out horrific crimes. It is no sur-prise then that Germany is today a top-ranking country globally for data privacy and protection laws, that Berlin has evolved to become one of the world capitals for hackers and data privacy advocates, and that one of the first peer-to-peer computational platforms to guarantee user privacy against unwanted electronic surveillance, Enigma, is named after the tool that the Nazis used to broadcast coded messages from. Yet, ironically, the power of today's mass surveillance systems — like those of the NSA, brought to light by Edward Snowden's revelations — far exceed what previous totalitarian regimes could have imagined. Surveillance has spread like a pandemic.

The general limitations to this argument come on the impact level. Although there are clear violations of privacy from these mass surveillance programs inside the United States, reading specific impact scenarios tend to be difficult given a lack of evidence. Thus, arguments stemming from privacy violations tend to work best in conjunction with a moral argument about what privacy should look like in the United States.

[4] https://harvardlawreview.org/2013/06/addressing-the-harm-of-total-surveillance-a-reply-to-professor-neil-richards/

3.2.2 Racism

Mass surveillance has historically been used to promote racist and targeted surveillance of people. The roots to surveilling Black people in America predates the formation of any government programs or agencies.

> "Black people's history in this country is an example of how surveillance was heavily used as a tool to be disruptive of folks challenging the social order, which is supposed to be one of those stated rights of Americans, to be able to voice our opposition to the status quo. Surveillance has served as an important deterrent." — Dayvon Love, Director of Public Policy for Leaders of a Beautiful Struggle.[5]

The foundation for today's expansive state surveillance system was built upon the lessons learned from America's history of monitoring Black people in America. As early as the seventeenth century, whites were constantly surveilling Black people. Slaves (and free Blacks) were observed closely in order to detect, prevent, investigate, and prosecute Black misconduct, whether serious or minor. Informants policed a wide variety of behavior, but were especially seen as valuable for the prevention and suppression of organized resistance and rebellions. Slave informants spoiled the infamous rebellions planned by Denmark Vesey and Gabriel Prosser, as well as many other lesser-known plans of resistance. Surveillance continued after Emancipation, when Black Codes and Jim Crow Laws were enacted and used to return many Blacks to another form of slavery – convict labor.[6]

Even if current surveillance efforts aim to protect America from foreign and domestic threats, the history of these practices imply the government only sees these threats in certain demographic groups.

> Mass surveillance has been a long-standing feature of American criminal justice, albeit a selective practice usually reserved for Blacks. But now, what has been and continues to be a normalized feature of Black people's lives is becoming commonplace for all Americans. It remains to be seen how Amer-ican citizens will respond to this new form of governance by the state and vice versa, but it is safe to say that Black people have always been and – at this rate – will always be under the watchful eye of the state, whether they are on the street or online.[7]

[5]https://www.aclu-md.org/en/news/racist-past-government-surveillance
[6]https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/
[7]https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/

The impacts of mass surveillance used to target specific groups or individuals are oc-curring in the status quo. On the global stage, China has been using mass surveillance tactics to control and eradicate large groups of Uighur Muslims.

> Uniformed shop assistants, knife controls and "convenience police stations" are only the most visible elements of the police state. The province has an equally extensive if less visible regime that uses yet more manpower and a great deal of technology to create total surveillance.
>
> Under a system called fanghuiju, teams of half a dozen—composed of po-licemen or local officials and always including one Uighur speaker, which almost always means a Uighur—go from house to house compiling dossiers of personal information. Fanghuiju is short for "researching people's con-ditions, improving people's lives, winning people's hearts". But the party refers to the work as "eradicating tumours". The teams—over 10,000 in ru-ral areas in 2017—report on "extremist" behaviour such as not drinking alco-hol, fasting during Ramadan and sporting long beards. They report back on the presence of "undesirable" items, such as Korans, or attitudes—such as an "ideological situation" that is not in wholehearted support of the party.[8]

The example of China and Uighur Muslims is just one example of where unchecked surveillance can lead us to. It is important to be careful of your rhetoric when debating about serious arguments like racism and to avoid commodifying these experiences for the ballot, read and research about Black experiences specifically.

3.2.3 Internet Fracturing

As more governments exercise control over their citizens and determine what they can or cannot access, the internet is at risk of becoming fractured.

> "The current lack of transparency about the nature of government surveil-lance in democratic countries undermines the freedom and the trust most citizens cherish, it also has a negative impact on our economic growth and security and on the promise of an Internet as a platform for openness and

[8]https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other

> free expression," Richard Salgado, Google's law enforcement and informa-tion security director, said."[9]

Large internet companies like Google, Apple, Microsoft, Facebook, and Twitter are lob-bying the government to prevent the spread of surveillance techniques like the ones we currently use. These programs take away from the data sharing that goes on between countries and makes it more difficult for these companies to spread the Internet. Along with the economic issues that these companies face with the expansion of their internet providing services, there are issues with the accessibility of the internet. With countries limiting the content that citizens can see, the Internet looks different in each different country, limiting the spread of free information and making it more difficult for compa-nies to adjust to different content being allowed in different countries.

This link provides access to many different types of impacts. Not only are there large, constitutional impacts about the freedom of speech and access to information, there are also impacts about the economy (stemming from the hardships that these large compa-nies are beginning to face from the United States and other countries) that may provide some diversity from large, perceptual impacts.

3.2.4 Cyber Security

The way that the NSA conducts mass surveillance is detrimental to the assurance of cyber security in our country. In order to be able to conduct surveillance and ensure that they have access to citizens data, the NSA deliberately weakens the security of consumer products.

> "We have examples of the NSA going in and deliberately weakening security of things that we use so they can eavesdrop on particular targets," said Bruce Schneier, a prominent cryptography writer and technologist. Schneier refer-enced a Reuters report that the NSA paid the computer security firm RSA$10 million to use a deliberately flawed encryption standard to facilitate easier eavesdropping, a charge RSA has denied. "This very act of undermining not only undermines our security. It undermines our fundamental trust in the things we use to achieve security. It's very toxic," Schneier said.[10]

[9]https://www.reuters.com/article/us-usa-security-hearing/google-warns-of-splinter-net-fallout-from-u-s-spying-idUSBRE9AC0S720131113

[10]https://time.com/2966463/nsa-spying-surveillance-cybersecurity-privacy-advocates-schneier/

Not only is the installation of backdoors into consumer products worrisome for the proctetion of those products, it also has economic ramifications for these companies.

> The agency has sought to install "backdoors," hardware and software sys-tems with deliberately weakened security, into some of the most commonly used tech products, as it did in the program codenamed PRISM. American tech companies say this hurts their business in the international marketplace, where users aren't keen to use software that comes bugged by an Ameri-can intelligence agency. Major tech firms, including Google, supported an amendment to the defense budget in May to prohibit the NSA from using funds for this kind of backdoor surveillance.[11]

The effort by the government to continue to seek access to citizen data has only continues in the recent months.

> Member nations of the Five Eyes intelligence-sharing alliance—which in-cludes the United States— along with Japan and India published a state-ment on Sunday calling on tech companies to allow law enforcement to gain backdoor access to communication that uses unbreakable end-to-end encryption.[12]

The perception of these backdoors and the deterioration of our cyber security standards in order for our government to be able to spy on us is harmful to our own democracy but also the rights of businesses. These backdoors could potentially cost companies millions of dollars if our foreign adversaries were able to penetrate through the same backdoors. As more countries seek these backdoors into technological advances into privacy, there are more concerns over the control governments may have over citizen's privacy.

3.2.5 AT: Terrorism

Given that the consistent justification for the creation and continuation of these mass surveillance program has always been to stop terrorism, it would be good for aff teams to have responses prepared for this argument. There are many ways to tackle the issue of terrorism. To start, mass surveillance does not address the root cause of terrorism as terrorism is vastly complex.

[11]https://time.com/2966463/nsa-spying-surveillance-cybersecurity-privacy-advocates-schneier/
[12]https://www.forbes.com/sites/siladityaray/2020/10/12/united-states-six-other-nations-ask-tech-companies-to-build-backdoors-to-encrypted-communications/?sh=1a9978174051

> Both camps make valid points. Yet, they also share important short- comings. The root causes of terrorism and violent radicalism are extremely complex, multifaceted, and often intertwined. They resist simplification and easy cat-egorization. It should therefore be stated from the outset that there is no unique panacea or simple formula to 'end' terrorism and radicalism. In the absence of 'one size fits all' measures, only a long-term and multi- pronged strategy, aimed at strengthening the institutional underpinnings of develop-ment, democracy, and security will achieve effective results [13]

The complexity of terrorism prevents mass surveillance tactics from being effective. Moreover, another line of attack for the aff would be to attack the effectiveness of these programs to deter terrorism in the first place. After Edwards Snowden's massive leak of classified information, there are large amounts of research that have been done to study the effectiveness of surveillance as a counterterrorism measure.

> The largest number of studies on effectiveness examine the actual effective-ness of surveillance technology – assessments and measurements of whether or not a given security program accomplishes its security goal. There is a sig-nificant body of work on evaluation of the effectiveness of counterterrorism measures. Lum et al. (2007), van Dongen (2009), and van Um and Pisoiu (2011) identify the numerous challenges of performing an effectiveness eval-uation, propose approaches to measuring effectiveness, and underline the lack of research in this field. Drakos and Giannakopoulos (2009) establish a formal statistical framework to determine the probability of authorities stopping a terrorist incident over time and the probability of human and property loss. Predictive data mining has been analyzed as a counterter-rorism method and argued to be ineffective (Jonas & Harper, 2006). One study purports to analyze the effectiveness of counterterrorism approaches in six countries, but in reality is an historical account of the terrorism in each country and the counterterrorism policies and practices put in place by the government (Alexander, 2006). A second study by van Dongen (2015) con-structs a new framework for evaluating counterterrorism policies and exam-ines whether there is a relation between the type of terrorist organization and the effectiveness of the counterterrorism approaches applied to combating it.

[13]https://www.brookings.edu/wp-content/uploads/2016/06/summer_fall_radicalism_taspinar.pdf

3.3 Neg Arguments

3.3.1 Terrorism

The main argument that most Neg teams will read will be some version of terrorism. Given that the support of these mass surveillance programs within the government and from cititzens in the perception that they are effective against terrorism. This means that most neg teams will benefit from proving that there are strong sources of terror that exist in the world. One of these sources is nuclear terror.

> But states are no longer the only source of nuclear threats to the U.S. Terror-ist groups also pose a credible threat of attacking the U.S. using nuclear or radiological materials. A nuclear or radiological terrorist attack in a U.S. or other major global city would have severe and possibly devastating politi-cal, security, and economic consequences for the country attacked, as well as globally. The Biden administration will have an opportunity in 2021 to re-energize global efforts to prevent nuclear and radiological terrorism, but it will need to act promptly to do so. Lack of knowledge about weaponizing nuclear or radiological materials is no longer an impediment to nuclear ter-rorism, but lack of nuclear or radiological material is — but these materials are in widespread use globally for a variety of mostly peaceful purposes: 22 countries have at least one kilogram of fissile nuclear material needed for an improvised nuclear bomb, and virtually every country has radiological sources that could be used for a "dirty bomb."[14]

The immediate threat of nuclear terrorism along with the relative ease to produce a dirty bomb creates imminent impact scenarios for the neg team that could be strategic against aff arguments. Another alternative form of terrorism that the neg team can argue would be domestic terrorism. The rise of domestic terror, especially in the second half of 2020, has created new and unique challenges that need to be addressed.

> Based on the data, this analysis has several findings, which are discussed at greater length later in this assessment. First, white supremacists and other like-minded extremists conducted 67 percent of terrorist plots and attacks in the United States in 2020. They used vehicles, explosives, and firearms

[14]https://thehill.com/opinion/national-security/527796-biden-must-act-promptly-to-strengthen-global-efforts-to-prevent

> as their predominant weapons and targeted demonstrators and other indi-viduals because of their racial, ethnic, religious, or political makeup—such as African Americans, immigrants, Muslims, and Jews. Second, there was a rise in the number of anarchist, anti-fascist, and other like-minded attacks and plots in 2020 compared to previous years, which comprised 20 percent of terrorist incidents (an increase from 8 percent in 2019). These types of ex-tremists used explosives and incendiaries in the majority of attacks, followed by firearms. They also targeted police, military, and government personnel and facilities. Third, far-left and far-right violence was deeply intertwined— creating a classic "security dilemma."[6] Since it is difficult to distinguish be-tween offensive and defensive weapons, armed individuals from various sides reacted to each other during protests and riots, and each side's efforts to protect itself and acquire weapons generally threatened others.[15]

In an approach that closely resembles the government's own stance, neg teams will probably find the most offense through reading arguments about imminent threats that need to be topped. This would be the only types of justification that the aff could not argue other types of solvency for.

3.3.2 A2 Privacy

Every aff team will immediately think of privacy arguments to read, meaning that every neg team should be prepared with responses. The aff's concerns over privacy while warranted, do not look at the alternatives that are currently going on. This means that the neg's best line of attack would be to say that privacy is being violated regardless of the NSA or not. In fact, the NSA are not the only actors that are gathering data on citizens.

> Regarding outrage over the NSA's collection of telephone calling records, or metadata, I don't know why anyone would have greater confidence in this information being held by private companies. And given the perceived threat to privacy, it's astonishing how little attention has been paid to the Senate commerce committee's recent report on companies that gather per-sonal information on hundreds of millions of Americans and sell it to mar-keters, often highlighting people with financial vulnerability. Some compa-nies group the data into categories including "rural and barely making it,"

[15]https://www.csis.org/analysis/war-comes-home-evolution-domestic-terrorism-united-states

> "retiring on empty" and "credit crunched: city families." The aim is often to sell financially risky products to transient consumers with low incomes, the report found.[16]

Although the government holding our data may be scary, it is still safer for government officials that know how to handle the data and have rules in place for protecting our citizens through these programs than for private companies retaining data on citizens that don't have to follow the same regulations that our government officials do.

This argument would work best against aff arguments that are dependent on a data col-lection link. If you are able to prove that there are other instances where data collection still happens, examples like social media or consumer data, their impacts also happens. Therefore, reading responses about how other companies are collecting the data of US citizens can act as a way to make your opponent's argument nonunique.

3.4 Conclusion

This is a tricky topic that will confuse many judges if teams aren't careful. It will be especially important to find true, real arguments rather than arguments based off what can happen. As you prepare for this topic, take time to think through how arguments on both sides interact and developing the strongest chain or warrants you can.

[16]https://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html

4 Topic Analysis by Siva Sambasivam

Siva Sambasivam debated in Public Forum for Saratoga High School in California, and is currently a freshman at Indiana University studying Business and Political Science. During his two years on the circuit, he amassed 4 gold bids, along with 2 autoquals to the TOC, placing 5th at the NCFL Grand National Tournament and in the top-14 at NSDA nationals. Most notably, Siva semi-finaled at MiniAp-ple, Santa Clara University, and the Presentation Round Robin; finaled at Golden Desert; placed second at the California Round Robin; and championed the Robert Garcia Invitational, reaching the top-5 of the national rankings his senior year. In-dividually, Siva was the top speaker at Stanford, third speaker at Apple Valley, and fifth speaker at Milpitas. Outside of Public Forum, Siva semifinaled Arizona State University twice in Congress, qualified to Nationals in Congress, and placed 6th in NSDA Nationals Extemporaneous Debate.

4.1 Background

4.1.1 Introduction

Hi y'all!

Welcome to my topic analysis for the January topic: "Resolved: The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents." Ever since the Snowden leaks, the NSA and its domestic surveillance has been a hot button issue in our government, but one that is also seldom discussed by politicians. Most Americans know that surveillance does exist, especially as a result of the recent whistleblowers and publicized leaks of classified intelligence. However, very few Amer-icans actually know how it's happening and the extent to which their privacy is being violated. This will be a cool topic in which debaters might finally get an answer to that question.

Generally speaking, January is a HUGE month for debaters, and a month where nu-merous teams will pick up their quals to the TOC. With 3 octas bid tournaments (Blake, Arizona State University, and Emory), along with a host of other quarters bids (James Logan, Durham, Sunvite), there will be numerous opportunities for you to do well with this topic. Specifically though, I would tailor your prep to focusing on the more techni-cal aspects of this resolution. Blake, ASU and Emory generally all have extremely flow judging pools, and each of those tournaments saw theory and critical arguments being read in elims last year. With a topic like this, which lends itself to numerous arguments with moral and ethical questions, it will be very important to sharpen those technical chops and make sure that you are well prepared heading into rounds.

With that, let's delve right in.

4.1.2 History of NSA Surveillance

After the 9/11 terrorist attacks, there was a need to institute a more comprehensive surveillance plan in our nation. In an effort to ensure that there was never a terrorist attack again, President Bush authorized the National Security Agency to increase their surveillance, and he gave them quite a broad mandate to surveil American citizens.

Since then, NSA surveillance has steadily increased, with recent documents[1] showing that the NSA tracks the phone calls and text messages of "hundreds of millions of Amer-icans." Over the past few years, whistleblowers have come forward to expose the large amount of surveillance that the NSA does, the primary example being Edward Snow-den, a former Central Intelligence Agency employee and subcontractor who leaked a trove of classified documents to the public in June of 2013. Since then, there has been a public outcry and a demand for privacy, however it has fallen on deaf ears. While numerous politicians have promised a reduction in this surveillance, there is very little evidence to show that any such reduction as happened, while smaller leaks continue to show the NSA's broad mandate is still in place.

The most common question asked is how specifically the NSA is allowed to do such a thing in a democratic nation such as America. The answer is: the FISA court. The FISA court is a special court of justices that hear on cases that pertain to national security and rule on them in a closed hearing. Goodwin 18 of Axios writes:

> FISA warrant investigations can't be opened "solely on the basis of First

[1]https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

> Amendment activities." In other words, affiliation with questionable par-ties isn't enough to warrant a FISA case. Evidence the FBI can use to sup-port the claim that the U.S. target is knowingly working on behalf of a for-eign entity can include information gathered from human sources, physi-cal surveillance, bank transactions, or even documents found in the target's trash. Once evidence has been accumulated, the information must be out-lined in an affidavit and application stating the grounds for the FISA warrant. The completed FISA application goes through the FBI chain of command, be-fore making its way to FBI Headquarters to receive approval and sign off by the Special Agent in charge of the field office before making it to the Justice Department where attorneys from the National Security Division vet the ap-plication to verify all the assertions made in it. The FISC then reviews the application in secret, and decides whether to approve the warrant.[2]

For this topic, it is going to be important to understand how the NSA surveillance pro-cess works. Especially because the NSA is not the only government agency that surveils American citizens, understanding the process will be important to delineating your ar-guments from FBI or DOJ surveillance.

4.1.3 Topic-Related Considerations

This topic is going to come down to impact scenarios and weighing. The vast major-ity of arguments won't have amazing link turns or disads to read in response to them. Arguments such as the AFF privacy argument will be generally regarded as true, so it is important to prepare your own weighing as well as common responses to general weighing that teams will read running certain arguments.

Especially since PF has slowly transitioned into an activity with teams spreading tons of arguments and hoping one gets conceded, it will be very nice to have a topic where impact calc and framing will be integral to winning rounds.

[2] https://www.axios.com/what-is-fisa-and-how-does-it-work-nunes-page-f661867c-e8b0-4d72-8b65-8302ad33da29.html

4.2 Affirmative Arguments

4.2.1 Information Overload

When the NSA collects data, it collects a lot of data. And the vast majority of this data trove will be completely useless in preventing terrorist attacks. This has caused many to argue that the data mining is actually *counterproductive* in stopping terrorist attacks as it both diverts resources away from more effective methods, while also decimating counterterror efforts through extremely high error rates. The thesis of this argument is that the mass data collection is simply an information overload for the NSA, and one that prevents effective and efficient counterterror operations. Indeed, Schneier 15 of the Harvard University writes in his book:

> The NSA repeatedly uses a connect-the-dots metaphor to justify its surveil-lance activities. Again and again — after 9/11, after the Underwear Bomber, after the Boston Marathon bombings — government is criticized for not con-necting the dots. However, this is a terribly misleading metaphor. Connect-ing the dots in a coloring book is easy, because they're all numbered and vis-ible. In real life, the dots can only be recognized after the fact. That doesn't stop us from demanding to know why the authorities couldn't connect the dots. The warning signs left by the Fort Hood shooter, the Boston Marathon bombers, and the Isla Vista shooter look obvious in hindsight. Nassim Taleb, an expert on risk engineering, calls this tendency the "narrative fallacy."
>
> Humans are natural storytellers, and the world of stories is much more tidy, predictable, and coherent than reality. Millions of people behave strangely enough to attract the FBI's notice, and almost all of them are harmless. The TSA's no-fly list has over 20,000 people on it. The Terrorist Identities Data-mart Environment, also known as the watch list, has 680,000, 40% of whom have "no recognized terrorist group affiliation."[3]

This offers a good understanding of the problem in the status quo; there are simply too many people that government organizations might suspect of having terrorist ties, and it is simply infeasible for government officials, or even systems, to parse through all of this information in order to generate actionable intelligence. But even if the NSA was able to do this, Schnieder further isolates 3 reasons as to why data mining will never truly work to stop terrorists:

[3]https://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist

> The first, and most important, issue is error rates. For advertising, data min-ing can be successful even with a large error rate, but finding terrorists re-quires a much higher degree of accuracy than data-mining systems can pos-sibly provide. Data mining works best when you're searching for a well-defined profile, when there are a reasonable number of events per year, and when the cost of false alarms is low ... The only cost of a false alarm is a phone call to the cardholder asking her to verify a couple of her purchases
>
> Terrorist plots are different, mostly because whereas fraud is common, ter-rorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be use-less. The reason lies in the mathematics of detection. All detection systems have errors, and system designers can tune them to minimize either false positives or false negatives. In a terrorist detection system, a false positive oc-curs when the system mistakenly identifies something harmless as a threat. A false negative occurs when the system misses an actual attack. Depend-ing on how you "tune" your detection system, you can increase the number of false positives to assure you are less likely to miss an attack, or you can reduce the number of false positives at the expense of missing attacks. Be-cause terrorist attacks are so rare, false positives completely overwhelm the system, no matter how well you tune. And I mean completely: millions of people will be falsely accused for every real terrorist plot the system finds, if it ever finds any.
>
> We saw this problem with the NSA's eavesdropping program: the false pos-itives overwhelmed the system. In the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obligated to investigate all the tips. We also saw this with the Sus-picious Activity Reports —or SAR — database: tens of thousands of reports, and no actual results. And all the telephone metadata the NSA collected led to just one success: the conviction of a taxi driver who sent $8,500 to a Somali group that posed no direct threat to the US — and that was prob-ably trumped up so the NSA would have better talking points in front of Congress.

Indeed, Schwartz of the New Yorker furthers this argument, even giving an example of how the Boston Marathon Bombings could have potentially been prevented without

this mass surveillance:

> By flooding the system with false positives, big-data approaches to coun-terterrorism might actually make it harder to identify real terrorists before they act. Two years before the Boston Marathon bombing, Tamerlan Tsar-naev, the older of the two brothers alleged to have committed the attack, was assessed by the city's Joint Terrorism Task Force. They determined that he was not a threat. This was one of about a thousand assessments that the Boston J.T.T.F. conducted that year, a number that had nearly doubled in the previous two years, according to the Boston F.B.I. As of 2013, the Justice Department has trained nearly three hundred thousand law enforcement of-ficers in how to file "suspicious-activity reports." In 2010, a central database held about three thousand of these reports; by 2012 it had grown to almost twenty-eight thousand. "The bigger haystack makes it harder to find the needle," Sensenbrenner told me. Thomas Drake, a former N.S.A. executive and whistle-blower who has become one of the agency's most vocal critics, told me, "If you target everything, there's no target." Drake favors what he calls "a traditional law-enforcement" approach to terrorism, gathering more intelligence on a smaller set of targets. Decisions about which targets matter, he said, should be driven by human expertise, not by a database.[4]

Schnieder goes on to explain two other reasons as to why data mining is counterpro-ductive, including the fact that each and every terrorist attack is too unique for previous data to accurately identify potential threats and the fact that terrorists are, well, terror-ists. They don't want to be found. Which makes the instances of false positives way higher than even a normal system.

> The second problem with using data-mining techniques to try to uncover terrorist plots is that each attack is unique. Who would have guessed that two pressure-cooker bombs would be delivered to the Boston Marathon fin-ish line in backpacks by a Boston college kid and his older brother? Each rare individual who carries out a terrorist attack will have a disproportion-ate impact on the criteria used to decide who's a likely terrorist, leading to ineffective detection strategies.
>
> The third problem is that the people the NSA is trying to find are wily, and they're trying to avoid detection. In the world of personalized marketing,

[4]https://www.newyorker.com/magazine/2015/01/26/whole-haystack

> the typical surveillance subject isn't trying to hide his activities. That is not true in a police or national security context. An adversarial relation-ship makes the problem much harder, and means that most commercial big data analysis tools just don't work. A commercial tool can simply ignore people trying to hide and assume benign behavior on the part of everyone else. Government data-mining techniques can't do that, because those are the very people they're looking for. Adversaries vary in the sophistication of their ability to avoid surveillance. Most criminals and terrorists — and po-litical dissidents, sad to say — are pretty unsavvy and make lots of mistakes. But that's no justification for data mining; targeted surveillance could poten-tially identify them just as well. The question is whether mass surveillance performs sufficiently better than targeted surveillance to justify its extremely high costs. Several analyses of all the NSA's efforts indicate that it does not.

While negative teams that read arguments about terrorism, and how NSA surveillance is key to stopping terrorists threats both domestically and abroad, Schnieder is quite specific about how there is no potential way to fix these problems. Indeed, he writes:

> The three problems listed above cannot be fixed. Data mining is simply the wrong tool for this job, which means that all the mass surveillance required to feed it cannot be justified. When he was NSA director, General Keith Alexander argued that ubiquitous surveillance would have enabled the NSA to prevent 9/11. That seems unlikely. He wasn't able to prevent the Boston Marathon bombings in 2013, even though one of the bombers was on the terrorist watch list and both had sloppy social media trails — and this was after a dozen post-9/11 years of honing techniques. The NSA collected data on the Tsarnaevs before the bombing, but hadn't realized that it was more important than the data they collected on millions of other people.
>
> This is a critical point. Ubiquitous surveillance and data mining are not suit-able tools for finding dedicated criminals or terrorists. We taxpayers are wasting billions on mass-surveillance programs, and not getting the secu-rity we've been promised. More importantly, the money we're wasting on these ineffective surveillance programs is not being spent on investigation.

In addition to the Boston Marathon Bombings example, these finds seem to be empiri-cally proven true in other countries. Indeed, Volz of the National Journal writes:

> Edward Snowden is pointing to the recent terrorist attacks in France as ev-

> idence that government mass-surveillance programs don't work because they are "burying people under too much data." "When we look at the Paris attacks specifically, we see that France passed one of the most intrusive, ex-pansive surveillance laws in all of Europe last year, and it didn't stop the attack," the fugitive leaker said in an interview with NOS, a Dutch news or-ganization, released Wednesday. "And this is consistent with what we've seen in every country."[5]

While a lot of this evidence is general to the problem of mass surveillance, the situation is amplified for the National Security Agency. Angwin 13 of the Wall Street Journal writes,

> William Binney, creator of some of the computer code used by the National Security Agency to snoop on Internet traffic around the world, delivered an unusual message here in September to an audience worried that the spy agency knows too much. It knows so much, he said, that it can't under-stand what it has. "What they are doing is making themselves dysfunctional by taking all this data," Mr. Binney said at a privacy conference here. The agency is drowning in useless data, which harms its ability to conduct legit-imate surveillance, claims Mr. Binney, who rose to the civilian equivalent of a general during more than 30 years at the NSA before retiring in 2001. Analysts are swamped with so much information that they can't do their jobs effectively, and the enormous stockpile is an irresistible temptation for misuse.[6]

4.2.2 Tech Competitiveness

Another interesting argument on the affirmative is about the US economy, and our tech sector. The argument boils down to the fact that the NSA has mass surveillance pro-grams, undermines the credibility of high-tech companies, by making it seem to the world that their data is insecure and might be taken by the NSA. Indeed, Kehl 14 of New America's Open Technology Institute writes:

> Trust in American businesses has taken a significant hit since the initial re-ports on the PRISM program suggested that the NSA was directly tapping

[5]https://www.nationaljournal.com/s/33264/snowden-frances-intrusive-surveillance-laws-failed-stop-paris-attacks
[6]https://www.wsj.com/articles/SB10001424052702304202204579252022823658850

> into the servers of nine U.S. companies to obtain customer data for national security investigations.28 The Washington Post's original story on the pro-gram provoked an uproar in the media and prompted the CEOs of several major companies to deny knowledge of or participation in the program.29 The exact nature of the requests made through the PRISM program was later clarified,30 but the public attention on the relationship between American companies and the NSA still created a significant trust gap, especially in industries where users entrust companies to store sensitive personal and commercial data. "Last year's national security leaks have also had a com-mercial and financial impact on American technology companies that have provided these records," noted Representative Bob Goodlatte, a prominent Republican leader and Chairman of the House Judiciary Committee, in May 2014. "They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global market-place damaged."[7]

This evidence emphasizes that this argument is purely perception based, which also means it is far easier to win as a link. It doesn't matter if the NSA is actually collabo-rating with US companies on their PRISM program, the fact that many believe this is a possibility erodes trust in said American companies. This means that as long as you win that currently there is a material impact to these companies in terms of economic losses, you win that the perceptual link is true. Kehl continues:

> Economic forecasts after the Snowden leaks have predicted significant, on-going losses for the cloud-computing industry in the next few years. An August 2013 study by the Information Technology and Innovation Founda-tion (ITIF) estimated that revelations about the NSA's PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years.42 On the low end, the ITIF projection suggests that U.S. cloud computing providers would lose 10 percent of the foreign market share to European or Asian competitors, totaling in about $21.5 billion in losses; on the high-end, the $35 billion figure represents about 20 percent of the com-panies' foreign market share. Because the cloud computing industry is un-dergoing rapid growth right now—a 2012 Gartner study predicted global spending on cloud computing would increase by 100 percent from 2012 to

[7] https://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internetfreedom-cybersecurity/

> 2016, compared to a 3 percent overall growth rate in the tech industry as a whole43—vendors in this sector are particularly vulnerable to shifts in the market. Failing to recruit new customers or losing a competitive advantage due to exploitation by rival companies in other countries can quickly lead to a dwindling market share.

While tech companies have made many denials to these claims, there still exists as a mistrust, especially with regards to international customers for US companies. In fact, there is a possibility that the NSA accesses data from companies without their knowl-edge. Eoyang 15 of Third Way writes:

> Allegations of intrusive U.S. government electronic surveillance activities have raised international outcry and created antagonism between U.S. tech-nology companies and the government. Without a bold and enduring re-form, American companies will continue to suffer a competitive disadvan-tage from perceptions of U.S. government intrusion into their data. We pro-pose bringing electronic surveillance collection from U.S. companies into an existing statutory framework in order to reassure international customers and to respect the rights of U.S. companies operating abroad. The Problem In the wake of the Snowden revelations, people around the world have be-come uneasy about the security of their communications that flow through the servers of American companies.1 They now fear—not without reason— that the NSA has broad access to a wide range of their data that may not have any direct relevance to the core foreign policy or security concerns of the United States.2 Snowden has also alleged that the NSA accessed American companies' data without their knowledge.3 American technology compa-nies reacted with outrage to media reports that, unbeknownst to them, the U.S. government had intruded onto their networks overseas and spoofed their web pages or products.4 These stories suggested that the government created and snuck through back doors to take the data rather than come through well-established front doors.[8]

[8]http://www.thirdway.org/report/restoring-trustbetween-us-companies-and-their-government-on-surveillance-issues

4.3 Negative Arguments

4.3.1 Terrorism

The primary argument that most negative teams will read concerns terrorism. This ar-gument is also quite simple. The entire reason mass surveillance exists in America right now is to prevent another terrorist attack like 9/11. Prior to the 2001 attacks, surveillance was minimal in our country. Since then, we've seen a steady rise. Now, it is contestable about whether this surveillance has indeed prevented any major terrorist attacks, but any way you slice it, counterterrorism is the primary purpose of NSA surveillance, and thus will be the primary NEG on this topic. Boot 13 of the Council on Foreign Relations writes:

> After 9/11, there was a widespread expectation of many more terrorist at-tacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon, bombing of), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's moni-toring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terror-ist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists.
>
> For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it. But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence
> — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic,

> Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours.[9]

The biggest weakness in this terrorism argument is the impact scenario. It is easy to win warrants as to why NSA surveillance is good at stopping terror attacks. It is easy to weigh those warrants against the AFF's warrant, as historically, the US has seen far less terrorist attacks and deaths due to terrorist attacks than many other developed countries without as large surveillance programs. However, it is extremely hard to quantify the number of attacks that are staved off, and the magnitude of these attacks. It is going to be extremely hard to win a clean, quantified impact, so instead, you will probably want to read good weighing and at least a couple pieces of evidence that contextualize your impact scenario. For example, Lewis 14 of the Center for Strategic and International Studies writes:

> Americans are reluctant to accept terrorism is part of their daily lives, but at-tacks have been planned or attempted against American targets (usually air-liners or urban areas) almost every year since 9/11. Europe faces even greater risk, given the thousands of European Union citizens who will return hard-ened and radicalized from fighting in Syria and Iraq. The threat of attack is easy to exaggerate, but that does not mean it is nonexistent. Australia's then-attorney general said in August 2013 that communications surveillance had stopped four "mass casualty events" since 2008. The constant planning and preparation for attack by terrorist groups is not apparent to the public. The dilemma in assessing risk is that it is discontinuous. There can be long periods with no noticeable activity, only to have the apparent calm explode. The debate over how to reform communications surveillance has discounted this risk. Communications surveillance is an essential law enforcement and intelligence tool. There is no replacement for it. Some suggestions for alter-native approaches to surveillance, such as the idea that the National Secu-rity Agency (NSA) only track known or suspected terrorists, reflect wishful thinking, as it is the unknown terrorist who will inflict the greatest harm.[10]

Another potential impact magnifier for your argument is the argument that, indepen-dent of the attacks that surveillance directly stops, the fact that we have a mass surveil-

[9]http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609
[10]http://csis.org/publication/underestimating-risk-surveillance-debate

lance program deters terrorist attacks. Indeed, Representative Robert Pittenger of the Congressional Task Force on Terrorism writes in 2014 of writes

> This February, I took that question to a meeting of European Ambassadors at the Organization for Security and Cooperation in Europe. During the con-ference, I asked three questions: 1. What is the current worldwide terrorist threat? 2. What is America's role in addressing and mitigating this threat?
> 3. What role does intelligence data collection play in this process, given the multiple platforms for attack including physical assets, cyber, chemical, bi-ological, nuclear and the electric grid? Each ambassador acknowledged the threat was greater today than before 9/11, with al Qaeda and other extreme Islamist terrorists stronger, more sophisticated, and having a dozen or more training camps throughout the Middle East and Africa. As to the role of the United States, they felt our efforts were primary and essential for peace and security around the world.
>
> Regarding the intelligence gathering, their consensus was, "We want pri-vacy, but we must have your intelligence." As a European foreign min-ister stated to me, "Without U.S. intelligence, we are blind." We cannot yield to those loud but misguided voices who view the world as void of the deadly and destructive intentions of unrelenting terrorists. The number of terrorism-related deaths worldwide doubled between 2012 and 2013, jump-ing from 10,000 to 20,000 in just one year. Now is not the time to stand down. Those who embrace an altruistic worldview should remember that vigilance and strength have deterred our enemies in the past. That same commitment is required today to defeat those who seek to destroy us and our way of life. We must make careful, prudent use of all available technology to counter their sophisticated operations if we are to maintain our freedom and liber-ties.[11]

4.3.2 Foreign Shift

One extremely unique and nuanced argument that I think would play very well on this topic is the argument about a foreign shift with regards to our surveillance. This argu-ment is effectively that when domestic constraints are put on the NSA's ability to surveil,

[11]https://www.washingtonexaminer.com/rep-robert-pittenger-bipartisan-bill-on-nsa-data-collection-protects-both-privacy-and-national-security

they will shift to cooperating with other countries to increase surveillance abroad. In-deed, Chandler of the California International Law Center writes:

> First, the United States, like many countries, concentrates much of its surveil-lance efforts abroad. Indeed, the Foreign Intelligence Surveillance Act is focused on gathering information overseas, limiting data gathering largely only when it implicates U.S. persons. n174 The recent NSA surveillance disclosures have revealed extensive foreign operations. n175 Indeed, con-straints on domestic operations may well have spurred the NSA to expand operations abroad. As the Washington Post reports, "Intercepting commu-nications overseas has clear advantages for the NSA, with looser restrictions and less oversight." n176 Deterred by a 2011 ruling by the Foreign Intelli-gence Surveillance Court barring certain broad domestic surveillance of In-ternet and telephone traffic, n177 the NSA may have increasingly turned its attention overseas.[12]

There is also a current alliance of multiple countries that would enable this shift to be relatively easy for the NSA. Brenner 15 of the University of Pittsburgh writes:

> FThe NSA coordinates its spying closely with Intelligence agencies of the four other English-speaking countries that participate in "Five Finger" al-liance: the UK, Canada, Australia and New Zealand. Their data sharing does not stop at that acquired by legal means. They do each other favors by relying on a partner to circumvent domestic restrictions in any one of them. There are credible reports that NSA has assisted Britain's GCHQ in this re-spect. Both have assisted the German NBD in spying on German targets- as has been revealed within the past few weeks. Therefore, the significance of last week legislation is undercut by this close collaboration.[13]

The reason I like this argument so much is because the impact scenarios are plentiful. There are so many ways to implicate this argument on any given round that it really creates a situation where if you win this argument, you likely win the round. Obvi-ously, you will need to have practiced implicating it to different arguments - for exam-ple, winning that surveillance still happens is likely a takeout to the majority of affir-mative argument, especially ones about privacy and/or racism. On top of that, you can make arguments that this type of surveillance would be more covert and thus less reg-

[12]http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf
[13]http://www.huffingtonpost.com/michael-brenner/the-nsas-second-coming_b_7535058.html

ulated by other government actors making the negative impact of any surveillance far worse. Obviously, reading this argument comes at a cost - you won't be able to read any surveillance good arguments unless you specifically nuance why only current NSA surveillance would be good, and why intel-sharing, or a foreign-shift of surveillance, would not solve your scenario.

4.4 Concluding Thoughts

With such a huge month ahead, the main piece of advice I can give you is to focus on one part of this resolution. This topic is extremely broad, and it is very unlikely that you will be well researched enough on every major argument by the time the first few tournaments roll around. Thus, it is important to master one main argument, and the framing/weighing attached to it. If you know any given argument better than any of your opponents, you are putting yourself in a great position to succeed.

As always, good luck with your tournament endeavours, and always remember to have fun. Feel free to reach out to me over facebook (Siva Sambasivam) or email: siva.m.sambasivam@gmail.com, if you have any questions.

5 Pro Evidence

5.1 Metadata

5.1.1 Mass Surveillance

NSA metadata collection programs survey <u>several billion</u> phone calls per day.

ProPublica 13

ProPublica (independent, nonprofit newsroom that produces investigative journalism with moral force). "FAQ: What You Need to Know About the NSA's Surveillance Programs." ProPublica, August 5, 2013. https://www.propublica.org/article/nsa-data-collection-faq

What information does the NSA collect and how?

We don't know all of the different types of information the NSA collects, but several secret collection programs have been revealed:

A record of most calls made in the U.S., including the telephone number of the phones making and receiving the call, and how long the call lasted. This information is known as "metadata" and doesn't include a recording of the actual call (but see below). This program was revealed through a leaked secret court order instructing Verizon to turn over all such information on a daily basis. Other phone companies, including AT&T and Sprint, also reportedly give their records to the NSA on a continual basis. All together, this is several billion calls per day.

Email, Facebook posts and instant messages for an unknown number of people, via PRISM, which involves the cooperation of at least nine different technology companies. Google, Facebook, Yahoo and others have denied that the NSA has "direct access" to their servers, saying they only release user information in response to a court order. Facebook has revealed that, in the last six months of 2012, they handed over the private

data of between 18,000 and 19,000 users to law enforcement of all types -- including local police and federal agencies, such as the FBI, Federal Marshals and the NSA.

Massive amounts of raw Internet traffic The NSA intercepts huge amounts of raw data, and stores billions of communication records per day in its databases. Using the NSA's XKEYSCORE software, analysts can see "nearly everything a user does on the Internet" including emails, social media posts, web sites you visit, addresses typed into Google Maps, files sent, and more. Currently the NSA is only authorized to intercept Internet communications with at least one end outside the U.S., though the domestic collection program used to be broader. But because there is no fully reliable automatic way to separate domestic from international communications, this program also captures some amount of U.S. citizens' purely domestic Internet activity, such as emails, social media posts, instant messages, the sites you visit and online purchases you make.

The contents of an unknown number of phone calls There have been several reports that the NSA records the audio contents of some phone calls and a leaked document confirms this. This reportedly happens "on a much smaller scale" than the programs above, after analysts select specific people as "targets." Calls to or from U.S. phone numbers can be recorded, as long as the other end is outside the U.S. or one of the callers is involved in "international terrorism". There does not seem to be any public information about the collection of text messages, which would be much more practical to collect in bulk because of their smaller size.

The NSA has been prohibited from recording domestic communications since the pas-sage of the Foreign Intelligence Surveillance Act but at least two of these programs -- phone records collection and Internet cable taps -- involve huge volumes of Americans' data.

5.1.2 AT: Metadata Anonymous

Metadata isn't anonymous – the NSA can collect content and correlates phone records with other types of information.

ProPublica 13

ProPublica (independent, nonprofit newsroom that produces investigative journalism with moral force). "FAQ: What You Need to Know About the NSA's Surveillance Programs." ProPublica, August 5, 2013. https://www.propublica.org/article/nsa-data-collection-faq

It's important to note that the NSA probably has information about you even if you aren't on this target list. If you have previously communicated with someone who has been targeted, then the NSA already has the content of any emails, instant messages, phone calls, etc. you exchanged with the targeted person. Also, your data is likely in bulk records such as phone metadata and Internet traffic recordings. This is what makes these programs "mass surveillance," as opposed to traditional wiretaps, which are authorized by individual, specific court orders.

What does phone call metadata information reveal, if it doesn't include the content of the calls?

Even without the content of all your conversations and text messages, so-called "meta-data" can reveal a tremendous amount about you. If they have your metadata, the NSA would have a record of your entire address book, or at least every person you've called in the last several years. They can guess who you are close to by how often you call someone, and when. By correlating the information from multiple people, they can do sophisticated "network analysis" of communities of many different kinds, personal or professional -- or criminal.

Phone company call records reveal where you were at the time that a call was made, be-cause they include the identifier of the radio tower that transmitted the call to you. The government has repeatedlydenied that it collects this information, but former NSA em-ployee Thomas Drake said they do. For a sense of just how powerful location data can be, see this visualization following a German politician everywhere he goes for months, based on his cellphone's location information.

Even without location data, records of who communicated with whom can be used to discover the structure of groups planning terrorism. Starting from a known "target"

(see above), analysts typically reconstruct the social network ”two or three hops” out, examining all friends-of-friends, or even friends-of-friends-of-friends, in the search for new targets. This means potentially thousands or millions of people might be examined when investigating a single target.

Metadata is a sensitive topic because there is great potential for abuse. While no one has claimed the NSA is doing this, it would be possible to use metadata to algorithmically identify, with some accuracy, members of other types of groups like the Tea Party or Occupy Wall Street, gun owners, undocumented immigrants, etc. An expert in network analysis could start with all of the calls made from the time and place of a protest, and trace the networks of associations out from there.

Phone metadata is also not “anonymous” in any real sense. The NSA already maintains a database of the phone numbers of all Americans for use in determining whether some-one is a “U.S. person” (see below), and there are several commercial number-to-name services in any case. Phone records become even more powerful when they are corre-lated with other types of data, such as social media posts, local police records and credit card purchase information, a process known as intelligence fusion.

5.1.3 Warrantless

Metadata surveillance programs are effectively warrantless surveillance.

ProPublica 13

ProPublica (independent, nonprofit newsroom that produces investigative journalism with moral force). "FAQ: What You Need to Know About the NSA's Surveillance Programs." ProPublica, August 5, 2013. https://www.propublica.org/article/nsa-data-collection-faq

Does the NSA need an individualized warrant to listen to my calls or look at my emails?

It's complicated, but not in all cases. Leaked court orders set out the "minimization" procedures that govern what the NSA can do with the domestic information it has inter-cepted. The NSA is allowed to store this domestic information because of the technical difficulties in separating foreign from domestic communications when large amounts of data are being captured.

Another document shows that individual intelligence analysts make the decision to look at previously collected bulk information. They must document their request, but only need approval from their "shift coordinator." If the analyst later discovers that they are looking at the communications of a U.S. person, they must destroy the data.

However, if the intercepted information is "reasonably believed to contain evidence of a crime" then the NSA is allowed to turn it over to federal law enforcement. Unless there are other (still secret) restrictions on how the NSA can use this data this means the police might end up with your private communications without ever having to get approval from a judge, effectively circumventing the whole notion of probable cause.

This is significant because thousands or millions of people might fall into the extended social network of a single known target, but it is not always possible to determine whether someone is a U.S. person before looking at their data. For example, it's not usu-ally possible to tell just from someone's email address, which is why the NSA maintains a database of known U.S. email addresses and phone numbers. Internal documents state that analysts need only "51% confidence" that someone is a non-U.S. person be-fore looking at their data, and if the NSA does not have "specific information" about someone, that person is "presumed to be a non-United States person."

Also, the NSA is allowed to provide any of its recorded information to the FBI, if the FBI specifically asks for it.

5.2 PRISM

5.2.1 Secrecy

PRISM surveys millions of Americans in secrecy away from judicial review.

Toomey 18

Patrick Toomey (Senior Staff Attorney, ACLU National Security Project). "The NSA Continues to Violate Americans' Internet Privacy Rights." *American Civil Liberties Union*, August 22, 2018. https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy

A federal court will be scrutinizing one of the National Security Agency's worst spying programs on Monday. The case has the potential to restore crucial privacy protections for the millions of Americans who use the internet to communicate with family, friends, and others overseas.

The unconstitutional surveillance program at issue is called PRISM, under which the NSA, FBI, and CIA gather and search through Americans' international emails, inter-net calls, and chats without obtaining a warrant. When Edward Snowden blew the whistle on PRISM in 2013, the program included at least nine major internet companies, including Facebook, Google, Apple, and Skype. Today, it very likely includes an even broader set of companies.

The government insists that it uses this program to target foreigners, but that's only half the picture: In reality, it uses PRISM as a backdoor into Americans' private com-munications, violating the Fourth Amendment on a massive scale. We don't know the total number of Americans affected, even today, because the government has refused to provide any estimate.

This type of unjustifiable secrecy has also helped the program evade public judicial re-view of its legality because the government almost never tells people that it spied on them without a warrant. Indeed, the government has a track record of failing to tell Americans about this spying even when the person is charged with a crime based on the surveillance. That's one reason why this case is so important — this time, the gov-ernment has admitted to the spying.

In this case, the government accused a Brooklyn man, Agron Hasbajrami, of attempting to provide material support to a designated terrorist organization in Pakistan. After he

pleaded guilty to one of the charges, the government belatedly admitted that it had read through his emails without a warrant.

Now Mr. Hasbajrami has challenged the government's warrantless surveillance and is asking the Second Circuit Court of Appeals to throw out the resulting evidence. The American Civil Liberties Union and the Electronic Frontier Foundation are supporting him as friends-of-the-court, arguing that the surveillance was unconstitutional (the brief we filed is here). At the hearing on Monday, we'll explain to a three-judge panel why the Fourth Amendment requires the government to get a warrant when it wants to exploit the communications of Americans who are swept up in PRISM.

This large-scale internet surveillance grew out of the Bush administration's post-9/11 warrantless wiretapping program. It is conducted under a controversial law known as Section 702 of the Foreign Intelligence Surveillance Act. Relying on Section 702, the gov-ernment intercepts billions of international communications — including many sent or received by Americans — and it hunts through them in investigations that have nothing to do with national security.

5.2.2 AT: Foreign Targets

This isn't a defense because the government has admitted its purpose is to spy on Americans without warrants through a backdoor.

Toomey 18

Patrick Toomey (Senior Staff Attorney, ACLU National Security Project). "The NSA Continues to Violate Americans' Internet Privacy Rights." *American Civil Liberties Union*, August 22, 2018. https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy

The government attempts to defend this spying by pointing out that its "targets" are foreigners located abroad. But this is no defense at all. Americans regularly communi-cate with individuals overseas, and the government uses PRISM surveillance to collect and sift through many of these private communications. The government has even ad-mitted that one of the purposes of Section 702 is to spy on Americans' international communications without a warrant.

The government casts a wide net, making it easy for innocent Americans who communi-cate with family, friends, and others overseas to be swept up. Relying on a single court order, the NSA uses Section 702 to put more than 125,000 targets under surveillance each year. These individuals need not be spies, terrorists, or accused of any wrongdo-ing — they can be journalists, business people, university researchers, or anyone else who may have information bearing remotely on "foreign affairs."

PRISM is a warrantless wiretapping program that operates around the clock, vacuuming up emails, Facebook messages, Google chats, Skype calls, and the like. Government agents do not review all of the information in real-time — there's simply too much of it. Instead, the communications are pooled together and stored in massive NSA, FBI, and CIA databases that can be searched through for years to come, using querying tools that allow the government to extract and examine huge amounts of private information.

5.2.3 Executive Power

PRISM allows for unchecked executive branch power on national security policy.

Toomey 18

Patrick Toomey (Senior Staff Attorney, ACLU National Security Project). "The NSA Continues to Violate Americans' Internet Privacy Rights." *American Civil Liberties Union,* August 22, 2018. https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy

One of the most problematic elements of this surveillance is the government's use of "backdoor searches" to investigate individual Americans. Although the government says PRISM is targeted at foreigners who lack Fourth Amendment privacy rights, it sys-tematically combs through its PRISM databases for the emails and messages of Ameri-cans. Indeed, FBI agents around the country routinely search for the communications of specific Americans using their names or email addresses — including at the earliest stages of domestic criminal investigations.

The result is an end-run around the Fourth Amendment. Investigators have easy ac-cess to a trove of Americans' private emails, calls, and messages, without ever seeking individualized approval from any judge, as the Constitution requires.

This surveillance leaves far too much unchecked power in the hands of executive branch officials. Today, that includes President Trump, who as a candidate called for expanded spying on Americans. The ACLU is taking on this threat to Americans' privacy rights, just as we challenged the government's warrantless wiretapping across both the Bush and Obama administrations. Now the courts must do their part to ensure that Ameri-cans' online communications receive the full protection of the Fourth Amendment.

5.3 AT: National Security

5.3.1 Already Out of Use

Impact is empirically denied – they stopped using the program for 6 months and no one noticed

Volz and Strobel 19

Dustin Volz and Warren P. Strobel (cover cybersecurity and intelligence for The Wall Street Journal). "NSA Recommends Dropping Phone-Surveillance Program." Wall Street Journal, April 24, 2019. https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247

There have been signs in recent weeks that the NSA is ready to drop the program. A national-security adviser for the Republican congressional leadership, Luke Murry, said in a March podcast interview with the Lawfare security blog that the NSA hadn't used the program in the six months prior.

"They tried to set up this compromise program, and it appears it just didn't really work," said David Kris, former head of the Justice Department's national-security division and founder of Culper Partners LLC, a consulting firm. "Some compromises are good for both sides of the debate, and some are good for neither."

Support for the phone-records program also appears to be receding in Congress. Sen. Mark Warner of Virginia, the top Democrat on the Senate Intelligence Committee, told the Journal that he doesn't currently believe it should be renewed.

"At this point I think it's going to be a pretty tough argument for them to make," Mr. Warner said. "I'll listen to whatever case they want to present, but I'm not convinced at this point that the advantages of the program have been worth the trouble."

Last month, a bipartisan group of lawmakers introduced legislation to end the NSA's domestic metadata program, saying it has never stopped a terrorist attack and continues to run afoul of civil liberties.

5.3.2 Costs

It's cost inefficient – the NSA spent $100 million to achieve <u>one</u> significant investigation.

Savage 20

Charlie Savage (Washington correspondent for The New York Times). "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads." New York Times, February 25, 2020. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

WASHINGTON — A National Security Agency system that analyzed logs of Americans' domestic phone calls and text messages cost $100 million from 2015 to 2019, but yielded only a single significant investigation, according to a newly declassified study.

Moreover, only twice during that four-year period did the program generate unique information that the F.B.I. did not already possess, said the study, which was produced by the Privacy and Civil Liberties Oversight Board and briefed to Congress on Tuesday.

"Based on one report, F.B.I. vetted an individual, but, after vetting, determined that no further action was warranted," the report said. "The second report provided unique information about a telephone number, previously known to U.S. authorities, which led to the opening of a foreign intelligence investigation."

The report did not reveal the subject matter of the one significant F.B.I. investigation that was spurred by the Freedom Act program, and it did not divulge its outcome.

But the high expense and low utility of the call records collected sheds new light on the National Security Agency's decision in 2019 to shutter the program amid recurring tech-nical headaches, halting a counterterrorism effort that has touched off disputes about privacy and the rule of law since the Sept. 11, 2001, attacks.

The information surfaced as Congress was weighing whether to allow the law that au-thorizes the agency to operate the system — the USA Freedom Act of 2015 — to expire on March 15, or whether to accede to the Trump administration's request that lawmak-ers extend the statute, so the agency could choose to turn the system back on in the future.

5.3.3 Encryption

Encrypted apps make surveillance mostly useless.

Savage 20

Charlie Savage (Washington correspondent for The New York Times). "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads." New York Times, February 25, 2020. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

The House Judiciary Committee will meet on Wednesday to consider a draft bill that would adjust surveillance law in several ways, including terminating the program's au-thority. Separately on Tuesday, Attorney General William P. Barr met with Republican senators to urge them to extend three other investigative powers also set to expire on March 15.

The privacy board is an independent agency created by Congress on the recommenda-tion of the commission that studied the Sept. 11 attacks. A declassified, partly censored version of the board's 103-page report was obtained by The New York Times.

In an interview, the board's chairman, Adam I. Klein, praised the National Security Agency for deciding last year to suspend the program — not only because of its high cost and low value, but because of continuing problems in which telecommunications companies kept sending the agency more people's phone records than it had legal au-thority to collect.

"It shows a lot of judgment to acknowledge that something that consumed a lot of re-sources and time did not yield the value anticipated," Mr. Klein said. "We want agen-cies to be able to reflect on their collection capabilities and wind them down where appropriate. That's the best way to ensure civil liberties and privacy are balanced with operational needs."

In a statement appended to the report, Mr. Klein also noted that phone records were becoming less important as people shifted to using encrypted chat apps. And, he noted, the government could still gain access to some phone logs through other means, like tra-ditional subpoenas for records of discrete accounts, or N.S.A. collection abroad, where there are fewer legal limits.

5.3.4 Err Pro

We should treat national security claims with skepticism. Experts have incentives to exaggerate risks and take threats more seriously than they actually are.

Shaw 17

Jonathan Shaw ('89, managing editor of Harvard Magazine). "The Watchers." Harvard Magazine, JANUARY-FEBRUARY 2017. https://harvardmagazine.com/2017/01/the-watchers

Openness: "We Have to be Extremely Skeptical"

IT MAY SEEM LOGICAL for a centralized military organization to provide national cy-bersecurity and defend against cyber war. But Yochai Benkler points out how 9/11 led to war and "unjustified claims for extending surveillance powers, or extending detention and kidnapping powers, let alone torture." The Berkman professor for entrepreneurial legal studies argues that "We have to be extremely skeptical of claims made in the name of national security in general, not because the people making them are bad people, but because the people making them…operate in a world where the only downside to fail-ing to extend their power is that one day somebody will look at them and say, 'Where were you when the world came down?'

"We should take with many grains of salt the claims of national security experts who see cyber war as the next domain," he continues, "and operate in an environment where they want to control everything as much as possible in order to minimize risks, but come to their conclusions from a framework that…is relatively insulated from potential alternative viewpoints."

Accordingly, Benkler advocates systems that allow personal data to remain in the hands of consumers—minimizing the privacy risks posed by governments, corporations, and hackers because personal information is not concentrated in a single place. (The techni-cal term is "distributed network ecosystems based on open-source software.") "Relying on a small number of high-end companies to provide security creates a single point of failure for hundreds of millions," he says, referring to the 2014 theft of Yahoo user ac-counts. "If all those…people had decentralized email storage at home, and sign-on cre-dentials that were not valid for diverse critical sites, collecting [that information] would be much harder."

"It's a challenge to get people to adopt safe habits," he admits, "but it's not impossible.

You have to change users' culture, and you have to design secure systems that are under the control of end users, not single companies." The iPhone, secured with a PIN or a fingerprint, is an example of such encrypted, secure-by-default systems. Such devices aren't hard to build—but, he says pointedly, "It's hard to do so [within] a business model that depends on spying on your customers so you can sell them to advertisers."

Furthermore, says Benkler, systems built in part with "free software developed by com-munities that don't have the imperatives either of profit-making companies, or of deal-ing with the tensions between rights and the state of emergency, get better as their vul-nerabilities are constantly probed, exposed, and then corrected in a constant, evolution-ary, back and forth." Such robustness is obviously desirable.

But it may not be as practicable as he hopes. Although the idea that users can enjoy more privacy and better security in a distributed computing environment is becoming more tangible as smartphones' computing power rivals that of desktops, executing it consistently poses significant challenges. Ben Adida, a software engineer and architect and former fellow of Harvard's Center for Research on Computation and Society, ac-knowledges this is "the vision that many security advocates, myself included, pushed for for a very long time."

But now he thinks "we are far less secure" adopting that technological approach. (For a computer scientist's perspective, and a description of a project to protect research data involving human subjects, see the online extra, "The Privacy Tools Project.") Adida de-veloped Helios, one of the first encrypted yet verifiable online voting systems; he's now head of engineering at Clever, a startup that manages private student data for schools. Providing security to a range of companies has led him to discover how easy it is for small companies to err when implementing and defending the security of their systems, whether in cryptography, access control, network-level security, or in the internal au-dit processes used to ensure data is compartmentalized. A large company like Google, on the other hand, "does a really good job of making sure that only I can log in," he explains. "They've added two-factor authentication, they have all sorts of heuristics to check whether a person is logging in from a different location than usual. There's all sorts of work that they do to make sure that only the right people are accessing the right data."

Like Benkler, Adida agrees that centralized data is too easily accessed by law enforce-ment, but says that for now, "We need to rethink how to defend that data through a combination of legal and technical means." Technically, that might mean discarding chats more than few months old, for example; and legally, resisting official requests for

user data in court. He advocates "evolution in the law, too." The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…," but historically, that has been interpreted to mean that obtaining data held by a third party doesn't require a search warrant. That means personal documents stored in Google's cloud, for example, are ex-posed. Adida says he nevertheless keeps "extremely private data hosted by a third party because that is the right operational thing to do. Everybody hosting their own stuff just doesn't make any sense"—but he hopes that someday, if the government wants access to that information, it "would require a warrant, just as if they were knocking down someone's door."

5.3.5 Intelligence Shift

No longer a priority – intelligence collection is shifting towards Chinese and Russian adversaries

Volz and Strobel 19

Dustin Volz and Warren P. Strobel (cover cybersecurity and intelligence for The Wall Street Journal). "NSA Recommends Dropping Phone-Surveillance Program." Wall Street Journal, April 24, 2019. https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247

"The candle is not worth the flame," one former senior intelligence official said about the phone-records program. Former officials also said the push to unplug the operation coincided with an NSA retooling that reflects a broader U.S. intelligence shift from coun-terterrorism to tracking the strategic intentions of adversarial nations, such as China and Russia.

The new system has been difficult to manage. For example, the NSA said last year it had purged hundreds of millions of records it had collected since 2015 because telecom-munications firms had supplied records NSA hadn't been authorized to obtain under the law.

5.3.6 No Evidence

There's no evidence of national security benefits – the NSA has admitted as much.

Eddington 19

Patrick Eddington (Policy Analyst in Homeland Security and Civil Liberties at the Cato Institute). "The Snowden Effect, Six Years On." *Just Security*, June 6, 2019. https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

Six years ago, the world was introduced to a previously unknown government contrac-tor who revealed the National Security Agency (NSA) was conducting an unparalleled level of warrantless electronic surveillance. Edward Snowden's explosive revelations about NSA's telephone metadata collection program triggered an uproar at home and abroad, culminating in the 2015 passage of the USA Freedom Act—legislation that sup-porters claimed would "end" the kind of mass surveillance Snowden had exposed to the world.

During the debate over Snowden's revelations, federal officials (including President Barack Obama) asserted the surveillance program had saved lives—going so far as to claim, without any evidence, that the program had foiled dozens of terrorist plots against the United States. And even after Obama's own hand-picked review group found the telephone metadata program not worth it (as did the Privacy and Civil Liber-ties Oversight Board (PCLOB) in their report), Congress renewed the program in 2015 via the USA Freedom Act.

Supporters claimed the new legislation would effectively end the NSA bulk telephone metadata program. Others, including myself, felt the bill was somewhere between ter-rible and disastrous, because its reforms didn't go far enough. Last year, critics who predicted that USA Freedom Act would not end NSA's telephone bulk collection were, ironically, vindicated by the Office of the Director of National Intelligence, which admit-ted that in fact three times as much American telephone data was being collected than before the law's enactment.

Amazingly, earlier this year NSA recommended to President Donald Trump that the telephone metadata program be terminated, claiming the program was too cumbersome to continue to execute and not worth the effort—a tacit admission that critics were right all along.

5.3.7 Not Worth It

The NSA wants to drop it – logistical and legal burdens outweigh intelligence benefits.

Volz and Strobel 19

Dustin Volz and Warren P. Strobel (cover cybersecurity and intelligence for The Wall Street Journal). "NSA Recommends Dropping Phone-Surveillance Program." Wall Street Journal, April 24, 2019. https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247

The National Security Agency has recommended that the White House abandon a surveillance program that collects information about U.S. phone calls and text mes-sages, saying the logistical and legal burdens of keeping it outweigh its intelligence benefits, according to people familiar with the matter.

The recommendation against seeking the renewal of the once-secret spying program amounts to an about-face by the agency, which had long argued in public and to con-gressional overseers that the program was vital to the task of finding and disrupting terrorism plots against the U.S.

The latest view is rooted in a growing belief among senior intelligence officials that the spying program provides limited value to national security and has become a logistical headache.

Frustrations about legal-compliance issues forced the NSA to halt use of the program earlier this year, the people said. Its legal authority will expire in December unless Congress reauthorizes it.

It is up to the White House, not the NSA, to decide whether to push for legislation to re-new the phone-records program. The White House hasn't yet reached a policy decision about the surveillance program, according to the people familiar with the matter.

The White House National Security Council and the NSA declined to comment.

The surveillance program began clandestinely—and, at first, without court approval— under the George W. Bush administration in the aftermath of the Sept. 11, 2001, attacks. The NSA operation has sought to collect the metadata of all domestic calls in the U.S. in order to hunt for links among potential associates of terrorism suspects. Metadata include the numbers and time stamps of a call or text message but not the contents of the conversation.

Former intelligence contractor Edward Snowden leaked the existence of the program— along with a tranche of documents exposing other surveillance operations carried out by the NSA—to journalists nearly six years ago. The disclosures ignited an international uproar over the scope of America's electronic-spying capabilities.

The Wall Street Journal reported last month that the NSA was considering ending the metadata program but that such conversations were in the early stages.

Following Mr. Snowden's 2013 disclosures, Congress passed the USA Freedom Act in 2015, requiring the spy agency to replace its bulk-metadata program with a pared-down system under which call records are retained by telephone companies. But that new sys-tem has run into compliance issues and is now viewed by many within the intelligence community as more of a burden than a useful tool.

5.3.8 AT: Any Risk of Terrorism

Even the one significant lead related to a few thousand dollars being donated --- not a terrorist attack.

Savage 20

Charlie Savage (Washington correspondent for The New York Times). "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads." New York Times, February 25, 2020. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

The Times reported last year that the National Security Agency had delivered a bleak internal assessment of the call records program's steep costs and minimal benefits with-out taking an explicit position on whether the Trump administration should seek to extend the law that authorized it. But the specific figures undergirding that briefing were previously classified.

The privacy board, working with the intelligence community, got several additional salient facts declassified as part of the rollout of its report. Among them, it officially disclosed that the system has gained access to Americans' cellphone records, not just logs of landline phone calls.

It also disclosed that in the four years the Freedom Act system was operational, the National Security Agency produced 15 intelligence reports derived from it. The other 13, however, contained information the F.B.I. had already collected through other means, like ordinary subpoenas to telephone companies.

The report cited two investigations in which the National Security Agency produced reports derived from the program: its analysis of the Pulse nightclub mass shooting in Orlando, Fla., in June 2016 and of a February 2016 incident in Ohio where a man attacked people at a restaurant with a machete. But it did not say whether the investigations into either of those attacks were connected to the two intelligence reports that provided unique information not already in the possession of the F.B.I.

The system traces back to a secret decision by President George W. Bush to unleash the National Security Agency from certain legal constraints after the Sept. 11 attacks. Among other things, the agency began collecting customer calling records in bulk from several large telecoms. Counterterrorism analysts used the data as a map of social links,

hunting for hidden associates of known terrorism suspects by looking at indirect con-nections.

In 2006, the Foreign Intelligence Surveillance Court secretly blessed the program under a legally disputed interpretation of the Patriot Act. In 2013, the program's existence was leaked by the former National Security Agency contractor Edward J. Snowden, prompt-ing an uproar over privacy rights and the rule of law.

Defenders of the program claimed that it could have stopped the Sept. 11 attacks. But in practice, its most concrete accomplishment, according to a 2014 report by the Privacy and Civil Liberties Oversight Board, was leading the F.B.I. to scrutinize a San Diego man who turned out to have donated several thousand dollars to the Shabab, the Islamist group in Somalia. There was no accusation that he was planning to a terrorist attack.

5.3.9 AT: Future Use

Allowing intelligence agencies access to information based on a purported future use is dangerous and ignores how programs could be reauthorized if they become necessary later.

Franklin 20

Sharon Bradford Franklin (policy director at New America's Open Technology Institute and the former executive director of the Privacy and Civil Liberties Oversight Board). "Congress Needs to Throw This Surveillance Program Away." *Slate*, January 27, 2020. https://slate.com/technology/2020/01/usa-freedom-act-renewal-section-215-cdr.html

Finally, as a matter of principle, intelligence agencies should not be given every tool they may want, but only those that they need, and only those that can be implemented in a manner that protects individual rights. Intelligence work is difficult, and foreign intelligence information can come from unexpected sources. But this does not mean that intelligence agencies should be given broad authorities to monitor everyone all the time. If, at some future date, our intelligence agencies conclude that collecting a new type of "session identifying information" on an ongoing basis would provide needed intelligence on terrorists and other valid targets, they can go back to Congress at that time to seek a new authority tailored to the new need, one that incorporates robust safeguards for privacy and human rights.

NSA surveillance programs won't be useful in the future, either!

Franklin 20

Sharon Bradford Franklin (policy director at New America's Open Technology Institute and the former executive director of the Privacy and Civil Liberties Oversight Board). "Congress Needs to Throw This Surveillance Program Away." *Slate*, January 27, 2020. https://slate.com/technology/2020/01/usa-freedom-act-renewal-section-215-cdr.html

Perhaps more importantly, the Section 215 CDR program is not effective in producing valuable intelligence. Scholars who have examined the technical features of the Section 215 CDR program have concluded that not only has the program been ineffective since its inception in 2015, but it is unlikely to be effective in the future. In June 2018, the NSA announced that it had discovered "technical irregularities" in some of the CDRs it had acquired, and that the NSA had received records it was not entitled to collect. As

a result, the NSA decided to purge all of the CDRs it had collected since the program began in late 2015. Several months later, the NSA suspended operation of the program altogether. As former Director of National Intelligence Dan Coats explained in an Au-gust 2019 letter to Congress, the intelligence community made the decision to suspend the program based on "balancing the program's relative intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities" of operating this program. The Privacy and Civil Liberties Oversight Board, which con-cluded in its 2014 report that the earlier bulk collection program had been ineffective, has also reviewed the current Section 215 CDR program and agreed with the intelligence community's assessment that it should be suspended. In short, this highly complex au-thority simply isn't worthwhile.

5.3.10 AT: Covid-19

Disease surveillance is not empirically effective and risks increasing surveillance.

Gallagher 20

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

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

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

Many of the approaches governments are taking have never been tried before. We are lab rats in a technological experiment, and it may take years before we learn the results. In some countries, forms of digital surveillance will undoubtedly provide some useful insights, helping epidemiologists to better understand the spread of the virus. In others, governments will use the moment to expand the reach of invasive technology, with little benefit to the pandemic recovery. Both of these outcomes, like the virus itself, will leave a legacy felt by future generations.

For Shoshana Zuboff, author of The Age of Surveillance Capitalism and a professor emerita at the Harvard Business School, one of the primary dangers is that democratic nations lurch toward authoritarian models in their efforts to contain Covid-19. "Those in power have long understood that times of crisis are opportunities for states of exception that allow all manner of ills to be rushed into normalization before anybody has even pulled up their socks," says Zuboff. Her post-pandemic outlook, however, remains tinged with optimism. "I don't agree that we are doomed to a future of biosurveillance and dystopia," she says. "There is nothing here that is inevitable. But it means that we have to rouse ourselves. And we have to move forward, doubling down on democracy as the way out of this."

5.4 AT: Political Controversy

5.4.1 Bipartisan

There is bipartisan skepticism towards NSA surveillance.

Franklin 20

Sharon Bradford Franklin (policy director at New America's Open Technology Institute and the former executive director of the Privacy and Civil Liberties Oversight Board). "Congress Needs to Throw This Surveillance Program Away." *Slate*, January 27, 2020. https://slate.com/technology/2020/01/usa-freedom-act-renewal-section-215-cdr.html

Fortunately, during the House and Senate Judiciary Committee hearings last fall, many members of Congress seemed aware of these issues, and thus skeptical of the govern-ment's request for reauthorization of the CDR program. And encouragingly, later in November, Sens. Richard Burr and Mark Warner, the chair and ranking member of the Senate Select Committee on Intelligence, respectively, introduced S. 2939, the Protecting Against International Terrorism Act, a bill that would "terminate" the Section 215 CDR program. Sens. Ron Wyden and Steve Daines and Reps. Zoe Lofgren, Warren David-son, and Pramila Jayapal have also introduced the Safeguarding Americans' Private Records Act, which would revoke the authority for the CDR program. It is likely that there will soon be additional surveillance reform legislation introduced in the House that would end the CDR program as well. As Congress considers key reforms to U.S. surveillance authorities, it is time to abolish the Section 215 CDR program.

The notion that we can never let a surveillance program expire because we never know when it may be useful may be tempting, but it is also dangerous. From the Church Committee's comprehensive investigation of domestic spying in the 1970s to the Snow-den revelations of the last decade, Americans have seen too many reminders of how surveillance powers can be abused.

5.5 Rights

5.5.1 Abolish the NSA

The NSA massively infringes on rights while returning no national security benefits.

Bailey 15

Ronald Bailey (the science correspondent for Reason). "Abolish the Intelligence-Industrial Complex." *Reason*, January 6, 2015. https://reason.com/2015/01/06/abolish-the-intelligence-industrial-comp/

In a 2012 Wired magazine article, former NSA cryptographer William Binney warned, "We are, like, that far from a turnkey totalitarian state." His chief concern is the massive increase in the capabilities of the NSA to watch and monitor the activities of Americans.

So let us turn now to the sorry record of the National Security Agency. First, who can ever forget the bald-faced lie of Director of National Intelligence James Clapper to Congress about the extent of NSA spying on the communications of millions of Ameri-cans?

The veil over the activities of this most secretive of spy bureaucracies was partly lifted by the revelations of whistleblower Edward Snowden in 2013. No doubt about it, the ability to intercept and decode the messages sent by adversaries can provide valuable insights into their intentions and their tactics. The problem is that the agency has turned its vast surveillance capabilities toward spying on the private communications of millions of Americans. This is an egregious violation of Fourth Amendment rights of Americans to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," unless a court issues a warrant based upon probable cause specifying the particular places, people, and items to be searched.

Instead, as Internet security expert Bruce Schneier told a Cato Institute conference last year, ""The NSA has turned the Internet into a giant surveillance platform." In response to Snowden's revelations, NSA director Keith Alexander essentially lied to Congress when he claimed that the NSA's spying had contributed to thwarting 54 terrorist plots. In January, 2014, the New America Foundation think-tank issued a report that con-cluded that NSA domestic spying had had "no discernible impact on preventing acts of terrorism." It certainly had no discernible impact on thwarting the Boston Marathon bombings in 2013 or the would-be Christmas jetliner bomber in 2009.

Also in January, President Obama's own Privacy and Civil Liberties Oversight Board (PCLOB) issued a report on the NSA's domestic spying program that damningly found, "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 countert-errorism investigation." The report added, "Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown ter-rorist plot or the disruption of a terrorist attack."

"Permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens," the PCLOB also warned. Its report further noted that "while the danger of abuse may seem remote, given historical abuse of personal information by the government during the twentieth century, the risk is more than merely theoretical."

Similarly, in December President Obama own hand-picked Review Group on Intelli-gence and Communications Technologies issued a report that found the NSA domestic spying was "not essential to preventing attacks." But more importantly, the Review Group worried if there is another significant terrorist attack that "many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy." They added, "The powerful existing and potential capabilities of our intel-ligence and law enforcement agencies might be unleashed without adequate controls. Once unleashed, it could be difficult to roll back these sacrifices of freedom." That's exactly right, which is why the NSA needs to be abolished now.

Abolishing the NSA reinstates transparency and liberty.

Bailey 15

Ronald Bailey (the science correspondent for Reason). "Abolish the Intelligence-Industrial Complex." *Reason*, January 6, 2015. https://reason.com/2015/01/06/abolish-the-intelligence-industrial-comp/

President Obama's response to the manifold failures and blatant violations of civil lib-erties perpetrated by the CIA and NSA has been totally inadequate. The December 26, 2014 New York Times offered this explanation: "Many presidents tend to be smitten with the instruments of the intelligence community. I think Obama was more smitten than most," said one former senior Obama administration official, speaking on the con-dition of anonymity to discuss classified intelligence matters.

In 1970, the Defense Science Board Task Force on Secrecy led by physicist Frederick Seitz was asked to evaluate the usefulness of the policy of classifying information as secret. The report concluded that the amount of "information which is classified could profitably be decreased perhaps as much as 90 percent." Even more intriguingly, the task force speculated that "more might be gained than lost if our nation were to adopt— unilaterally, if necessary—a policy of complete openness in all areas of information."

In 1994, former CIA operative and foreign policy analyst William Pfaff argued, "The useful information today is that supplied by area specialists, historians and ethnologists, and through conventional diplomatic observation and journalism. The United States government needs intelligence, not spying. There is a difference."

These insights about the value of transparency and seeking advice from independent scholars are even more apposite in the Internet era.

Given their massive records of incompetence and the inherent threat of secret govern-ment to undermine the liberty of citizens, both the CIA and the NSA should be abol-ished. As Moynihan urged nearly 25 years ago the State Department would be tasked with collecting political intelligence and the Defense Department would monitor for-eign military enemies. It is often claimed that we live in a dangerous world, but it is not at all clear that the CIA and NSA have made it a less menacing place.

5.5.2 Right to Privacy

NSA surveillance violates the right to privacy – that's unconstitutional

York 14

Jillian York (Director for International Freedom of Expression at the Electronic Frontier Foundation). "The Harms of Surveillance To Privacy, Expression And Association." *Global Information Society Watch*, 2014.

The equal rights to privacy, speech and association

When we talk about surveillance, it often follows that we speak of the importance of privacy, of being free from observation or disturbance, from public attention. In the US, privacy is a fundamental right, enshrined in the Fourth Amendment to the Constitution.

Of course, this is no coincidence – under King George II, the American colonisers found themselves at the mercy of writs of assistance, court-issued orders that allowed the King's agents to carry out wide-ranging searches of anyone, anytime; a precursor to the modern surveillance state.4 Once issued, an individual writ would be valid for the King's entire reign, and even up to six months past his death.

It was only after the death of King George II that a legal challenge was mounted. When a customs officer in Boston attempted to secure new writs of assistance, a group of Boston merchants, represented by attorney James Otis, opposed the move. Otis argued that the writs placed "the liberty of every man in the hands of every petty officer," an argument that founding father John Adams later claimed "breathed into this nation the breath of life." It was from this societal shift that the Fourth Amendment was born.

5.5.3 Right to Privacy – Democracy Impact

Privacy is vital to democratic governance. NSA surveillance violates it.

Shaw 17

Jonathan Shaw ('89, managing editor of Harvard Magazine). "The Watchers." Harvard Magazine, JANUARY-FEBRUARY 2017. https://harvardmagazine.com/2017/01/the-watchers

Confidentiality: "Privacy Is about Accountability"

IN THE HERE AND NOW, using encryption, firewalls, and passwords is one way to keep information secret. But secrecy is just "a very small slice" of what privacy is about, says Marc Rotenberg of EPIC. Through "creative advocacy, litigation, and public en-gagement," the Washington, D.C.-based nonprofit aims to shape policy and advance the legal framework for safeguarding personal liberty. Rotenberg, an attorney and adjunct professor at Georgetown University Law Center, has won cases before the Supreme Court, filed numerous amicus briefs, testified before Congress, and given awards to leading privacy advocates across the political spectrum.

"Privacy is about accountability," he says. "It's about the fairness of decisionmaking. It's about holding large government actors and private companies accountable for their de-cisionmaking. It turns out to be an extraordinarily powerful and comprehensive human-rights claim, particularly in the digital age, because so much about us is based on our data."

Getting a loan or health insurance, or gaining admission to a certain school, are all data-driven determinations, Rotenberg points out. He asks how those data are being used. What personal information does an organization consider relevant? Are people pulled out of line at an airport because of their nationality, their religion, or because of a book purchased on Amazon? Given all the ways in which personal information drives de-cisions, Rotenberg says, secrecy "almost isn't even relevant to the discussion. Because paradoxically, what we keep secret is almost certainly what we don't need privacy law for. We need privacy law for everything else: for the things that we don't have the phys-ical ability to control. When you give sensitive test information to your doctor, for exam-ple, it's no longer in your control. The credit card company has all your transactional records. What are you going to do? Nothing. That's when we start to ask questions about what type of safeguards are in place to protect our personal information held by others."

"I see privacy as closely tied to the strength of democratic governance," he continues. Recalling the first time he read the NSA's foreign intelligence surveillance court order demanding that Verizon turn over all customer telephone-call records (perhaps the most significant of Snowden's revelations), Rotenberg says, "I looked at that order, 'Provide all records, because all records are relevant,' and actually thought it was satirical, a joke from The Onion, or an exercise attached to a privacy-law exam asking students to draft an unlawful court order….And then I realized it was a real order—that the
NSA thought it had the authority to collect all domestic telephone records on all U.S. telephone customers."

EPIC brought a petition to the Supreme Court arguing that the Foreign Intelligence Surveillance Court had exceeded its legal authority, and a broad coalition of legal ex-perts and former members of Congress joined the campaign. But the Court did not rule on the merits of the petition. "That was after the Solicitor General twice sought ex-tensions," Rotenberg explains, "which gave the foreign intelligence surveillance court enough time to issue an opinion justifying the program. We call that just-in-time law-making." The EPIC petition nevertheless marked the beginning of a broad bipartisan coalition to pass legislation, the USA Freedom Act of 2015, ending the NSA's bulk col-lection of such information.

Such battles almost never stay won, says Rotenberg. "The Europeans were very upset, obviously, about the U.S. surveillance activities that Snowden had documented, but then you had the terrible tragedy of Charlie Hebdo, and suddenly the French govern-ment created new surveillance authorities that go beyond what the U.S. does."

"When governments make these decisions," he reflects, "it is almost as if they're saying, 'We can't afford as much democracy, we can't afford as much openness, we can't afford to trust our citizens as much, we need to engage in more surveillance, we need less judicial review and less accountability.' " But privacy, he says, is not a trade-off: "I've been in Washington long enough to know that when someone says, 'We need to strike the right balance,' it means they probably don't know what they're talking about. A sacrifice of privacy is also a sacrifice of democracy."

In the mid 1990s, The New York Times quoted Rotenberg saying that the protection of privacy in the Information Age would be like the protection of the environment in the Industrial Age—"which is to say it's so much a part of the nature of economic pro-duction today, you don't solve it, you have to manage it." Many people predicted the end of privacy. But Rotenberg believes people don't understand the full consequences: "Among other things, you would lose your democratic state if everyone said, 'Why do

we care if the government knows everything about us? Who needs a private phone call? Who needs a building with walls? Why should data be accurate?' Everything collapses. And we know what that world looks like: that's what [Jeremy] Bentham described as the Panopticon"—designed so an observer can watch everything, but without being seen. "When you're under constant surveillance," says Rotenberg, "you're in a prison."

On the corporate front, EPIC brought the complaint that forced Snapchat, the photo-sharing service, to fulfill its promise to delete images. When Google tried to move all Gmail users onto Buzz, its social-media platform, EPIC complained to the Federal Trade Commission (FTC), and established a significant precedent for Internet privacy. When WhatsApp announced that it would share users' secure-message data with Facebook (which had recently acquired the company), EPIC intervened. Likewise, when Face-book started changing user privacy settings after consumers had set them, EPIC brought the matter to the FTC, which stopped the practice. Most recently, EPIC has been active in the discussion over how student data are collected and used.

EPIC may seem the proverbial finger in the dike, barely holding back the flood. But Rotenberg says he is "actually a bit of an optimist about all of this," citing the Supreme Court's "remarkable 9-0 opinion, written by Chief Justice Roberts, that says the search of a cell phone following an arrest requires a warrant"—a case in which EPIC's extensive brief was cited. Rotenberg calls the 2014 decision "a strong statement about privacy in the modern age. And the fact that it was a unanimous court, I think, was remarkable."

EPIC also studies diverse privacy laws to advance legal protections. A project begun in 2015 to identify states with the best privacy laws examines data security and breaches, drone surveillance, police body cameras, and student privacy, to name a few. EPIC considers Massachusetts's 2007 data-protection law one of the best in the country; Cali-fornia has crafted very good data-breach-notification regulations. Farther afield, Roten-berg admires the European Court of Justice's decision on the "right to be forgotten," which involved personal bankruptcy records that had been published in a newspaper 10 years earlier. The Spanish plaintiff asked both the newspaper and Google to remove the records. Spain's privacy agency decided not to touch the newspaper, but ordered Google to remove the record from search results—drawing "a very thoughtful line" be-tween the protected free expression of news organizations and the commercial opera-tions of data brokers, who commodify personal information.

5.5.4 Right to Privacy – Social Progress Impact

Privacy is vital to social progress.

Shaw 17

Jonathan Shaw ('89, managing editor of Harvard Magazine). "The Watchers." Harvard Magazine, JANUARY-FEBRUARY 2017. https://harvardmagazine.com/2017/01/the-watchers

DO PEOPLE BEHAVE DIFFERENTLY when they think they are being watched? When former National Security Agency contractor Edward Snowden revealed the mass surveillance of American citizens in June 2013, the question suddenly grew in importance. Can the behavior of an entire population, even in a modern democracy, be changed by awareness of surveillance? And what are the effects of other kinds of privacy invasions?

Jon Penney was nearing the end of a fellowship at Harvard Law School's Berkman Klein Center for Internet & Society in 2013, and he realized that Snowden's disclosures presented an opportunity to study their effect on Americans' online behavior. Dur-ing research at Oxford the following year, Penney documented a sudden decline in Wikipedia searches for certain terrorism-related keywords: Al Qaeda, Hezbollah, dirty bomb, chemical weapon, and jihad, for example. More than a year later, when the study ended, such searches were still declining. "Given the lack of evidence of people being prosecuted or punished" for accessing such information, Penney wrote in the Berkeley Technology Law Review (which published his research last June), he judged it unlikely that "actual fear of prosecution can fully explain the chilling effects suggested by the findings of this study." The better explanation, he wrote, is self-censorship.

Penney's work is the sort of evidence for negative social effects that scholars (and courts of law) demand. If democratic self-governance relies on an informed citizenry, Penney wrote, then "surveillance-related chilling effects," by "deterring people from exercising their rights," including "…the freedom to read, think, and communicate privately," are "corrosive to political discourse."

"The fact that you won't do things, that you will self-censor, are the worst effects of per-vasive surveillance," reiterates security expert Bruce Schneier, a fellow at the Berkman and in the cybersecurity program of the Kennedy School's Belfer Center for Govern-ment and International Affairs. "Governments, of course, know this. China bases its surveillance on this fact. It wants people to self-censor, because it knows it can't stop

everybody. The idea is that if you don't know where the line is, and the penalty for crossing it is severe, you will stay far away from it. Basic human conditioning." The ef-fectiveness of surveillance at preventing crime or terrorism can be debated, but "if your goal is to control a population," Schneier says, "mass surveillance is awesome."

That's a problem, he continues, because "privacy is necessary for human progress. A few years ago we approved gay marriage in all 50 states. That went from 'It'll never happen' to inevitable, with almost no intervening middle ground." But to get from immoral and illegal to both moral and legal, he explains, intervening steps are needed: "It's done by a few; it's a counterculture; it's mainstream in cities; young people don't care anymore; it's legal. And this is a long process that needs privacy to happen."

As a growing share of human interactions—social, political, and economic—are com-mitted to the digital realm, privacy and security as values and as rights have risen in importance. When someone says, "My life is on my phone," it's meant almost liter-ally: photos, passwords, texts, emails, music, address books, documents. It is not hard to imagine that the Declaration of Independence, redrafted for an information society, might well include "security and privacy," in addition to the familiar "life, liberty, and the pursuit of happiness," among its examples of "unalienable rights."

5.5.5 Abuse

The NSA program's potential for abuse far outweighs its national security benefits.

St.Vincent 19

Sarah St.Vincent (a researcher on U.S. national security and surveillance at Human Rights Watch). "NSA's Domestic Spying Program Needs to End—Permanently." Progressive.org, March 18, 2019. https://progressive.org/op-eds/nsa-domestic-spying-must-end-st.vincent-190318/

The U.S. National Security Agency has reportedly mothballed a large domestic spying program that the NSA and its allies in Congress fought vigorously to retain just a few years ago.

This program, first publicly revealed by former NSA contractor Edward Snowden in 2013, allows the NSA to gather records of U.S. phone calls and texts from major telecom-munications companies in secret under Section 215 of the USA Patriot Act.

Such records – which show who we called, when and for how long – can be highly revealing. They can show that we called a psychiatrist or marriage counselor, consulted with a religious adviser, helped plan a protest, or reached out to a rape hotline. They can also let the government create an elaborate picture of our relationships – not just who our friends are, but who our friends' friends are.

Congress took a step toward reining in this surveillance when it passed the USA Free-dom Act in 2015, ending the NSA's collection of U.S. phone records in bulk. However, the reformed law still allows the agency to review and collect phone records. In 2017, even under the new constraints, the NSA reported collecting a startling 534 million of these records. Thus, while this domestic surveillance is no longer as sweeping as it once was, the government has still had vast, intrusive powers under Section 215.

The reported discontinuation of this monitoring during the past six months is not neces-sarily permanent. The U.S. executive branch could still ask Congress to renew Section 215, which will otherwise expire in December.

This is a good time for us to reflect on the program's many problems. For example, despite the enormous scale and long duration of the snooping, there is no evidence that it was ever used to thwart a terrorist offense aimed at the United States.

Moreover, the Section 215 program's implementation was botched so badly that last year the NSA deleted years' worth of the records.

Routinely gathering the phone records of potentially thousands of Americans is a seri-ous and disproportionate intrusion on rights, especially given that there are alternatives.

If authorities suspect someone in the United States is involved in planning a crime, in-cluding a terrorism offense, they can easily obtain the person's phone records through a subpoena. Law enforcement officers do this routinely.

If the government believes it needs to conduct surveillance of someone in the United States for intelligence reasons, it can seek a specific order from the Foreign Intelligence Surveillance Court. Agents can do this when, for example, they suspect someone of being a spy for a foreign power or part of a terrorist organization.

The Section 215 phone records program, it seems, was from the beginning a large-scale fishing expedition. Letting government stockpile sensitive information about individ-uals, especially in secret, should raise alarm in any society. The potential for abuse is clear.

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

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

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

5.5.6 1st Amendment

NSA surveillance violates 1st Amendment rights to expression and association.

York 14

Jillian York (Director for International Freedom of Expression at the Electronic Frontier Foundation). "THE HARMS OF SURVEILLANCE TO PRIVACY, EXPRESSION AND ASSOCIATION." *Global Information Society Watch*, 2014.

The opposition to surveillance, however, is not borne only out of a desire for privacy. In the United States, the First Amendment – that which prohibits the creation of law "re-specting an establishment of religion, or prohibiting the free exercise thereof; or abridg-ing the freedom of speech, or of the press; or the right of the people peaceably to assem-ble, and to petition the Government for a redress of grievances" 5 – is often debated, but rarely restricted. It is a set of rights that is paramount in US culture; as Supreme Court Justice Hugo L. Black once stated:

First in the catalogue of human liberties essential to the life and growth of a government of, for, and by the people are those liberties written into the First Amendment of our Constitution. They are the pillars upon which popular government rests and without which a government of free men cannot survive. 6

Article 19 of the Universal Declaration of Human Rights similarly provides for the right to freedom of opinion and expression, to "seek, receive and impart information and ideas through any media and regardless of frontiers." 7

Documents leaked by Edward Snowden in 2013 have demonstrated the extraordinary breadth of the US's and other governments' mass surveillance programmes, pro-grammes which constitute an intrusion into the private lives of individuals all over the world.

The violation of privacy is apparent: indiscriminate, mass surveillance goes against the basic, fundamental right to privacy that our predecessors fought for. The negative ef-fects of surveillance on the fundamental freedoms of expression and association may be less evident in an era of ubiquitous digital connection, but are no less important.

In a 2013 report, Frank La Rue, Special Rapporteur to the United Nations on the pro-motion and protection of the right to freedom of opinion and expression, discussed the ways in which mass surveillance can harm expression. He wrote:

Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization. 8

The harmful effects of surveillance on expression and association are undeniably linked – the right to organise is imperative for political expression and the advancement of ideas. In the US, although the two rights are linked in the First Amendment, historically, they have sometimes been treated separately.

In a landmark 1958 case, NAACP v. Alabama, the Supreme Court of the US held that if the state forced the National Association for the Advancement of Colored People (NAACP) to hand over its membership lists, its members' rights to assemble and or-ganise would be violated.9 This case set the precedent for the Supreme Court's foray into the constitutionally guaranteed right to association after decades of government attempts to shun "disloyal" individuals.

Justice John Marshall Harlan wrote for a unanimous court:

This Court has recognized the vital relationship between freedom to associate and pri-vacy in one's associations. Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs. 10

Today, the data collected by the NSA's various surveillance programmes poses a similar threat to the collection of membership lists. The vast majority of what the NSA collects is metadata, an ambiguous term that in this case describes the data surrounding one's communications. That is to say, if the content of one's phone call is the data, the meta-data could include the number called, the time of the call, and the location from which the call was made.

The danger in metadata is that it allows the surveiller to map our networks and activities, making us think twice before communicating with a certain group or individual. In a surveillance state, this can have profound implications: Think of Uganda, for example, where a legal crackdown on lesbian, gay, bisexual and transgender (LGBT) activists is currently underway. Under surveillance, a gay youth seeking community or health care faces significant risks just for the simple act of making a phone call or sending an email.

In many countries, there has long been a legal distinction between the content of a mes-sage (that is, the message itself), and the "communications data", or metadata. This

distinction is based on the traditional model of postal mail, where information written on the outside of an envelope is distinguished from the content of the envelope. This distinction is, however, rendered nearly meaningless by modern surveillance methods, which can capture far more than the destination of a communication, and en masse.11

In order to argue effectively for and reclaim the right to associate freely without surveil-lance, it is imperative that such a distinction be made. Digital metadata is different from analogue metadata and its wide-scale capture creates a chilling effect on speech and as-sociation. It is time for fresh thinking on the impact of the culture of surveillance on our daily habits.

5.5.7 AT: Squo Reforms Solve

Current debates are not over halting illegal NSA surveillance, but rather how to extend it – that's not enough.

Reed 20

Kevin Reed (World Socialist Web Site). "US Senate reauthorizes domestic surveil-lance, allows access to internet histories." *World Socialist Web Site*, May 16, 2020. https://www.wsws.org/en/articles/2020/05/16/surv-m16.html

The US Senate voted on Thursday to approve the USA Freedom Reauthorization Act of 2020. The law authorizes government surveillance of the public, including federal law enforcement agency access to the internet browsing and search histories of American citizens.

Voting 80 to 16, the Senate approved a two-and-a-half-year extension of the Foreign Intelligence Surveillance Act (FISA) provisions that have been the basis of expanding abuses by US intelligence, which originated in the aftermath of the terror attacks of September 11, 2001 and were authorized in the USA PATRIOT Act.

According to congressional procedures, although the House of Representatives already approved a similar bill last March, the modified version adopted by the Senate must now go back to the House for final approval before it can be sent to the White House to be signed into law by President Trump.

The Senate reauthorization of the FISA provisions was supported by both Democrats and Republicans and easily surpassed the sixty-vote threshold necessary for passage.

Under the FISA rules, law enforcement is supposed to obtain approval from a special FISA court—an individual judge who reviews FBI and CIA requests in secret—before engaging in eavesdropping and surveillance operations on US citizens.

Significantly, the Senate vote restored FISA elements that have become known as the "business records," "lone wolf" and "roving wiretap" provisions in counterterrorism or espionage investigations, which were the subject of debate in recent months. All three of these rules had expired last December. They involve details about what law enforce-ment officers are permitted to do once the FISA court authorizes the secret surveillance of an individual.

As has been the case throughout the history of the PATRIOT Act as well as the revised USA Freedom Act (2015) adopted during the Obama era, the official political debate in

the lead-up to the Senate vote on Thursday was never about halting the illegal govern-ment surveillance of the US public that has been going on for two decades, but rather how to extend it.

This fact was proven in the first of three amendments to the law that were discussed during the Senate deliberations. When Republican Senator Rand Paul from Kentucky proposed to block the use of FISA courts on US citizens because "you don't get a lawyer," his amendment was quickly rejected by 11–85.

A second amendment proposed by Republican Senator Mike Lee of Utah and Demo-cratic Senator Patrick J. Leahy of Vermont was adopted with the support of 77 senators. The Lee-Leahy amendment lowers the threshold for the FISA court to appoint an "ami-cus curiae" advisor in cases that involve a "sensitive investigative matter."

Prompted by numerous abuses of FISA procedures uncovered during the 18 month-long "Russia probe" in 2018–2019, the proposal enables the court to appoint an advisor who, according to Lee, "can raise any issue with the court at any time and give both the amicus and the FISA court access to all documents and information related to the surveillance application."

According to publicly available FISA data, such amici have been used only 16 times among the thousands of surveillance applications that have been approved in the past five years. However, even this minuscule adjustment by the Senate was criticized by the US Justice Department, with national security spokesman Marc Raimondi stating, "We appreciate the Senate's reauthorization of three expired national security authorities. As amended, however [the bill] would unacceptably degrade our ability to conduct surveillance of terrorists, spies and other national security threats."

In a very significant vote, the Senate rejected a third amendment to the reauthorization bill that would have prevented federal law enforcement agencies from obtaining the internet browsing and search histories of American citizens without a warrant.

The vote on the amendment—drafted by Democratic Senator Ron Wyden of Oregon and Republican Senator Steve Daines of Montana—was 59–37, one vote shy of the 60 needed for adoption. The provision allowing the FBI and CIA access to internet brows-ing activity histories without court approval is contained in Section 215 of the act.

In discussing the implications of the warrantless data gathering on the Senate floor, Wyden warned, "Collecting this information is as close to reading minds as surveillance can get. It is digital mining of the personal lives of the American people … without this bipartisan amendment, it is open season on anybody's most personal information."

Wyden went on, "Under Section 215, the government can collect just about anything so long as it is relevant to an investigation. This can include the private records of innocent, law-abiding Americans. They don't have to have done anything wrong. They don't have to be suspected of anything. They don't even have to have been in contact with anyone suspected of anything."

Wyden also pointed out that tens of millions of Americans are now stuck at home during the pandemic and using the internet more than ever as their only connection to the outside world.

The corporate media was quick to point out that the amendment failed in part because four Senators did not cast a vote at all, including former Democratic presidential can-didate and senator from Vermont Bernie Sanders, Republican Senator from Tennessee Lamar Alexander, Democratic Senator from Washington Patty Murray and Republican Senator from Nebraska Ben Sasse.

Concerns in the Senate were so high that the Wyden-Daines amendment might pass that Republican Majority Leader Mitch McConnell was reportedly working on his own measure to officially write into the law a provision that the government may collect records of internet search and browsing histories without a warrant.

According to Recode, "that amendment never came to the floor, likely because Mc-Connell knew the Wyden-Daines amendment wouldn't get enough votes."

Privacy and civil rights groups have pointed to the dangers posed by the Senate reautho-rization of the FISA domestic surveillance measures. However, they focused almost ex-clusively on the use of these tools in the hands of the Trump administration. Sean Vitka, senior policy counsel at Demand Progress, which led a coalition of 36 organizations in-cluding the American Civil Liberties Union (ACLU) and Freedom Works supporting privacy amendments to the legislation, said on Thursday, "[T]he loss of the warrant protection for browser history due to absences during the vote by supportive senators was a huge disappointment."

Vitka went on, "These protections are particularly critical given the Trump administra-tion's history of abusing marginalized communities and others the president regards as enemies. Without more protections that would limit the information spy agencies can collect without a warrant, Congress will be giving the Trump administration the power to snoop on billions of data points for every single person in the United States."

5.6 Social Control

5.6.1 Anti-Capitalism

NSA surveillance is used to bolster state power in preparation for a major confrontation with the working class. Surveillance is targeted towards individuals who oppose the government and the capitalist system as a whole.

Reed 20

Kevin Reed (World Socialist Web Site). "US Senate reauthorizes domestic surveil-lance, allows access to internet histories." *World Socialist Web Site*, May 16, 2020. https://www.wsws.org/en/articles/2020/05/16/surv-m16.html

Snowden exposed a secret NSA program called XKeyscore that allowed intelligence an-alysts to search without authorization through databases containing the email messages, online chats and browsing histories of everyone. In the training materials leaked by the whistleblower, the NSA boasted that XKeyscore was the "widest-reaching" intelligence gathering system, which collects "nearly everything a typical user does on the internet" in real time.

In describing the NSA system to the Guardian in 2013, Snowden explained its purpose: "Because even if you're not doing anything wrong, you're being watched and recorded… You simply have to eventually fall under suspicion from somebody—even by a wrong call. And then they can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."

Under conditions of an increase in strikes and class conflict arising from the pandemic and the deepening economic crisis, the state is bolstering its internet browser data gath-ering measures as part of the preparations for a major confrontation with the working class.

End-to-end encryption tools built into the mobile devices and apps are being used by tens of millions of people, blocking law enforcement's ability to monitor the content of individual communications. This means that the gathering of browsing data becomes one of the main electronic surveillance windows into the private and political activity of individuals and organizations that will be targeted for their opposition to the govern-ment and the capitalist system as a whole.

5.6.2 Chilling Effect

NSA surveillance has a chilling effect on discourse and behavior.

York 14

Jillian York (Director for International Freedom of Expression at the Electronic Frontier Foundation). "THE HARMS OF SURVEILLANCE TO PRIVACY, EXPRESSION AND ASSOCIATION." *Global Information Society Watch*, 2014.

On 5 June 2013, the Washington Post and the Guardian simultaneously published doc-uments that would rock the world. The documents, leaked by ex-National Security Agency (NSA) contractor Edward Snowden, were not the first disclosures about the United States' vast surveillance complex, but have arguably had the most impact.

Before last year, awareness of digital surveillance in the US – and indeed, in much of the world – was minimal. Disclosures made by WikiLeaks in 2011 can be credited for an uptick in reporting on surveillance 1 – particularly in the Middle East – but did little to inspire research on the societal impact of it.

The knowledge, or even the perception, of being surveilled can have a chilling effect. A 2012 industry study conducted by the World Economic Forum found that in high internet penetration countries, a majority of respondents (50.2%) believe that "the gov-ernment monitors what people do on the Internet." At the same time, only 50% believe that the internet is a safe place for expressing their opinions, while 60.7% agreed that "people who go online put their privacy at risk." 2

A member survey conducted by writers' organisation PEN American Center in Decem-ber 2013 discovered that, since the publication of the first NSA leaks, 28% of respon-dents have "curtailed or avoided social media activities," while another 24% have "de-liberately avoided certain topics in phone or email conversations." Perhaps even more worryingly, a full 16% have avoided writing or speaking on certain topics.3

Surveillance affects us in myriad ways. It infringes on our personal freedoms, submits us to state control, and prevents us from progressing as a society.

5.6.3 Surveillance Capitalism

Surveillance has morphed into surveillance capitalism, which uses technology as an instrument to maintain and transform a capitalist social order. Affirming privacy as a human right is vital to bind capitalism to pro-social and pro-democratic principles.

Shaw 17

Jonathan Shaw ('89, managing editor of Harvard Magazine). "The Watchers." Harvard Magazine, January-February 2017. https://harvardmagazine.com/2017/01/the-watchers

*Note: Zuboff (the "she" quoted) = American author, Harvard professor, social psychol-ogist, philosopher, and scholar

"I think it's very important to connect the dots," she explains, "and see that all of this makes sense when we frame it as a new form of capitalism that has particular require-ments in order to be successful. Technology is never a thing in itself. It is always designed and deployed to reflect the aims and needs of a particular economic order. Suddenly, we can see that these ventures are part of a cohesive, internally consistent, and coherent economic logic. And when we can do that, then I think as a society we are far better positioned to increase and expand our advocacy and reform efforts, [to figure out how] to successfully tether information-based capitalism to pro-social and pro-democratic values and principles," rather than solely serving third-party economic interests. "The challenge of surveillance capitalism becomes part of the larger historical project of harnessing capitalism to society."

Surveillance capitalism, driven by the profit motive, "has been able to gather to itself concentrations of knowledge and power that exceed anything imaginable even a few years ago," she says. "One of its consequences is the deletion of privacy. But if we fight this only on the grounds of privacy, we're bound to meet with constant frustration and limited success. This is an economic logic that must delete privacy in order to be suc-cessful." This is why, despite the "brilliant and heroic scholarship" that has come out of Berkman, and despite the "brilliant and heroic advocacy that has come from many quar-ters in the United States, including Marc Rotenberg and his amazing team at EPIC,…this thing keeps growing."

History may suggest better ways to respond, she says. "We have experience in tam-ing capitalism, and binding it to pro-social and pro-democratic principles. In the late nineteenth century, the Gilded Age, there was no protection for labor, and capital had complete freedom to do whatever it wanted to do with resources, with people, with

communities, producing extreme economic and social inequality along the way." The twentieth century "was a long journey to correct that imbalance." The social challenge now, she says, is to insist on a new social contract, with its own twenty-first century leg-islative and regulatory innovations, that harnesses information capitalism to democratic values and norms. This begins, she believes, with deepening social understanding and awareness. "We have to create the political context in which privacy can be successfully defended, protected, and affirmed as a human right. Then we'd have a context in which the privacy battles can be won."

6 Con Evidence

6.1 NSA Action Fails

6.1.1 Congress Key

Only Congressional action ensures adequate safeguards.

Guliani 19

Neema Singh Guliani (Former Senior Legislative Counsel, American Civil Liberties Union). "Ending the NSA's Massive Phone Spying Program Would Be a Good Start — But There's a Lot More to Do." American Civil Liberties Union, March 5, 2019.

https://www.aclu.org/blog/national-security/privacy-and-surveillance/ending-nsas-massive-phone-spying-program-would-be

Even aside from the call detail records program, the government collects a staggering amount of information under Section 215. Under it, the government claims the author-ity to collect any "tangible" thing, covering everything from financial records to library records. Despite the 2015 reforms, this collection does not appear to be targeted and narrow. For example, in 2017, investigations of 74 targets resulted in the disproportion-ate collection of information regarding 87,000 unique phone numbers, email addresses, or other account identifiers.

Unlike surveillance prior to the Patriot Act, under Section 215, the government can tar-get individuals who are not members of terrorist organizations, affiliated with foreign nations, or suspected of any criminal wrongdoing at all. The government merely has to show that the information it seeks is "relevant" to an ongoing terrorism or intelligence investigation. This extremely low bar leaves ample room for government abuse, evi-denced by the fact that for over a decade the government interpreted this standard as permitting the collection of records of nearly everyone in the U.S.

Given this history, Congress should allow Section 215 to expire at the end of this year

unless the law can be substantially reformed to prevent rights intrusions. In addition to Section 215, however, Congress must also revisit other surveillance authorities that the government still abuses.

According to transparency reports, the government continues to collect information about tens of thousands of unique accounts under other Patriot Act authorities that were changed in 2015. Congress must pass additional reforms to halt this large-scale surveillance and put in place safeguards to prevent these powers from being used as a tool to target minorities, suppress journalists and critics, or circumvent existing criminal laws.

For example, Congress must adopt procedures that prevent the government from en-gaging in practices that wrongly target or impact people based on race, religion, na-tional origin, or other protected classes. This is particularly important given the ample evidence of bias in intelligence analyses and practices. For example, recently leaked FBI intelligence assessment suggests that the agency wrongly labels black activists as "extremists," and media disclosures revealed that the government used FISA to spy on prominent Muslim-Americans who were never charged with committing a crime.

Congress must also strengthen existing First Amendment protections. Section 215 and other Patriot Act authorities prohibit surveillance based "solely" on First Amendment-protected activities. Yet partially redacted intelligence court opinions suggest that these safeguards are being interpreted far too narrowly. The 2015 reforms also did not ad-dress concerns that large-scale surveillance would likely sweep in the information of individuals, like journalists, engaged in First Amendment-protected activities.

6.1.2 EO 12333

EO 1233 gets reissued by every new administration and is used for NSA surveillance – that loophole means the Biden administration will just reinstate the program.

Eddington 19

Patrick Eddington (Policy Analyst in Homeland Security and Civil Liberties at the Cato Institute). "The Snowden Effect, Six Years On." *Just Security*, June 6, 2019. https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

As it stands, the USA Freedom Act is set to expire on December 15 of this year. So, why not just let it die and move on? Because even if the USA Freedom Act expires, other vast—and in my view, unconstitutional—domestic surveillance powers and technolo-gies will remain untouched and, in at least one case, completely unexamined publicly.

Executive Order 12333

Executive Order 12333, issued by President Ronald Reagan in 1981 and reissued by ev-ery administration since, is the governing federal regulation for overseas intelligence collection for the NSA and each of the other 16 agencies that comprise the U.S. Intelli-gence Community (IC). Until the establishment of the PCLOB in 2004, no element of the federal government had ever conducted a comprehensive examination of IC activities carried out under EO 12333.

But now, the PCLOB has conducted an investigation of the IC activities carried out un-der EO 12333, which is good news. However, the bad news is that the PCLOB is refusing to release the results of their investigation.

In a May 21 response to my Freedom of Information Act (FOIA) request, the PCLOB said that it had "determined that it is appropriate to withhold in full the Board's completed Executive Order 12333 deep dive report pursuant to Exemption 1 of the FOIA, 5 U.S.C. § 552(b)(1). Exemption 1 protects from disclosure information that has been deemed classified 'under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy.' " (I am appealing the denial of my FOIA request.)

This lack of transparency is at odds with the PCLOB's approach to its own NSA tele-phone metadata program report as well as its report on the controversial (and in my view, unconstitutional) Foreign Intelligence Surveillance Amendment Act (FAA) Sec-tion 702 program.

Interestingly, the PCLOB has agreed in principle to provide me correspondence in any form to or from the Board regarding alleged or actual violations of laws, regulations, or executive orders by any federal department or agency under the purview of the Board. Whether such violations involve activities carried out under EO 12333 is just one reason why the PCLOB report should be released. One thing we do know: NSA employees have in the very recent past violated EO 12333 to spy on innocent people.

Thanks to Sen. Chuck Grassley (R-Iowa), we know that between 2003 and 2013, NSA employees violated EO 12333, as well as federal statutes, by using NSA collection sys-tems to spy on their current or former romantic partners, as well as other individuals— foreign nationals and American citizens.

According to a September 2013 NSA Inspector General letter to Grassley, two military members who committed violations were fined, reduced in rank, or received other ad-ministrative punishments under the Uniform Code of Military Justice. Most of the civil-ian employees implicated in other episodes were allowed to resign, including cases where criminal referrals were made to the Justice Department. To date, Grassley's reve-lations about NSA employee abuses of power and technology granted them remain the only substantive, published insights available to the public on abuses committed under EO 12333.

6.1.3 EO 1233 – AT: Not Domestic

It's not limited to non-Americans – EO 1233 includes over 9 million US citizens abroad.

Eddington 19

Patrick Eddington (Policy Analyst in Homeland Security and Civil Liberties at the Cato Institute). "The Snowden Effect, Six Years On." *Just Security*, June 6, 2019. https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

EO 12333 covers overseas intelligence collection, but what's often overlooked is that it's not limited to non-Americans. In 2016, the State Department's Bureau of Consular Affairs estimated that some 9 million Americans live overseas. Those expatriate Amer-icans communicate with family, friends, business associates, and government agencies on a daily basis. In light of what Grassley uncovered and what Snowden exposed, it's absolutely fair to ask—and imperative to determine publicly—the scope of potential compromises of the communications of American citizens by NSA or any other federal department or agency under EO 12333.

Disturbingly, the PCLOB is also withholding in full "responsive documents regarding refusal by a federal department or agency to provide information requested by the PCLOB pursuant to its oversight mission…" (I am appealing this denial as well.)

The PCLOB's credibility as an oversight body rests in large part on its ability to get documents from NSA, FBI, CIA and any other IC element regarding activities that might infringe on the constitutional rights of Americans. If it is encountering resistance to its oversight efforts, the public should know who the culprits are and Congress should bring the offenders to heel by any available means.

To date, House Intelligence Committee Chairman Rep. Adam Schiff (D-Calif.), and his GOP counterpart Rep. Devin Nunes (R-Calif.) have shown far more interest in either at-tacking or defending Trump over the "Russiagate" affair than conducting serious over-sight of the IC agencies. And while their Senate Intelligence Committee counterparts have feuded less publicly over Russian interference in the 2016 elections, they remain just as obsessed—and thus distracted—by the issue, at the expense of ongoing federal domestic surveillance excesses.

The USA Freedom Act expiration deadline is an opportunity to holistically address the wide range of these abuses, as well emerging technologies that further threaten the con-

stitutional rights and privacy of all of us. Whether Congress has the will to do so is an open question.

6.1.4 Voluntary Actions Fail

Voluntary NSA halts fail – the NSA argues it retains authority to restart surveillance programs it ends.

Guliani 19

Neema Singh Guliani (Former Senior Legislative Counsel, American Civil Liberties Union). "Ending the NSA's Massive Phone Spying Program Would Be a Good Start — But There's a Lot More to Do." American Civil Liberties Union, March 5, 2019.

https://www.aclu.org/blog/national-security/privacy-and-surveillance/ending-nsas-massive-phone-spying-program-would-be

Now, news reports suggest that the NSA may have voluntarily halted the program. The NSA has yet to confirm why, and it may have simply replicated this collection under a different authority.

Even if these reports are true, however, Congress must still act to prevent this program from ever being resurrected. In the past, the NSA has argued that it retains the authority to restart surveillance programs it voluntarily ends. The agency will likely take the same position here. That's why Congress must completely eliminate this power to prevent this program from ever being resurrected under Section 215 or any other authority.

But this alone is not enough.

6.1.5 Other Agencies

Other agencies like the FBI will abuse data.

Guliani 19

Neema Singh Guliani (Former Senior Legislative Counsel, American Civil Liberties Union). "Ending the NSA's Massive Phone Spying Program Would Be a Good Start — But There's a Lot More to Do." American Civil Liberties Union, March 5, 2019.

https://www.aclu.org/blog/national-security/privacy-and-surveillance/ending-nsas-massive-phone-spying-program-would-be

The lack of these protections is compounded by the fact that there are not enough limits on how federal agencies can access and use information that's collected. The FBI and other agencies should be prohibited from searching and using this information for pur-poses unrelated to why it was collected, circumventing existing protections that exist in the criminal context. They must also meet their constitutional obligation to provide no-tice to individuals when this information is used in criminal proceedings — something that they have denied they have the responsibility to do when using information from Section 215 and other authorities.

There are other significant issues that Congress must also address, including closing Section 702's backdoor search loophole, which is exploited to warrantlessly spy on indi-viduals in the U.S. Congress also needs to reform the secret Foreign Intelligence Surveil-lance Court, in part by requiring more declassification of its opinions, ensuring trans-parency.

Even if the NSA call records program has ended, that is not enough to protect our rights. Congress must end the call-detail-record authority altogether. In addition, it must take steps to put an end to other abuses under Section 215 and similar surveillance authori-ties.

6.2 Outsourcing

6.2.1 Five Eyes

Surveillance gets outsourced to allies in the Five Eyes program. That's worse – there are no legal checks.

Pangburn 18

DJ Pangburn (WRITER AND EDITOR WITH BYLINES AT VICE). "How Coun-tries"Outsource" Electronic Surveillance And Threaten Privacy." Vice, May 2, 2018.
https://www.fastcompany.com/40566948/how-countries-outsource-electronic-surveillance-and-threaten-privacy

One might assume that countries like the United States and United Kingdom simply col-lect data on citizens through their own mass surveillance systems. Many governments around the world, however, work in concert to maintain intelligence sharing partner-ships that allow them to pool their mined electronic communications. In a new report ti-tled "Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards," Privacy International describes these partnerships as the outsourcing of surveillance. In "allowing governments to bypass domestic constraints on their surveillance activities," the watchdog group says that the partnerships can "con-tribute to, or facilitate, serious human rights abuses, such as unlawful arrest or deten-tion, or torture and other cruel, inhuman or degrading treatment."

Depending on the countries' specific intelligence sharing arrangements, most anything can be shared, says Edin Omanovic, Privacy International's State Surveillance Pro-gramme Lead. The system's trove includes information like raw internet and phone data, intelligence reports about individuals, watchlists, information about intelligence gathering techniques, information about encryption and decryption techniques, and more.

"Basically anything you would imagine an intelligence agency collecting," Omanovic explains. "But obviously some arrangements are closer than others, so, for example, the U.S. has a closer intelligence-sharing relationship with the U.K. and other countries in the Five Eyes than other countries."

The report, gleaned from research with 40 partners reaching out to oversight bodies in 42 countries, lays out the appearance and depth of these intelligence sharing partnerships.

It also dives into the partnerships' legality and existing oversight, which is quite weak. In all, only 21 oversight organizations sent Privacy International information on these intelligence sharing arrangements from their respective governments.

Omanovic says that few people actually think of this intelligence sharing network. This, he says, is because it was designed to be a secretive system. Many countries exhibit varying levels of trust between one another, which influences their level of cooperation.

6.2.2 Backdoors

The US will shift to forcing backdoors – Australia proves.

Shackford 19

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

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

Should the White House accept the NSA's recommendation here and let the USA Free-dom Act expire, that makes it all the more important that we pay attention to govern-ments' efforts across the world to force social media platforms and app makers to in-troduce backdoors to encryption or some other form of structural weakness that would allow government spies to access our private communications without our knowledge.

This fight is heating up now that Australia has passed expansive, intrusive legislation that essentially forces people who work at or run private communication platforms or apps to assist Australian officials in secretly bypassing encryption. Australia has an intelligence-sharing agreement with the United States, so anything it gathers could be passed along to the feds. Microsoft has warned that it may stop storing data in Australia entirely to keep officials there from forcing the company's employees to give them access to private data.

One avenue of secret, unwarranted surveillance appears to be closing. But the struggle to protect our privacy from government snoops is far from over.

6.2.3 XKeyscore

XKeyscore ensures that surveillance continues in the absence of NSA programs.

** Omanovic = Edin Omanovic, Privacy International's State Surveillance Programme Lead

Pangburn 18

DJ Pangburn (WRITER AND EDITOR WITH BYLINES AT VICE). "How Coun-tries"Outsource" Electronic Surveillance And Threaten Privacy." Vice, May 2, 2018.
https://www.fastcompany.com/40566948/how-countries-outsource-electronic-surveillance-and-threaten-privacy

"Certainly when it started post-Second World War, [NATO allies] foresaw that they would be able to share collection capabilities from satellite interception," says Omanovic. 'And because those agreements were there, it's just kind of mutated into mass-scale internet surveillance in a way they would have never foreseen."

The very nature of how the internet works has, according to Omanovic, helped this intelligence-sharing system expand and thrive. Since the internet is global, flowing through various nodes in many countries, the governments involved in intelligence sharing can easily pick up internet traffic from various points.

A great deal of internet traffic, for instance, flows through data centers in the Five Eyes partnership—the U.S., U.K., Australia, New Zealand, and Canada. These countries col-lect and distribute a massive amount of internet traffic. Elsewhere, the Club de Berne is an intelligence-sharing arrangement amongst EU members states, while The Shang-hai Cooperation Organization—a security, economic, and political cooperation forum— facilitates intelligence sharing between China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan.

One of the most disturbing aspects of intelligence sharing systems, says Omanovic, is that "they're completely shrouded in secrecy, making it impossible to know how much data is being shared."

"I think the Edward Snowden revelations highlighted how advanced these relationships, not just from exchanging information but actually providing one another with raw in-telligence as it's being collected," says Omanovic. "Even though the term is intelligence sharing, it goes far beyond that. It's basically acting as a unitary intelligence collection system. Basically, you couldn't even tell who was collecting the intelligence."

The intelligence taken in by the Five Eyes, for example, is fed into a central query system known as XKeyscore, a program unveiled through Snowden's revelations. XKeyscore essentially allows agents to run searches for various vectors of interest. Omanovic de-scribes this data, and other information generated by different partnerships, as not being of really any intelligence value. It's simply everything that can be hoovered up through various domestic surveillance programs: raw traffic of general internet packets.

6.2.4 Legal Checks

There's no legislation on the books to prevent it – means voluntary NSA action will be insufficient.

** Omanovic = Edin Omanovic, Privacy International's State Surveillance Programme Lead

Pangburn 18

DJ Pangburn (Writer and Editor with bylines at Vice). "How Countries"Outsource" Electronic Surveillance And Threaten Privacy." Vice, May 2, 2018. https://www.fastcompany.com/40566948 countries-outsource-electronic-surveillance-and-threaten-privacy

While identifying and thwarting cybersecurity threats is a legitimate state interest, Pri-vacy International and its partners believe governments shouldn't lose sight of privacy. Again, for them, it's a human right—one that requires vigilance in safeguarding.

"[This system] is one of the most fundamental threats to privacy at the moment, and it needs to be governed and overseen correctly," says Omanovic. "We found only one country [Canada] which has introduced specific legislation to explicitly regulate intelli-gence sharing—the rest lack domestic legislation which regulates intelligence sharing. This means that such practices are extremely under-regulated and open to abuse: it is essential that stronger oversight measures are urgently implemented."

6.3 Covid-19

6.3.1 Tracking Infections

Mass government surveillance is being used to assess infection rates, dangerous crowding, and compliance with stay-at-home orders.

Biddle 20

Sam Biddle (reporter focusing on malfeasance and misused power in technology). "Privacy Experts Say Responsible Coronavirus Surveillance Is Possible." *The Intercept*, April 2, 2020. https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/

IN LESS than a decade, whistleblowers like the NSA's Edward Snowden and Cam-bridge Analytica's Christopher Wylie helped spur a global sea change in the public's attitude toward privacy and global data dragnets. We may now be in the midst of an-other seismic moment in the history of digital privacy: Mass surveillance methods could save lives around the world, permitting authorities to track and curb the spread of the novel coronavirus with speed and accuracy not possible during prior pandemics.

It's an extraordinary moment that might call for extraordinary surveillance methods. But privacy advocates tell The Intercept that our ongoing public health crisis doesn't have to mean creating a civil liberties crisis in turn.

The coronavirus tracking ramp-up is already well underway around the world. In South Korea, Taiwan, and Israel, authorities use smartphone location data to enforce individ-ual quarantines. Moscow police say they've already busted 200 quarantine violators caught via facial recognition-enabled cameras. NSA contractor and perennial privacy offender Palantir is helping Britain's National Health Service track infections. Apps that leverage a smartphone's bounty of built-in, highly accurate sensors to enforce social dis-tancing or map the movements of the infected have been deployed in Singapore, Poland, and Kenya; MIT researchers are now pitching a similar, but more "privacy friendly," app. In Mexico, Uber sent government authorities rider data to trace the route of an infected tourist, also banning 240 users who'd taken rides with the same driver.

In the U.S., public health officials, hoping to assess broad compliance with stay-at-home orders and to spot dangerous crowding, are obtaining personal location data in bulk from loosely-regulated online advertisers, and have discussed obtaining it from Google,

according to news reports. A maker of "smart" thermometers, Kinsa Health, set up a special website to provide access to geographical fever clusters and other data uploaded from the hundreds of thousands of homes that use its app-enabled devices, earning Kinsa some buzz, including a recent New York Times article in which public health experts praised the predictive power of its user data.

These surveillance methods have been enabled by the rise of the smartphone and cloud computing — and of an entire tracking ecosystem around them. Over the past decade or so, the kindred spirits of the advertising industry and intelligence community have worked tirelessly and on parallel tracks to perfect their exploitation of the unimaginably vast trails of personal data collected through various mobile apps. The ability to learn your location and predict your behavior is priceless to both Silicon Valley and the Pen-tagon, whether the ultimate goal is to target you with a Warby Parker ad or a Hellfire missile.

As the Covid-19 pandemic worsens and death tolls increase, it stands to reason that the notion of reappropriating these technologies of war and profit into the preservation of human life will only make mass surveillance more palatable to a frightened public, particularly one desensitized by a decade of smartphone ubiquity and data-siphoning apps.

6.3.2 AT: Privacy Spillovers

Allowing health officials to drive data decisions checks broader civil rights overreach.

Biddle 20

Sam Biddle (reporter focusing on malfeasance and misused power in technology). "PRIVACY EXPERTS SAY RESPONSIBLE CORONAVIRUS SURVEILLANCE IS POSSIBLE." *The Intercept*, April 2, 2020. https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/

Health Officials Must Drive Data Decisions

"Whatever decisions or policies are implemented with respect to responding to this catastrophe have to be those that are demanded by public health officials and experts" as opposed to others in government, particularly "people in the security or law enforce-ment business," said Mohammad Tajsar, an attorney with the American Civil Liberties Union of Southern California.

This, said Tajsar, will help ensure that governments only collect information that is ac-tually useful rather than making a mad grab for anything that might potentially help. "Governments tend to have a pretty voracious appetite when it comes to data without really understanding the limitations of [the] information, and how and what the use cases are for responding to crises like this one," he said.

Allowing data collected for Covid-19 purposes to expire solves.

Biddle 20

Sam Biddle (reporter focusing on malfeasance and misused power in technology). "PRIVACY EXPERTS SAY RESPONSIBLE CORONAVIRUS SURVEILLANCE IS POSSIBLE." *The Intercept*, April 2, 2020. https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/

Data Collected for Covid-19 Purposes Should Expire

"Any program must be strictly time-limited," said Faiza Patel, director of the Brennan Center for Justice's Liberty and National Security Program at NYU Law. "Our physical safety is paramount, but at some point we will emerge on the other side of this crisis." When that happens, she added, lawmakers and citizens should be vigilant to ensure that

there has been no compromise of constitutional civil liberties and that data collected for Covid-19 is not retained.

6.4 National Security

6.4.1 Metadata

NSA metadata collection serves vital future national security interests.

Wiegmann, Orlando, and Morgan 19

Bradford Wiegmann, Michael J. Orlando, and Susan Morgan (Deputy Assistant Attorney General, DOJ, Deputy Assistant Director, FBI, and National Security Agency official, respectively). "BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE AT A HEARING ENTITLED 'REAUTHORIZING THE USA FREEDOM ACT OF 2015'." *Committee on the Judiciary, United States Senate*, November 6, 2019. https://www.judiciary.senate.gov/imo/media/doc/Wiegmann-Orlando-Morgan%20Testimony.pdf

The fourth authority—the Call Detail Records ("CDR") provision—permits the targeted collection of telephony metadata but not the content of any communications. Congress added this authority to FISA four years ago in the FREEDOM Act as one of several sig-nificant FISA reforms designed to enhance privacy and civil liberties. It replaced the National Security Agency's ("NSA") bulk telephony metadata collection program with a new legal authority whereby the bulk metadata would remain with the telecommu-nications service providers. The CDR authority provides a "narrowly-tailored mecha-nism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized inves-tigation to protect against international terrorism." H. Rep. 114-109, at 17 (2015). The FREEDOM Act also permanently banned bulk collection under FISA's business records and pen-trap provisions and under the National Security Letter statutes. As this Com-mittee is aware, the NSA recently discontinued the CDR program for technical and op-erational reasons. But the CDR program retains the potential to be a source of valuable foreign intelligence information. The CDR program may be needed again in the future, should circumstances change. NSA's careful approach to the program, and the legal obligations imposed by the FREEDOM Act in the form of judicial oversight, legislative oversight, and transparency, support the reauthorization of the CDR program.

We urge the Committee to consider permanently reauthorizing these authorities based not only on the Government's demonstrated record and the importance of the authori-ties to national security, but also on the significant reforms contained in the FREEDOM

Act. These include authorizing the FISC to appoint amici curiae to address privacy and civil liberties concerns and enhancing public transparency and reporting requirements under FISA. Four years ago, the FREEDOM Act was passed after extensive oversight and comprehensive hearings, and received strong bipartisan support in the Senate. In the wake of repeated reviews and bipartisan authorizations over nearly two decades, the Administration's view is that the time has come for Congress to extend these au-thorities permanently.

6.4.2 Metadata – AT: NSA Scrapped It

The program was scrapped due to modern technical constraints, not a lack of usefulness. Maintaining flexibility is key to a dynamic national security policy.

Wiegmann, Orlando, and Morgan 19

Bradford Wiegmann, Michael J. Orlando, and Susan Morgan (Deputy Assistant Attorney General, DOJ, Deputy Assistant Director, FBI, and National Security Agency official, respectively). "BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE AT A HEARING ENTITLED 'REAUTHORIZING THE USA FREEDOM ACT OF 2015'." *Committee on the Judiciary, United States Senate*, November 6, 2019. https://www.judiciary.senate.gov/imo/media/doc/Wiegmann-Orlando-Morgan%20Testimony.pdf

The Government has used this authority responsibly. In 2018, the NSA identified certain technical irregularities in data it received from telecommunications service providers under the CDR provision. Because it was not feasible for NSA to resolve the issue tech-nologically, in May of 2018, NSA began the process of deleting all CDR data that it had received since 2015. Then, after balancing the program's intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes, NSA sus-pended the CDR program.

NSA's decision to suspend the CDR program does not mean that Congress should al-low the CDR authority to expire. Rather, that decision shows that the Executive Branch is a responsible steward of the authority Congress afforded it, and that the numerous constraints on the Government imposed by the FREEDOM Act, including oversight by the FISC, are demanding and effective. As technology changes, our adversaries' trade-craft and communications habits continue to evolve and adapt. In light of this dynamic environment, the Administration supports reauthorization of the CDR provision so that the Government will retain this potentially valuable tool should it prove useful in the future.

The Administration looks forward to working with this Committee and the rest of the Congress to reauthorize on a permanent basis these important national security provi-sions.

6.4.3 White Nationalism

NSA surveillance could provide forewarning to white supremacist terror attacks.

Levinson 19

Robert Levinson (retired U.S. Air Force intelligence officer with over 20 years of service. Since retirement he has worked as a lobbyist, defense contractor, and now works as a defense analyst). "THE FIGHT IN THE RIGHT: IT IS TIME TO TACKLE WHITE SUPREMACIST TERRORISM GLOBALLY." War on the Rocks, August 22, 2019.

https://warontherocks.com/2019/08/the-fight-in-the-right-it-is-time-to-tackle-white-supremacist-terrorism-globally/

Short of outright drone strikes or other forms of direct military action, there is still much more that can probably be done. Hoffman suggests that "additional intelligence sharing, training, and education to keep pace with this dynamic, unfolding threat is needed." In addition to intelligence sharing, the CIA and other intelligence agencies probably need to include white supremacist groups overseas in their collection target set. The killer in New Zealand was from Australia. Apparently, he had never been on any law enforce-ment or intelligence agency radar. In the future, if the United States can identify some of these people, then agencies can warn allies that they were headed their way and they could do the same for America. U.S. anti-terror "No Fly" lists are admittedly problem-atic from a civil liberties perspective. What linkages to terrorism get one placed on the list are secret and ambiguous; however, these lists might be reformed, with linkages to white supremacist terror included in the criteria for putting people on them.

After any Islamic extremist attack there is always much discussion of whether or not there was "chatter" picked up by the NSA which might have provided forewarning. Given white supremacists' extensive presence online in social media, are American on-line collection efforts postured to pick up this kind of chatter? We know that the New Zealand and the Poway killers — and possibly the El Paso shooter as well — posted manifestos online shortly before their acts. Would sophisticated early warning algo-rithms have picked these up in time to prevent the attacks? Probably not. However, tuning these collection tools in the direction of white supremacism could point to sus-pect individuals.

On July 8 the FBI put out a request for proposal to industry soliciting just such a capa-bility. The request for proposals stated:

The use of social media platforms, by terrorist groups, domestic threats, foreign intel-

ligence services, and criminal organizations to further their illegal activity creates a demonstrated need for tools to properly identify the activity and react appropriately. With increased use of social media platforms by subjects of current FBI investigations and individuals that pose a threat to the United States, it is critical to obtain a service which will allow the FBI to identify relevant information from Twitter, Facebook, Insta-gram, and other Social [sic] media platforms in a timely fashion.

6.4.4 White Nationalism – Empirics

Empirically, European surveillance agencies have spied on white nationalists in attempt to maintain security.

Levinson 19

Robert Levinson (retired U.S. Air Force intelligence officer with over 20 years of service. Since retirement he has worked as a lobbyist, defense contractor, and now works as a defense analyst). "THE FIGHT IN THE RIGHT: IT IS TIME TO TACKLE WHITE SUPREMACIST TERRORISM GLOBALLY." War on the Rocks, August 22, 2019.

https://warontherocks.com/2019/08/the-fight-in-the-right-it-is-time-to-tackle-white-supremacist-terrorism-globally/

Increasingly though, there is recognition that white supremacist terror in the United States is part of a global phenomenon. In January 2019, the Diaspora Affairs Ministry of Israel, which monitors global antisemitism, released a report, identifying far-right linked incidents as the most serious threats to Jews worldwide and noted "that the most violent antisemitic incidents in the US came from far Right elements such as Neo-Nazis and white supremacists." The New York Times highlighted how the shooter in New Zealand "drew inspiration from white extremist terrorism attacks in Norway, the United States, Italy, Sweden, and the United Kingdom." The article went on to examine 350 white extremist terrorism attacks in Europe, North America and Australia from 2011 through 2017 and illustrated the connections, at least ideologically, between the various attacks across the globe. Bruce Hoffman wrote recently that attacks which aren't explic-itly directed by a higher authority — a seeming hallmark of today's Islamic terrorists — owe their origins to a Ku Klux Klan leader in the United States in the 1980s. Hoffman notes:

White nationalist terrorism and its violent, politically motivated variants — embracing racism, antisemitism, anti-immigration, and anti-government sentiments — have ex-isted in the United States, the United Kingdom, France, Germany, Italy, and Australia among other countries for decades.

While violent Islamic extremists have different ideological goals, it would seem that their networks and tactics are strikingly similar.

Vidhya Ramalingam, founder and director of Moonshot CVE, a company working to disrupt violent extremism, testified before congress on April 30 that "White nationalist terrorism has always been international, with fighters and ideologues moving across

borders," and that "The ongoing conflict in Ukraine drew in white nationalist foreign fighters on an unprecedented scale, with neo-Nazis and white supremacists from Brazil, the UK, Ireland, Italy, France, Sweden and dozens of other countries flocking to join the fight," in this case apparently against the Russian separatists.

Many of our allies are taking this seriously. The Dutch General Intelligence and Security Service has identified right-wing extremism as "a phenomenon in motion." Both the German and British domestic intelligence services have increased their efforts to track white nationalist extremism.

Writing in the Guardian, my cousin Rosa Schwartzburg has written how "white re-placement theory," which inspired the shooter in New Zealand and apparently also the shooter in El Paso, originated with the killer of 80 students in Norway in 2011. Re-call too that the marchers in Charlottesville were chanting "The Jews will not replace us."

6.4.5 White Nationalism – Impact

The impact is real – white nationalism is the deadliest national security threat

Levinson 19

Robert Levinson (retired U.S. Air Force intelligence officer with over 20 years of service. Since retirement he has worked as a lobbyist, defense contractor, and now works as a defense analyst). "THE FIGHT IN THE RIGHT: IT IS TIME TO TACKLE WHITE SUPREMACIST TERRORISM GLOBALLY." War on the Rocks, August 22, 2019.

https://warontherocks.com/2019/08/the-fight-in-the-right-it-is-time-to-tackle-white-supremacist-terrorism-globally/

But now, sparked by the March 15 attack on a mosque in Christchurch, New Zealand, and reinforced by the April 28 attack at the synagogue in Poway, California and the latest shootings in Gilroy and El Paso, it may be time to consider whether terrorism variously categorized as being inspired by white supremacy, white nationalism, Neo-Nazi, etc., and its various manifestations and adherents, has reached the threshold of "terrorists of global reach" who are now claiming victims in the United States home-land. The El Paso shooter posted a diatribe online specifically citing the manifesto of the shooter in New Zealand as inspiration. This doesn't seem far removed from the Ft. Hood shooter's communication with a radical Islamic cleric overseas. Does the United States now need to devote resources and develop strategies to counter this threat with a level of effort similar to that which we devote to counter the Islamic State and other Islamic extremist groups?

Beyond the Home Front

That there is a serious domestic terrorist threat is not disputable; rather, it is the grow-ing international component that requires new strategies and tools. In testimony be-fore the House of Representatives in April, FBI director Christopher Wray included the threat from "white supremacist" with other forms of violent extremism as a "persis-tent, pervasive threat." On July 23, Wray said that the agency has made about 100 do-mestic terrorism-related arrests since October, the majority of which were tied to white supremacy. "I will say that a majority of the domestic terrorism cases that we've investi-gated are motivated by some version of what you might call white supremacist violence, but it does include other things as well," Wray said.

A report from the Anti-Defamation League reports, "In 2018, domestic extremists killed at least 50 people in the U.S., a sharp increase from the 37 extremist-related murders doc-

umented in 2017," and that "White supremacists were responsible for the great majority of the killings, which is typically the case." The organization's heat map for 2018 shows 1,318 incidents ranging from propaganda to murder tied to white supremacy across the United States.

An extensive report from Vice News in November detailed "a project to unify fascists and link that vast coalition of individuals into a network training new soldiers for a so-called forthcoming"race war." Not ironically, the effort is called "The Base," a literal translation of the Arabic term, "al-Qaeda." Clearly the case for a persistent, pervasive, and growing white supremacist-inspired domestic terrorist threat is strong, and law enforcement agencies seem alert to the domestic problem.

6.4.6 AT: No Evidence

The best evidence of surveillance working is the lack of terror attacks since 9/11.

Francis 13

David Francis (correspondent for The Fiscal Times). "5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)." Business Insider, June 11, 2013. https://www.businessinsider.com/nsa-surveillance-prism-phone-nsa-big-deal-2013-6

1. Online surveillance has been effective and is an important tool in the fight against terrorism. Lawmakers have said that data mining stopped attacks in the United States and overseas. The programs also provide U.S. authorities with leads on potential and existing terrorists. One NSA official told the Washington Post that PRISM provided a "field of dots" which allowed authorities to connect the rele-vant ones.

But the best justification for the program has been what has not occurred. Since 9/11, there has only been one major terror attack on U.S. soil.

The increasing role of technology in society means that surveillance will gain more importance for national security purposes.

Gerstell 20

Glenn S. Gerstell (served as general counsel of the National Security Agency from 2015 to 2020 and is now a senior adviser at the Center for Strategic and International Stud-ies). "FISA's Current Controversies and Room for Improvement (Part Two)." *Council on Foreign Relations*, June 24, 2020. https://www.cfr.org/blog/fisas-current-controversies-and-room-improvement-part-two

No one should minimize the intrusiveness of government surveillance or argue that it shouldn't be strictly regulated. Nonetheless, the imbalance between the ability of the government to obtain information for national security purposes, and the vast, largely unlimited and unregulated abilities of the private sector to collect and use personal data needs rationalization. As the private sector generates ever more data, due to the advent of 5G telephony, the proliferation of the internet of things, and the increasing role of

artificial intelligence, it makes sense to permit the government to use that data for na-tional security purposes, with whatever limitations our society wishes to impose. FISA, as currently constructed, is largely ignorant of these technological trends.

6.4.7 AT: Out of Use

NSA surveillance never stopped.

Reed 20

Kevin Reed (World Socialist Web Site). "US Senate reauthorizes domestic surveil-lance, allows access to internet histories." *World Socialist Web Site*, May 16, 2020. https://www.wsws.org/en/articles/2020/05/16/surv-m16.html

However, the rejection of the Wyden-Daines amendment was bipartisan. That vote explicitly makes key aspects of the National Security Agency (NSA) data gathering op-eration, exposed by former intelligence contractor Edward Snowden in 2013, a legal government practice and shows that the electronic surveillance of US citizens is ongo-ing and has never stopped.

6.5 Political Controversy

6.5.1 Trump

NSA surveillance has become impossibly political --- ending NSA surveillance is politically radioactive and gives Trump an avenue to reintroduce false claims he was spied on by the Obama administration.

Gerstell 20

Glenn S. Gerstell (served as general counsel of the National Security Agency from 2015 to 2020 and is now a senior adviser at the Center for Strategic and International Stud-ies). "FISA's Current Controversies and Room for Improvement (Part Two)." *Council on Foreign Relations*, June 24, 2020. https://www.cfr.org/blog/fisas-current-controversies-and-room-improvement-part-two

President Trump's claims of improper surveillance during his 2016 presidential cam-paign and the ensuing highly publicized inquiries by the executive branch and Congress have all created an atmosphere where the Foreign Intelligence Surveillance Act (FISA) has become almost impossibly political. First, recently declassified documents [PDF] show that conversations between former National Security Adviser Michael Flynn and the Russian ambassador to the United States were apparently captured under FISA, pre-sumably with the ambassador as a target. (Normally, the U.S. government does not con-firm or deny the existence or nature of any FISA surveillance.) Members of the Repub-lican Party later alleged that in its closing days the Obama administration improperly combed through FISA intelligence reports to dig for political dirt on incoming Trump administration officials who were having conversations with foreign officials. There hasn't been any showing that the foreign surveillance was improper; Flynn's statements to the FBI in the subsequent investigation were the basis for criminal charges. The al-legations about the Obama administration's use of intelligence reports have also been discredited, since it appears that no digging for or "unmasking" of Flynn's name was required in the first place.

The so-called "unmasking" controversy lingers, however, and colors the current debate about reauthorizing parts of FISA that came up for renewal at the end of 2019, which had been put in place for only a short time to allow Congress to revisit controversial sections of the act in light of operational success or failure or any intervening technolog-ical changes. The most significant of the expiring provisions were ones permitting the

FBI to obtain a broad range of business records for foreign intelligence purposes and enabling the National Security Agency (NSA) to continue its by then-abandoned call data records program.

Any renewal of those provisions would already have been problematic, given increased attention to (among other things) digital privacy, but it became exceptionally difficult in the current political environment. In particular, the report [PDF] of the Department of Justice inspector general regarding the FBI's investigation of Carter Page, former ad-visor to President Trump, was erroneously cited as evidence of the need for FISA re-form. Although the report found sloppy procedures (and worse) at the FBI, none of the report's nine recommendations said anything about problems with FISA itself; more-over, the sections of FISA relevant to Carter Page had nothing to do with the provisions coming up for renewal. Although the Trump administration supported a reauthoriza-tion, Congress proved unable to agree on anything other than a short-term extension to March 15, 2020, and thereafter the authority for those provisions expired.

6.6 AT: Privacy

6.6.1 Alternate Causes

Businesses and personal sharing of data are massive alternate causes.

Francis 13

David Francis (correspondent for The Fiscal Times). "5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)." Business Insider, June 11, 2013. https://www.businessinsider.com/nsa-surveillance-prism-phone-nsa-big-deal-2013-6

3. Private businesses are collecting data too. The government isn't the only one in the data collection business. Private businesses are also are mining data. Check out the below chart from MIT's Technology Review:

As the chart shows, businesses are quietly collecting data on consumers to better posi-tion advertising and to inform their business strategies. And much of the information is given to these companies willingly.

4. Any terrorist who doesn't think they're under constant surveillance is an amateur. Effective terrorists aren't stupid; the 2001 terrorist attack proved that. The truly dangerous ones know they are under constant surveillance and take steps to avoid detection. Any would-be jihadist who uses their mobile phone to explicitly make plans to destroy America is probably not a danger (and is also probably headed to a secret prison).
5. We're all complicit in this. Americans love to share data. We post photos and videos on social media without a second thought. Rarely do we think about what they're letting the world know.

For instance, I can outright determine or logically deduce the following things about the most active people in my Facebook feed: where they live; where they work; roughly how much money they make; how many children they have; where their children go to school; what time they drop off and pick up these kids at school; where they vacation; where they spend social time; what and when they eat; what family and interpersonal issues they're having; their politics; where they were educated; their television and read-ing habits; what music they listen to; and when they and the other members of their family were born.

All of this - and much, much more - can be determined with just a brief visit to Facebook. Why are people worried about the government invading their privacy when they've been volunteering private information online for years?

6.6.2 Not Invasive

No privacy invasion – individual conversations aren't being monitored.

Francis 13

David Francis (correspondent for The Fiscal Times). "5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)." Business Insider, June 11, 2013. https://www.businessinsider.com/nsa-surveillance-prism-phone-nsa-big-deal-2013-6

2. We've been under surveillance for more than a decade. The government has been monitoring online and telephone activity for more than a decade. During the Bush years, NSA was able to monitor phone calls without a warrant.

President Obama said he has put strict protocols in place that require judicial review and a warrant for all PRISM targets. He and other officials also said the government is not listening to your conversations or reading your email. It's simply identifying phone numbers that could be connected to terrorists.

6.6.3 Protections Now

The NSA maintains privacy protections in the status quo.

ProPublica 13

ProPublica (independent, nonprofit newsroom that produces investigative journalism with moral force). "FAQ: What You Need to Know About the NSA's Surveillance Programs." ProPublica, August 5, 2013. https://www.propublica.org/article/nsa-data-collection-faq

Does the NSA do anything to protect Americans' privacy?

Yes. First, the NSA is only allowed to intercept communications if at least one end of the conversation is outside of the U.S. -- though it doesn't have to distinguish domes-tic from foreign communication until the "earliest practicable point" which allows the NSA to record bulk information from Internet cables and sort it out later. When the NSA discovers that previously intercepted information belongs to an American, it must usu-ally destroy that information. Because this determination cannot always be made by computer, this sometimes happens only after a human analyst has already looked at it.

The NSA also must apply certain safeguards. For example, the NSA must withhold the names of U.S. persons who are not relevant to ongoing investigations when they dis-tribute information -- unless that person's communications contain evidence of a crime or are relevant to a range of national security and foreign intelligence concerns.

Also, analysts must document why they believe someone is outside of the U.S. when they ask for addition information to be collected on that person. An unknown number of these cases are audited internally. If the NSA makes a mistake and discovers that it has targeted someone inside the U.S., it has five days to submit a report to the Department of Justice and other authorities.

6.6.4 AT: Metadata

There's no evidence of metadata privacy abuses under the new Freedom Act.

Wiegmann, Orlando, and Morgan 19

Bradford Wiegmann, Michael J. Orlando, and Susan Morgan (Deputy Assistant Attorney General, DOJ, Deputy Assistant Director, FBI, and National Security Agency official, respectively). "BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE AT A HEARING ENTITLED 'REAUTHORIZING THE USA FREEDOM ACT OF 2015'." *Committee on the Judiciary, United States Senate*, November 6, 2019. https://www.judiciary.senate.gov/imo/media/doc/Wiegmann-Orlando-Morgan%20Testimony.pdf

To be sure, this authority has generated substantial controversy because it was em-ployed, with FISC approval, to support NSA's bulk telephony metadata collection pro-gram. However, that program has been terminated and replaced by the more targeted collection of telephony metadata authorized under the CDR provisions of the FREE-DOM Act, as discussed below. The FREEDOM Act permanently banned bulk collec-tion altogether under the business records authority and required the use of a "specific selection term" to justify an application for a business records order. The law defines "specific selection term" as a term that "specifically identifies a person, account, address, or personal device, or any other specific identifier [that] is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought, consistent with the purpose for seeking the tangible things." 50 U.S.C. § 1861(k)(4)(A)(i). It does not in-clude terms, or a combination of terms, that are not so limited. See id. § 1861(k)(4)(A)(ii). Moreover, the FREEDOM Act provided that the FISC may evaluate the adequacy of min-imization procedures issued under the business records provisions, and may require additional, particularized minimization procedures beyond those otherwise required, with regard to the production, retention, or dissemination of certain business records, including requiring the destruction of such records within a reasonable period of time. See id. § 1861(g)(3).

The Government has used the business records authority judiciously. On average, be-tween 2015 and 2018, the Government sought and obtained records under this provision less than 76 times per year. The number of business records applications approved has decreased every year since 2012. Many of these investigations involve scenarios that are outside the scope of the National Security Letter statutes, and often a business records

order is sought because national security interests preclude the use of less secure crimi-nal authorities, or because there may be no criminal investigation underway. Given the importance of the authority, the absence of any evidence of abuse, and the additional safeguards Congress imposed in 2015, we urge the Committee to support permanent reauthorization of this provision.

6.6.5 AT: Unconstitutional

Surveillance regimes are constitutionally sound – SCOTUS cases are explicitly narrow and can't be extrapolated to new technologies.

Gerstell 20

Glenn S. Gerstell (served as general counsel of the National Security Agency from 2015 to 2020 and is now a senior adviser at the Center for Strategic and International Stud-ies). "FISA's Current Controversies and Room for Improvement (Part Two)." *Council on Foreign Relations*, June 24, 2020. https://www.cfr.org/blog/fisas-current-controversies-and-room-improvement-part-two

Congress will have more latitude than one might think to craft new surveillance regimes that are constitutionally sound. The Fourth Amendment sets limits on how the govern-ment may access increasingly revealing and important data, but there is surprisingly little specific guidance offered by the judiciary in this area. Most Fourth Amendment cases deal with specific surveillance techniques, such as the use of cellphones to track location, infrared detectors, or GPS tracking devices, and are difficult to extrapolate to new technologies. Indeed, the Supreme Court's most recent pronouncement in this area explicitly said it was a "narrow decision" [PDF].