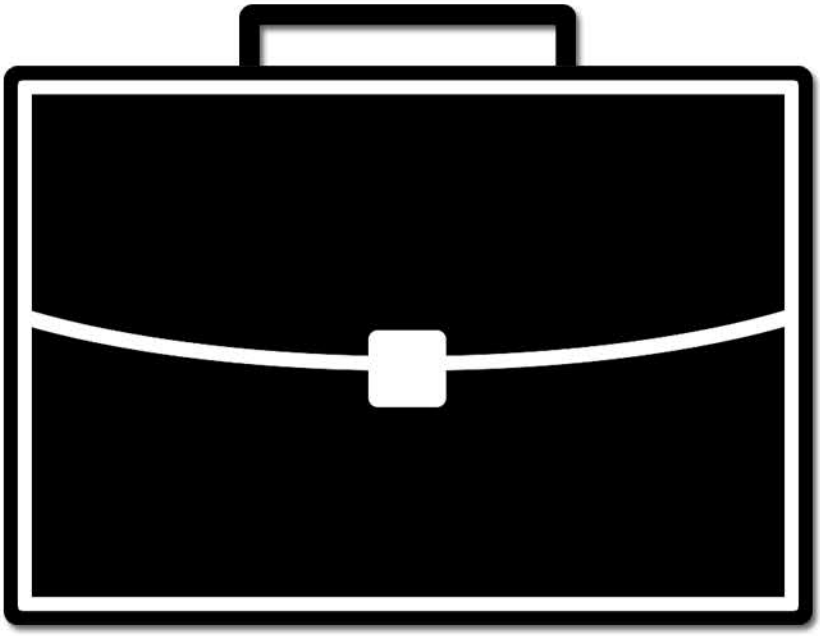
# Champion Briefs

## January 2021

## Public Forum Brief



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

# Champion Briefs

Resources for Speech & Debate



## About Our Briefs

Our briefs help students expand their knowledge base, improve their analytical skills, and prepare for competition. Each brief includes:

- Varied perspectives from expert writers
- In-depth topic analyses
- Cited evidence sorted by argument
- Peer-reviewed and edited guidance
- Background information & topic framing

# Second Semester Subscriptions

## Lincoln-Douglas

Non-Subscription: $74.97

**Subscription: $69.99**

Includes briefs for every Lincoln-Douglas debate topic from September through April plus briefs for the novice topic and for NSDA National Tournament

## Public Forum

Non-Subscription: $149.94

**Subscription: $134.99**

Includes briefs for every Public Forum debate topic from September through April plus briefs for the NCFL and NSDA National Tournaments

## PF/LD Combo

Non-Subscription: $224.91

**Subscription: $194.99**

**Save an additional 15%**

**Coupon: WINTER20**

Expires: 1/1/2021

**We accept purchase orders and all major credit cards**

# www.ChampionBriefs.com

ISD
INSTITUTE for SPEECH and DEBATE
#ISDDIFFERENCE

# Experience the #ISDDifference at ISD 2021!


## Equal Access to Instructors

-Our junior instructors have been on the big stage and know how to prepare you to get there.
-We don't rank our labs. All students get access to our championship staff and individualized attention.

## The Adults are in Charge

-Senior Instructors lead EVERY lab at ISD.
-We focus on skills, not tricks. We win the right way.
-Multiple NSDA Hall of Fame Members are on staff.

## The ISD Family

-We're more than a camp. We form a community that will support you all season long.


## Student Safety is Our Priority

-A dedicated residential life staff, including a 24/7 on-campus nurse that is available to all students.
-A firm and unapologetic zero tolerance policy for substance use and other egregious behavior.

**ISD: Online**
June 20 - July 3

**ISD: Florida**
June 26 - July 9

**ISD: Carolina**
July 11 - July 24

# Learn more at ispeechanddebate.com!

## The Evidence Standard

Speech and Debate provides a meaningful and educational experience to all who are involved. We, as educators in the community, believe that it is our responsibility to provide resources that uphold the foundation of the Speech and Debate activity. Champion Briefs, its employees, managers, and associates take an oath to uphold the following Evidence Standard:

1. We will never falsify facts, opinions, dissents, or any other information.
2. We will never knowingly distribute information that has been proven to be inaccurate, even if the source of the information is legitimate.
3. We will actively fight the dissemination of false information and will provide the community with clarity if we learn that a third-party has attempted to commit deception.
4. We will never knowingly support or distribute studies, news articles, or other materials that use inaccurate methodologies to reach a conclusion or prove a point.
5. We will provide meaningful clarification to any who question the legitimacy of information that we distribute.
6. We will actively contribute to students' understanding of the world by using evidence from a multitude of perspectives and schools of thought.
7. We will, within our power, assist the community as a whole in its mission to achieve the goals and vision of this activity.

These seven statements, while simple, represent the complex notion of what it means to advance students' understanding of the world around them, as is the purpose of educators.

## Letter from the Editor

The resolution for Public Forum Debate for January 2021 will be, “Resolved: The NSA should end its surveillance of U.S. citizens and lawful permanent residents.” This topic is an interesting choice, given that there are so many other issues that have dominated the headlines more prominently as of late, but it’s still a very good topic for debate. It’s also relevant given that courts have recently sided with Snowden by ruling that the NSA’s practices he exposed were in fact illegal, as he claimed. It also looks increasingly likely that he will remain in Russia, as he was granted permanent residency by the Russian government earlier this year. All in all, while NSA surveillance hasn’t been the most talked about issue of 2020, it remains an incredibly relevant discussion surrounding the tradeoff of personal freedom for security.

What intrigues me about this topic is that it will force students to compare immeasurable impacts. In Public Forum, debaters often trend towards quantifiable, measurable impacts yet this topic is likely to force students out of their comfort zone in the sense that it will require them to make arguments about why rights violations outweigh more tangible impacts and vice versa. From my perspective, this will be a great chance for debaters to practice their weighing skills, as too often PF debate rounds come down to a clash of cost versus lives saved.

Ultimately, I believe this topic will provide all of you with a great chance to discuss one of the most important tradeoffs in the world of national security. As always, I wish you the best of luck. I encourage you to explore the history of the NSA, and reconsider your own beliefs about surveillance.

Michael Norton
Editor-in-Chief

## Table of Contents

**The Evidence Standard ..... 5**

**Letter from the Editor ..... 6**

**Table of Contents ..... 7**

**Topic Analyses..... 10**

Topic Analysis by Sara Catherine Cook ..... 11
Topic Analysis by Jakob Urda ..... 23
Topic Analysis by Tucker Wilke..... 30

**General Information..... 42**

**Pro Arguments ..... 54**

PRO: The NSA surveillance program amounts to authoritarianism ..... 55
PRO: The NSA surveillance program can be hacked ..... 62
PRO: The NSA surveillance program should be ended by the Freedom Act..... 69
PRO: The NSA surveillance program harms mental health ..... 75
PRO: The NSA surveillance program runs contrary to the right to be forgotten..... 83
PRO: NSA Surveillance hurts U.S. credibility ..... 91
PRO: NSA surveillance is unconstitutional..... 95
PRO: Ending NSA Surveillance ends surveillance on minorities ..... 99
PRO: NSA Surveillance is inefficient..... 106
PRO: NSA Surveillance hurts the economy ..... 110
PRO: The NSA spies on activists and protestors..... 114
PRO: NSA spying is unpopular among Americans ..... 118
PRO: The NSA is subject to leaks ..... 121
PRO: The NSA antagonizes China and Chinese Americans..... 124
PRO: NSA surveillance is an invasion of privacy..... 127

**Pro Responses to Con Arguments..... 131**

A/2: NSA will be critical to stopping cyber attacks ..... 132
A/2: The NSA Prevents Terrorist Attacks..... 136
A/2: NSA Surveillance Maintains Safety..... 140
A/2: The NSA is good for the economy ..... 144

A/2: Surveillance can stop the spread of COVID-19 ..... 148
A/2: Reforming NSA surveillance is preferable to ending it ..... 151
A/2: NSA surveillance is preferable to FBI surveillance ..... 155
A/2: Ending NSA surveillance props up Big Tech ..... 158
A/2: NSA surveillance enables offensive cyber operations ..... 162
A/2: The NSA surveillance program is well regulated ..... 166
A/2: The NSA is essential to stopping Chinese cyberattacks ..... 168
A/2: The NSA stops radical anti-government groups ..... 170
A/2: The NSA saves lives ..... 172
A/2: The NSA is cost-efficient ..... 174
A/2: The NSA surveillance program is justified under the constitution ..... 176

**Con Arguments ..... 178**

CON - NSA will be critical to stopping cyber attacks ..... 179
CON - The NSA Prevents Terrorist Attacks ..... 184
CON - NSA Surveillance Maintains Safety ..... 190
CON - The NSA is good for the economy ..... 194
CON – Surveillance can stop the spread of COVID-19 ..... 200
CON – Reforming NSA surveillance is preferable to ending it ..... 204
CON – NSA surveillance is preferable to FBI surveillance ..... 208
CON – Ending NSA surveillance props up Big Tech ..... 212
CON – NSA surveillance enables offensive cyber operations ..... 217
CON – The NSA is essential to stopping Chinese cyberattacks ..... 221
CON – The NSA stops radical anti-government groups ..... 225
CON – The NSA saves lives ..... 228
CON – The NSA is cost-efficient ..... 230
CON – The NSA surveillance program is justified under the constitution ..... 232
CON – The NSA surveillance program is well regulated ..... 235

**Con Responses to Pro Arguments ..... 238**

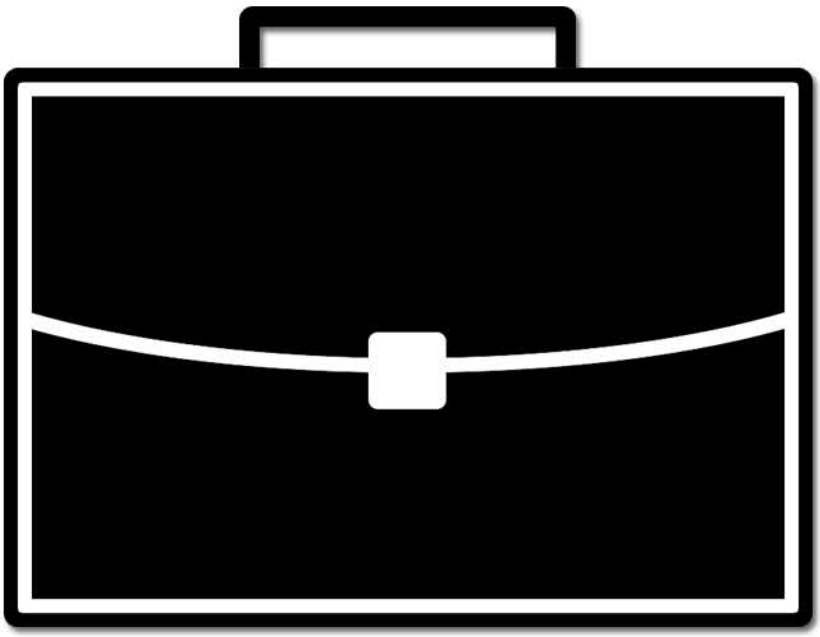
A/2: The NSA surveillance program amounts to authoritarianism ..... 239
A/2: The NSA surveillance program can be hacked ..... 244
A/2: The NSA surveillance program should be ended by the Freedom Act ..... 248
A/2: The NSA surveillance program harms mental health ..... 253
A/2: The NSA surveillance program runs contrary to the right to be forgotten ..... 257
A/2 - NSA Surveillance hurts U.S. credibility ..... 260
A/2 - NSA surveillance is unconstitutional ..... 263

A/2 - Ending NSA Surveillance ends surveillance on minorities....266
A/2 - NSA Surveillance is inefficient....270
A/2 - NSA Surveillance hurts the economy....274
A/2: The NSA spies on activists and protestors....277
A/2: NSA spying is unpopular among Americans....280
A/2: The NSA is subject to leaks....283
A/2: The NSA antagonizes China and Chinese Americans....285
A/2: NSA surveillance is an invasion of privacy....288

# Champion Briefs

## January 2021

## Public Forum Brief



# Topic Analyses

# Topic Analysis by Sara Catherine Cook

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

**Introduction**

The National Security Agency was created in the 1950s by President Truman to decode communications during WWII, and since then, has become the largest U.S. intelligence organization. There are two main departments of the NSA: signals intelligence and cybersecurity. This topic will likely focus on the former. Signals intelligence is derived from electronic signals like communication signals, weapon signals, and radars. The NSA is specifically limited to gathering information about international terrorists and foreign powers and has special regulations on domestic surveillance. The NSA's domestic activities are supposed to be limited by the Fourth Amendment, which prohibits unreasonable searches and seizures. Even more so, the Foreign Intelligence Surveillance Act (FISA) regulates domestic surveillance by prescribing procedures for requesting judicial authorization for electronic surveillance and punishing those who do not comply. Unfortunately, the NSA has not always been compliant. In 2013, Edward Snowden publicized NSA surveillance of the communications of over a billion people worldwide, including U.S. citizens, as well as NSA tracking of hundreds of millions of people's movements using cell phone metadata. There has been controversy regarding what signal intelligence can be used for since the rise of NSA surveillance in the

aftermath of 9/11. In September 2020, the now-defunct NSA surveillance programs that collected bulk logs of domestic phone calls were deemed unlawful by the Supreme Court.

**What is the status quo for this topic?**

Due to the secrecy of the NSA as well as their track record for lying about surveillance, the status quo of surveillance will be up for debate on this topic. The NSA apparently quietly shut down the program that analyzes logs of domestic phone calls in 2019 but continues officially to accept customer data from Facebook, Google, Apple, as well as other tech companies, as legally required by the PRISM program. This includes things like emails, messages, and documents. The NSA also has a hacking unit, Tailored Access Operations that enables the NSA to break into consumer electronic devices and IT systems. In the past, they have retained backdoors by planning to give themselves built-in access to data through popular products. Lastly, even though the NSA claims it no longer collects bulk data on your movements, cell phone providers are required to do so via cell phone towers and have to give those records to the NSA when ordered by a court. Essentially, even when there are regulations on what type of domestic data the NSA can collect, they can find many ways through the tech sector to obtain the same data they were pre-regulations. This is, of course, mostly speculation based on the capabilities of the NSA and past precedent of what they have done. Ultimately, it will be up to debaters in the round to define the status quo of surveillance, which will affect potential impacts on things like terrorism and the harms of decreased personal privacy in the round. Neg teams will want to limit the scope of surveillance to minimize the impact on the average American citizen but preserve that the government is doing enough surveillance to

deter and catch terrorism before it happens. Aff teams, on the other hand, will want to minimize the usefulness of the data that the NSA does collect and emphasize the mass invasion of privacy through current NSA surveillance measures. One other complication of this topic is that there have been numerous changes to surveillance practices over the past couple of decades; this makes it incredibly important for teams to be well informed on which practices are still happening and which practices have been left in the past.

**Why Impacts Deserve Special Attention**

Along with the challenge of understanding the true nature of NSA surveillance, impacting on this topic will also be challenging. Let's talk about this for each common impact you might see on this topic. The first is the impact of decreasing or deterring terrorism. The main issue with this sort of impact is that it is hard in any context to quantify and contextualize prevented terror attacks. There is simply no way to know how many terrorist attacks would happen in a world without NSA surveillance. Similarly, there is also no way for us to know how many terrorist attacks the NSA has prevented, with Snowden even claiming that they have never prevented one. This means that teams reading arguments about terrorism should pay special attention to the warranting of the argument. To make a clear argument, teams will need to explain why the NSA prevents or emboldens terrorists rather than relying on statistics or assumptions to make the argument for them. Terrorism in itself is often a hard argument to make. Because terrorist attacks in nature are somewhat unpredictable, it is hard to correlate a rise or fall in terrorism with one specific factor. Look no further than continuous debates on whether counterterrorism mechanisms are effective or counterproductive to see that there is a

controversy of whether U.S. actions improve or worsen the situation. Teams should handle this ambiguity by understanding and preparing for arguments about alternative factors that could have contributed to the rise or fall of terrorism over the past few decades.

Another common impact on this topic will be the various harms of decreased personal privacy or, in other words, the harms of surveillance to the average citizen. These are not only similarly hard to quantify because of the limited information each person has on surveillance, but also have effects that are hard to understand or measure. For example, while it is clear that post-9/11 surveillance took on a new form, it is impossible to attribute all of the changes, islamophobia, racism, etc. specifically to surveillance and thus hard to quantify the effect the NSA had. Similarly, it is hard to prove that surveillance specifically caused enough harm to an individual or domestic citizens as a whole to cause the type of meaningful impact teams would find easy to use in a debate round. This means that teams reading arguments related to the impact of surveillance on the average citizen should also focus on further harms that different narratives can cause. Has NSA surveillance contributed to and heightened widespread racism and islamophobia within this country? What have the consequences of that been? Has surveillance led to widespread distrust of the government or some sort of psychological distress? What does that mean in the context of the debate round? While terrorism often carries a lot of weight in magnitude despite having seemingly low probability, everyday harms of surveillance encounter the exact opposite issue. They often accumulate over time and are sometimes invisible compared to more publicized impacts.

My final note about impacting on this topic is that it is also possible that there would not be a large or super tangible impact on passing this resolution. Teams on this topic might have to

dig for less likely or exaggerated scenarios to present a convincing and meaningful narrative in the round. Keep in mind that more ambiguous impacts should be compensated by a more detailed analysis of why NSA surveillance causes that effect.

**A Note about Building Complete Arguments on this Topic**

This is a policy resolution, which means that affirming the resolution passes a specific motion and negating retains the status quo. Many teams on this topic will find it easy to build a case either on something happening in the status quo or the future prescribed by the Aff world. Here is why both of these methods are incomplete. Let's say, for example, you make an argument about why NSA surveillance is bad, and thus you should affirm the resolution. This is a good argument to make given that you are supporting ending NSA surveillance on domestic citizens, but you have failed to account for what a world will look like after you have passed the resolution. Even if you prove that surveillance has some tangible harm, you specifically need to show some tangible benefit for eliminating that harm. Similarly, some teams will also build a case about why eliminating some facet of surveillance will be a bad thing for the world. They also have a burden of proving how that facet of surveillance somehow improves the world in the status quo. If the other teams were to come up and provide evidence about how the status quo methods of surveillance are ineffective, the case would be considerably less strong. This is all to demonstrate that in policy resolutions, you have to look at the before and the after of each situation to build a particularly strong argument for either side.

**Affirmative Argumentation**

Now that we have discussed some of the specific considerations and I would argue complications of this topic, let's discuss some possible Affirmative arguments. The first deals with the decreased personal privacy of citizens and the possible racial targeting of domestic surveillance. Along with the rise of islamophobia and racial targeting in the aftermath of 9/11, the NSA has been found to target Muslim-Americans in its surveillance. This can definitely be correlated with the rise of islamophobia in the country and is similar to the era of McCarthy-ism that drummed up communist fear during the cold war. Teams could take this argument in a few different directions. One option would be to attempt to solidify and quantify the effects on Muslim Americans as well as Middle Eastern Americans assumed to be Muslim via racial profiling from NSA surveillance. These could include direct effects from surveillance including psychological effects like living in fear as well as correlated effects of islamophobia that could be correlated with NSA targeted surveillance. Another option would be to make an advocacy argument, essentially pointing out that in an educational setting as well as in the world in general, we have an obligation to reject policies that support and embolden racial targeting and discrimination. This type of argument forces more on the moral consequences of the action rather than trying to quantify the harms of racism that have been repeatedly minimized in both debate rounds and policy considerations at large.

Focusing on the individual citizen, teams could make arguments about the consequences of decreased personal privacy. This could relate to the legality and potential consequences for society as a whole of government overstep. An interesting argument to make

could concern hacking efforts. The idea that the NSA leaves widespread technology with loopholes in it so that they can access the information could lead to hackers finding those same flaws and gaining access to that information. This not only could leave the U.S. open to cyberattacks at large, but could also hurt individual citizens via things like identity theft, which would be made easier by built-in loopholes that the NSA mandates.

Let's also talk about a world without NSA domestic surveillance. First and foremost, the money going into those programs would be directed elsewhere. You could make arguments regarding the most likely scenario of where that money will go, whether it be used to strengthen other NSA operations or used in a completely different section of the budget. There are two things to be cautious about when running funding arguments. First, you need to make sure to find concrete and warranted evidence about why the money would be redirected somewhere else in this particular scenario; otherwise, your argument would be a plan rather than a solid contention. Secondly, you should also be specific about the impacts of that spending. Small increases in spending in certain areas of the budget will have relatively small impacts. Second, you could make the argument that the NSA will shift focus away from domestic surveillance, leading to surveillance elsewhere. This really could be an Aff or Neg argument depending on whether you argue foreign surveillance is a good or bad thing.

One final argument I will mention here is one dealing with economic competitiveness. Because the NSA has special deals to collect the records of big tech companies in the U.S., there are arguments to be made that this hurts different companies' economic competitiveness, as other countries might be suspicious of the U.S. spying within the devices. We have seen a similar issue on the flip side with foreign-made companies like TikTok and Huawei. Because the

NSA both takes the records from these companies and obligates them to include loopholes in the devices, it makes sense that other countries, especially our adversaries could be skeptical of allowing U.S. technology into their countries. The one issue with this argument is of course that technology companies within the U.S. are extremely successful. Teams would need to show a tangible negative impact on the companies in the status quo or show a large benefit to the potential expansion of this technology into other countries.

**Negative Argumentation**

The first main argument on the Negative side deals with the actual goal of NSA surveillance: to protect the United States from terrorism, or more broadly any planned attacks. There are two ways that this could potentially happen. First, because the NSA collects information, they can find out about terrorism before it happens and therefore prevent it. The main issue with this argument is that Snowden, who leaked most of the information we know about NSA surveillance now, claims that the NSA has actually never prevented a terrorist attack directly. One reason this could be true is that it may be challenging and extremely time-consuming to sift through all of the information that the NSA collects. Even if there was sensitive information received, how often does the NSA receive it on time or receive it at all with the large bulk of the information they have access to? The second way the NSA could prevent terrorism is through deterrence. Even if the NSA does not directly find information to stop terrorist attacks, the institution as a whole could deter acts of terrorism because terrorists know that the NSA would intercept their information before the attack. Similarly, if the NSA is good at sifting through the information, this would make it much more difficult for groups of

people to communicate with each other outside of the watch of the NSA because they would be unable to use technology. This complication in itself could thwart the efforts and effectiveness of terrorists. Ultimately, worldwide we often see terrorism pop up most in areas of instability. This would mean that the best way to stop efforts of terrorism is to keep all institutional protections against them, regardless of how effective or ineffective they may seem.

Another argument one could make on the Negative side deals with how NSA surveillance affects undocumented immigrants and other countries. Though domestic surveillance would end, "international" surveillance affects immigrant and border communities. One could make the argument that when the NSA can no longer surveil domestically, it may specifically use immigrant communities to somehow tap into domestic surveillance. Even more so, just having to shift focus further to international surveillance could increase the money and time spent surveilling both undocumented immigrants in the United States as well as foreign countries. If teams were able to prove that eliminating domestic surveillance would lead to an increase in the time and money spent on surveillance abroad, they could also argue that an increase in international surveillance could increase tensions with other countries or increase the risk of things like a miscalculation. For example, if the U.S. received some sort of false indication that another country wanted to attack us, they could choose to strike first, leading us into a conflict that could have been avoided.

Overall, the mainline of argumentation on the Neg will focus on surveillance being used to prevent attacks and keep citizens safe. This means that it is paramount that teams find solid warranting and evidence of the NSA doing this in the status quo and prove that terrorists,

hackers, or other powers would see the limiting of the NSA as an opportunity to strike the U.S. On that note, there is potential for different types of perception arguments to be made on this topic, so teams should also explore the type of signal sent by limiting the powers of the NSA.

**Final Thoughts**

As mentioned before, this topic may be more challenging than others from a research perspective given the secrecy of the NSA and the many changes it has undergone in the past few years. I will emphasize again that this ambiguity makes it necessary to build arguments on strong warranting and logic, as much of the evidence on this topic will lack clear statistical backing. This topic also relates heavily to topics of the past, which may be helpful for your understanding. If you want to gain a deeper understanding of some of the harms to personal privacy, you should watch rounds on Youtube from the Internet of Things topic from November 2016. Though it deals less with the specific uses of information to the government, the Negative side was specifically limited to arguing via decreased harms to personal privacy which deals with similar issues this topic does. Ultimately, remember to build your arguments from both the status quo and from what would happen in a world without NSA domestic surveillance. Good luck on this topic and let's hope for a better 2021!

**Works Cited**

Dans, Enrique. "Will the US economy lose competitiveness over the NSA revelations?" 15 Jul 2013. https://medium.com/enrique-dans/will-the-us-economy-lose-competitiveness-over-the-nsa-revelations-ff6249f0dac7

McCarthy, Tom. "NSA director defends plan to maintain 'backdoors' into technology companies." *The Guardian.* 23 Feb 2015. https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

Risen, Tom. "Racial Profiling Reported in NSA, FBI surveillance." *US News.* 9 Jul 2014. https://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance

Savage, Charlie. "Disputed N.S.A. Phone Program is Shut Down." *The New York Times.* 4 Mar 2019. https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html

"How U.S. Intelligence Surveillance May Affect Immigrants." *Human Rights Watch.* 21 Feb 2017. https://www.hrw.org/news/2017/02/21/how-us-intelligence-surveillance-may-affect-immigrants#

"8 Ways the NSA is Spying on You Right Now" *ExpressVPN.* 7 May 2020. https://www.expressvpn.com/blog/8-ways-the-nsa-spies-on-you/

**About Sara Catherine Cook**

Sara Catherine Cook grew up in Birmingham, Alabama, and competed for The Altamont School for three years in Public Forum Debate. She was one of the first teams from her school to qualify for the Tournament of Champions and NSDA Nationals, being the only team from her state to qualify for the TOC in the 2018-2019 season. She now attends Dartmouth College in Hanover, NH where she plans to study Mathematics and competes with the Dartmouth Parliamentary Debate Team.

# Topic Analysis by Jakob Urda

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

**Introduction**

In the post-9/11 security space, few issues are more polarizing than domestic surveillance. Domestic surveillance is the newest iteration of the age-old “security versus liberty” debate. On one side are Thomas Hobbes and Jeremy Bentham, on the other side are John Stewart Mill and John Locke. This debate underpins many of our most pressing policy discussions, from the war on terror to counternarcotic policy. It is also deeply philosophical, forcing ourselves to ask questions such as 'what is privacy' and 'what do we give up to live in a safe society.' Finally, the topic is difficult because of the opacity involved in it. The government does not disclose the extent or results of its domestic surveillance programs, making conducting an accurate cost-benefit analysis difficult.

This is a topic that is pulled straight from modern headlines, and debaters must be able to speak to judges of many different political leanings to win rounds. Arguments must be crafted so as not to alienate judges of divergent political ideologies, but still hold firm in their convictions. Students need to understand and empathize with the other side of the topic and be able to step into their shoes to reveal their hidden assumptions.

**Strategic Considerations/Framing of the Debate**

Most arguments on this topic will center around a few narrow themes – privacy/liberty/discrimination, preventing terrorism and cyber-crime, and creating back doors. This is a strategic problem for most debaters for two reasons: (1) These impacts are generally hard to weigh against each other and unquantifiable and (2) if the NSA did not do these things another government agency probably would. The resolution only states that "the NSA" should end its surveillance of US citizens. However, it never says that America should reduce its overall espionage budget or ban domestic surveillance outright. The budget of the Intelligence community would remain the same (and probably increase) and other agencies would still be free to engage in domestic surveillance. Indeed, the FBI, CIA, DHS, and other government agencies all operate covert surveillance programs that spy on American citizens and lawful residents. If the NSA were barred from doing such activity, another agency would pick up the slack.

Thus, the strongest arguments on this topic will deal with a comparative analysis between the NSA and the other government agencies which would likely replace it. Being a good debater means understanding inherency and tradeoffs, and this topic is rife with both. Debaters must be able to paint a convincing picture about what will happen in a wild where the resolution is affirmed. What cascading policy changes will go into effect? How will funding be reallocated? These are the questions that will truly shape the terrain of the topic.

One crucial question about the resolution is how funding will be reallocated from the NSA. The resolution does not actually stipulate a decrease in the budget of the NSA. This leads

to two possible conclusions. First is the NSA retains its existing budget and repurposes the money towards spying on undocumented immigrants and foreigners. Remember that the resolution only stipulates no surveillance against American citizens and lawful permanent residents. Because undocumented immigrants are often the target of political ire, they are a likely candidate for surveillance. Debaters must reckon with the reality that the American government is not likely to simply throw up its arms and give up domestic surveillance altogether. The combination of lobbying, paranoia, and national security bureaucracy run too deep.

The other option is that the money is taken away from the NSA. However, it is unlikely that the money leaves the national security world. This is because of the "ratchet effect" where politicians are generally unwilling to reduce national security funding for fear of being seen as weak. Thus, even when individual programs are cut, the money is simply reallocated in the national security world. Debaters should be cautious before assuming that just because the NSA's programs are cut, the overall amount of money going to government domestic surveillance programs meaningfully decreases. In truth, the opposite might be the case; politicians feel pressured to appear tough so pair their individual cuts with broad across-the-board spending increases. This can lead to an overall increase in spending on surveillance and militarism, even if the NSA's specific surveillance budget goes down.

The question of where the money will go is part of the debate about *inherency*. Inherency is the idea that the resolution does not spell out all of the changes which happen when the resolution is enacted. Inherency means debating the topic as it would actually happen if it were to be affirmed in the real world, that is to say, looking at the most likely

implementation of the topic. The resolution is vague and does not cover every aspect of the topic such as the budget. Therefore many crucial aspects of the topic will have to be decided by the debaters in the round itself. The debate over inherency sets the terrain for the rest of the round.

**Affirmative Argumentation**

The affirmative should think about which impacts on the topic are quantifiable and well weighable. The issue with privacy impacts is that they are hard to stack up against lives lost and tangible national security outcomes. As such, affirmative teams should begin with arguments that can be stacked up effectively against common negative arguments.

One argument which the affirmative can make is about encryption back doors and foreign cyberattacks. Historically, the NSA has pressured companies to create and provide the NSA with “back doors” into their technology. This means that the NSA has methods of easily decrypt security systems around the country.

Unfortunately, by providing the NSA with the back doors that it needs to conduct domestic surveillance, we make the country more susceptible to cyber-attacks. This is because if information systems have built-in vulnerabilities then malign actors OTHER THAN the NSA may also exploit them. Back doors make the decryption of computer systems easier for everyone, not just the NSA. The impact is that cyber attacks can happen with increasing severity and cause more damage.

This is a strong argument because cyberattacks have large, quantified impacts. Debaters should look to history to understand the sheer amount of devastation which can come from

cyber attacks. The WannaCry attack, which some political commentators link back to the Russian government, caused millions of dollars in damage and froze vital systems in hospitals. Last year, hackers exploited a back door in an old Windows Operating System to wreak havoc on city and state governments around America. These systems can delay government programs such as welfare from being delivered, or freeze business owners out of their enterprise systems.

The crucial advantage of this point is that it is historically validated and weighable. It does not exist in the abstract, and every judge values it somewhat equally. There will be many judges who do not understand an abstract right to privacy, but all judges will agree that preventing cyber attacks against critical infrastructure is a core American national security interest.

**Negative Argumentation**

The negative should make simple, intuitive arguments about preventing crimes and terrorism. The core arguments on the negative side of this topic are simple to understand and weighable. Negative teams should focus on finding examples of specific instances where the NSA used domestic surveillance to foil plots. The affirmative will be able to dole out a litany of statistics on why the NSA is generally ineffective, but being able to provide examples will persuade the judge that a few, high impact scenarios are true.

NSA surveillance has been used in the conviction of dozens of criminal cases. The difficulty for the negative is proving what the impact of these contentions is. Because the terrorist plots were foiled, it is impossible to say what the exact impact would have been. However, the negative team can appeal to history and use examples of successful terrorist

plots. Negative teams will want to steer away from citing examples such as 9/11 because it is difficult to prove that this is the scope of the plot which would have been achieved. Instead, negative teams should use examples of lone-wolf style terrorist attacks that have been carried out in the recent past as proof that such attacks are possible and devastating. Negative teams must remember that these subjects are politically charged and also deeply personally sensitive to many.

Aside from terrorism, negative teams can argue that the NSA helps prevent cybercrime. There is some evidence that the NSA's domestic surveillance program has helped to crack down on deep-web cybercrime. The deep web is a part of the internet where anonymity allows people to exchange illicit goods and services, from drugs to prostitution. There is some evidence that the NSA's surveillance of American citizens allowed them to shut down some of the most active and dangerous parts of the deep web.

This topic is rich for interesting, provocative rounds. It will help educated debaters on an important contemporary issue and deepen their knowledge of politics and policy. The topic will reward those who diligently research and think creatively. Concentrate on well thought out research and simple but high impact contentions. Good luck and have fun!

**About Jakob Urda**

Jakob grew up in Brooklyn, New York. He attends the University of Chicago, where he will receive a BA in Political Science, and is interested in security studies and political economy. Jakob debate for Stuyvesant High School where he won Blake, GMU, Ridge, Scarsdale,

Columbia, the NCFL national championship, and amassed 11 bids. He coached the winners of the NCFL national tournament, Harvard, and Blake.

# Topic Analysis by Tucker Wilke

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

**Introduction**

After reverting to the tradition of foreign policy topics for January last year, the topic committee has changed things by making this year's January Public Forum topic about a controversial piece of domestic policy, as it is "The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents." As is now custom, this is the first single month topic this year, although even that is not quite the case, as the Blake tournament, which takes place in late December, still famously uses the January topic, a tournament which often sets the table for the month of argumentation. Given the shortened month, teams may be tempted to cut back on background research and general information to get their arguments ready as quickly as possible. While teams will have to prioritize, I would encourage them to resist this urge as much as possible. NSA surveillance is a vast issue, dipping its tentacles into a range of different places, and debaters should try to be familiar with as many of them as possible. Winning rounds off of topic knowledge is immensely satisfying while losing rounds because a lack of background knowledge is incredibly frustrating. Debaters should be ready to extra deep in their research for this topic, and make sure to take a critical lens with anything they read. Much of the info about NSA surveillance will come from the NSA itself, and while that is unavoidable on a topic like this, debaters should not be afraid to question things simply

because they come from a government authority. Learning to be conscious of where information is coming from is, after all, part of the point of debate. With that, let's dive into the arguments, strategies, and research that will dominate the next month!

**Strategic Considerations**

Despite how it may initially seem, January is actually a pivotal month for the Public Forum debate season. After all, since the payoff of prep is higher for a two-month topic, many teams prepped extra hard for November and December, are likely to rest up a bit for January. So if you're a team that didn't do all that much work in the previous months, or you haven't been as successful as you would have hoped, you now have an excellent chance to turn your season around for the new year. Luckily, January is choc-full of both big national tournaments and smaller local ones, providing a perfect opportunity for teams to prove themselves. Many students are also given time off of school for winter break in December, which provides an extra opportunity for teams to get good research in should they desire. Teams looking to gear up for January should also pay attention to the Blake tournament in December. Even if they are not going to the tournament, I would recommend talking to friends or coaches who might be going, or even seeing if they can watch some of them out rounds on Zoom. Obviously, teams should not simply copy arguments that they hear, but the limited time to prep for Blake forces teams to think outside the box, and makes it an excellent testing ground to see which arguments work and which ones don't; don't be surprised if the arguments run in late Blake out rounds end up being the arguments that dominate the topic.

Another thing that debaters must keep in mind for the upcoming month is how to engage their judges. As anyone taking Zoom classes or holding Zoom meetings can attest, paying attention to anything for a sustained period of time over Zoom is challenging, let alone spending an entire day judging debates. Additionally, through no fault of their own, simple wifi missteps or communication errors mean that judges will inevitably miss things on the flow. When judges feel lost in a round, they are more likely to default to whatever their intuitions about the topic are (especially on a topic such as this, where judges are likely to have strong personal feelings). As such, it's up to debaters to keep their judges listening and engaged! They can do this by making sure their cases are accessible and understandable, something they cant test by reading them aloud to non-debate parents or friends. They should also cut out all technical jargon, and, given the inevitability of judges missing small things, be ready to sacrifice some of the minute details on the flow in favor of bigger picture weighing and analysis. Finally, they should use good old-fashioned rhetorical techniques, speaking clearly and slowly and using volume control to highlight their most important lines. To technical purists, this may seem trivial, but all of these small things can make or break the result in dozens of rounds. More importantly, learning how to effectively communicate with laypeople about an issue is one of the most useful skills debaters will take away from the activity, so don't be afraid to lean into it.

One topic speciation thing for debaters to keep in mind is that, as mentioned above, this is a topic where judges are likely to have strong personal feelings. Obviously, the vast majority of judges try very hard to stay neutral throughout the round, but all judges, even the most experienced technical judges, are not free from their intuitions. Debaters can help overcome that through their weighing. Specifically, instead of dismissing their opponent's arguments and

weighing mechanisms, they should be charitable and sympathetic in their rhetoric to the values that lay beneath their opponent's arguments and try to frame their arguments as better ways of accessing those same values. Remember that trust in the government, privacy, and security are all very personal issues to people, so make sure to validate all of those perspectives in a round, while still defending your side, if of great importance. This is especially true given that the online environment eliminates a lot of the geographic barrier to tournaments, so tournaments are likely to attract teams and judges from a diverse set of places and with a diverse set of perspectives.

As a final strategic consideration before we dive into the arguments, teams should make sure to give a clear conception of what the extent of NSA surveillance looks like as early as possible in the round. Obviously, time in case is precious and teams want to spend as much of it as they can on pure argumentation, but even a little framing of what this surveillance looks like at the outset of the round can go a long way in controlling how judges see and evaluate the round. And if teams don't do this, they run the risk of letting their opponent's set the terms for the debate, and will be forced to debate the round on their opponent's turf, rather than their own. In many rounds, whichever teams end up successfully establishing their conception of the world concerning the resolution is the one that ends up winning, so do not underestimate the value of doing that worldbuilding as early as possible. With all that said, let's look at the core arguments for each side of the topic!

**Affirmative Argumentation**

Affirmative teams will want to paint a picture of an NSA that has gone out of control with power using incredibly invasive methods to spy on its own citizens. Far beyond just collective meta-data, the NSA has a vast number of potentially unnerving tools in their arsenal, including turning on people's computer cameras to spy on them and remotely controlling a SmartTV in someone's home, among many others. A major Wikileaks release several years ago detailed many of these tools that teams can look around in to get concrete examples.[1] Obviously, some judges may be suspicious of WikiLeaks as an organization, so debaters can try to find other sources that discuss these tools, but regardless, listing a couple of examples of the really egregious tools the NSA has at their disposal is an excellent way for pro teams to frame the round, as many judges will intuitively find these practices concerning. In other words, by the end of the pro team's case, any judges that walked into the room thinking the NSA just looks at meta-data should have their eyes opened to the extent of this surveillance. The next question for pro teams is where to go with this information, as unlike many debate topics, it is very difficult to impact these arguments to "x number of people will die" or "the chances of war go up by x percent," so many debaters will be forced to make arguments and impacts they are not used to making. One example of such arguments is a principled argument about the 4th amendment right to privacy. Few debaters have experience making these kinds of principles arguments, which can be very tricky to execute. That's not a reason to stay away from them – the only way to improve is by trying it – but debaters interested in running this rights-based

[1] https://wikileaks.org/ciav7p1/cms/index.html

argument may want to look at some Lincoln Douglas cases online to get a sense of how people structure these arguments (though they will no doubt need to adapt that structure for a lay audience). The upshot of all this is that many PF teams, including very high-level ones, will likely not have experience responding to and weighing against such arguments, since these arguments fall outside the "cost-benefit analysis" framework that PFers are trained to internalize. So for teams willing to put in the work, arguments about the violation of the right to privacy can be very effective. With that, here's some advice on how to think about this argument: 1) Make the impacts specific to the actual violations the NSA are committing, rather than just opine on why privacy is in general important. Privacy is a pretty vaguely defined right, and you want to make sure your justification matches your impact. 2) Think about constraints on the scope of government. People need some sort of sphere in their lives that the government does not control, and privacy creates that space. 3) Look at some legal scholars who talk about why the constitution matters, and why having a government institution brazenly violating its fundamental protections produces a broader threat to democracy. As mentioned, these are challenging topics, but thinking about them and researching them will make you a better debater, regardless of whether or not they make it into your final case.

A second argument that affirmative teams can make regards the potential for this technology to, in the wrong hands, do immense amounts of harm. This argument holds that invasive surveillance by the government should always be opposed, as even if it is not being used to suppress free speech or target disruptive political movements right now, it has in the past and could be used to do so in the future, especially with both the increase in capabilities and the increase in instability. Debaters can look to radical minority movements of the 1960s

and 1970s, which were subject to mass surveillance by various government agencies "simply because their views differed from the government's," as the ACLU puts it. [2] Indeed, some leaked evidence in recent years reveals a similar practice today of surveilling Muslim communities, and that the government has been monitoring and tracking some minority civil rights leaders.[3] If minority groups looked to form their own political parties or organized in more formal ways, it is not unfathomable that the NSA might unleash some very suppressive tactics against them. This argument has the potential to be effective since it gives a more concrete picture of what some of the negative impacts/potential dangers of this surveillance are, as opposed to the principled rights violations mentioned above. Often, judges might be a bit skeptical of these arguments that can sound almost conspiratorial at times, but given the democratic backsliding of the past few years, and the aftermath of the recent elections, judges will likely be even more receptive to this argument than ever. So long as teams have real examples of US surveillance ages conducting this kind of suppression and profiling in the past, as well as examples of how they could use them in the future, this is an extremely viable argument with large weighable impacts.

Something else that pro teams must consider when crafting their arguments is the actual efficacy of these programs, and to what extent they actually work. Obviously, much of the information if classified, investigations into the information that has been released shows that these programs really do not even do that much in preventing terrorism. In response to

[2] https://www.aclu.org/blog/national-security/secrecy/whats-government-doing-targeting-civil-rights-leaders
[3] Ibid

public pressure, the NSA has repeatedly claimed that their surveillance efforts have thwarted "more than 50 terror attacks," but they have only discussed four of them publicly, and in only one case, about a San Diego taxi driver who sent $8,500 to the Somali terrorist group al-Shabab, did surveillance play a key role (and even the details of that case are vague).[4] Lots of good journalists have done deep dives into the NSA's claims, and many have found scant evidence of these programs actually preventing terrorist activity.[5] While these claims may seem purely defensive at first, when framed correctly they can be a key part of an affirmative case. For pro teams that want to run arguments about privacy rights but are hesitant go purely on principle, they can use this to create a kind of cost-benefit analysis, saying that if there is going to be some infringement on constitutional rights, the threshold for benefit must be incredibly high, and the NSA programs simply do not come close to reaching that threshold, without evening mentioning the billions of dollars spent on these ineffective programs. In fact, there's even some evidence to suggest that programs are actively harmful when it comes to security. The logic, as explained by an NSA whistleblower, is that the agency is collecting such an incredibly large amount of bulk data that the agency literally cannot process all of it, and when threats come up they are "left trying to find a needle in a haystack".[6] He even cites the Boston Bombing as an example of a terrorist attack the NSA should have been able to stop but failed to do so given their ineffective practices. Given the number of high ranking officials that swear by the need for this surveillance, pro teams looking to run certainly face an uphill battle. The

[4] https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much
[5] https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/
[6] https://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/

upside, however, is that this argument would be incredibly powerful and almost certainly round winning for the pro since the vast majority of con teams will likely focus on security. For pro teams willing to get into the weeds and understand the intricacies of the NSA data collection services, this argument certainly has great potential. As such, despite a debate about the NSA appearing to be a rather classic PF topic, many of the arguments hereby discussed will allow debaters to develop new ways of impacting, something I would encourage them to lean into as much as possible. With that, let's look at the key negative arguments!

**Negative Argumentation**

Much like the affirmative side of the cyber attacks resolution from last November, the spiritual predecessor to this month's resolution, negative teams will want to focus on core concepts of security, deterrence, and safety. The NSA, after all, has indeed said that these tools have been used in the successful thwarting of over 50 terrorist events, and there is a laundry list of top security officials who swear by these programs, who neg teams will no doubt want to be quoting in their rounds.[7] The central problem for con teams, of course, is that the information around these events is still largely classified, leading many to doubt its veracity. Nevertheless, clever con teams can still weigh this information to be incredibly powerful. For example, con teams could acknowledge that perhaps the NSA is exaggerating a bit about the total number of incidence, but even if half of those examples are legitimate, or even if only three of the 50, that is still an incredible amount of harm prevented by these surveillance

[7] https://www.washingtonpost.com/world/national-security/officials-surveillance-programs-foiled-more-than-50-terrorist-plots/2013/06/18/d657cb56-d83e-11e2-9df4-895344c13c30_story.html

programs, and a significant number of US lives saved. If the con team can convince the judge that even a few terrorist incidents are prevented by this surveillance, they have an excellent chance to win the round. Further, con teams should harness the seeming public indifference to these programs. Few events have garnered more attention than the Snowden leaks, and while Snowden himself has seen modest gains in popularity, it is not as though thousands of people are outside the pentagon demanding the program's end. Many people seem willing to part with some degree of privacy for their safety, uncomfortable as the decision may be. In addition to pointing towards attacks that have been thwarted, con teams should also make arguments about deterrence, arguing that these programs do massive work in preventing people from trying to plan these attacks in the first place, which cannot be empirically proven but is nevertheless very plausible – con teams will again need to rely on quotations from top defense officials. Debaters often find winning arguments about catastrophic events to be an uphill battle, as people tend to underestimate the chances of bad things happening, so judges are often primed to be more skeptical of those kinds of arguments. Unconventional as it may seem, con teams may even want to be explicit about it in rounds, mentioning that the judge may intuitively doubt the possibility of these catastrophic events happening, but that these threats are very real, and the work done by the NSA is necessary for preventing them.

Another, potentially more bold strategy that negative teams can use is to try and ditch some of the conventional security and deterrence arguments and try to beat the pro on its own terms. How? Well, neg teams can start from the premise that these surveillance programs certainly create the perception of security, and give off the image of a government doing everything it can to protect its citizens. Thus, if the NSA announced that it was ending these

programs, some significant portion of the population would likely feel less safe, even if the programs are not, in reality, that effective. Why is this a problem? Because terrorist attacks are, to some degree, an inevitability, and unfortunately, at some point in the future, another will happen. In fact, even if the programs themselves are ineffective, it is very plausible that their termination could be seen as a sign of weakness from terrorist groups around the world and embolden them to try and plan more attacks. All it would take is one terrorist attack, or even the threat of one, in the months or years after the termination of these programs to validate the entire security state and create a political landscape likely to earn defense officials a blank check to pursue any surveillance programs in the name of security (similar to the post 9/11 environment). This is potentially incredibly dangerous, as con teams can paint programs now as relatively benign, but that a full validation of the security system would give them the authority to ramp up all of the suppression and profiling such as was seen during the Cold War, only with far more capability from the defense agencies themselves. As seems to be the story with several arguments on this topic, the link chain may be a bit tenuous, but the upside is gigantic, giving the con full access to the impacts likely run by the pro side.

**Conclusion**

As should come as no surprise for a topic dealing with classified government information, research, and argument writing on this topic may prove tricky. Rather than a deterrent to working, however, I hope that you'll see this as an invitation to think outside the box, get deep into the weeds of research, and push yourself to experiment, all of which will be in service to improving your abilities as a debater and a thinker more broadly. As has been

proved in the past, these kinds of topics reward teams willing to put in the world to untangle them. Good Luck!

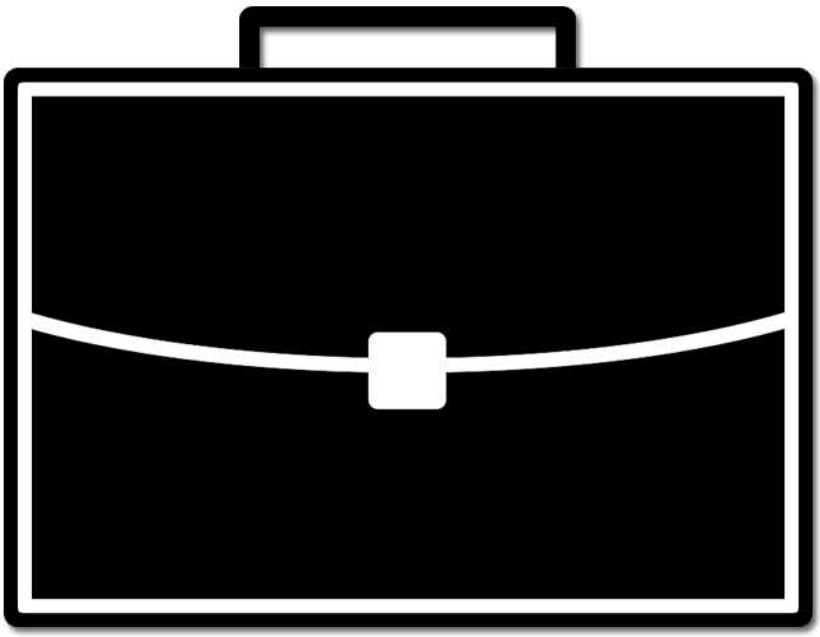
**About Tucker Wilke**

Tucker is from Westchester, New York, where he attended the Hackley School. He is now attending Brown University, where he debates for the Brown Debating Union and studies English and Economics. Over the course of his career, Tucker amassed 8 bids to the Tournament of Champions. In addition, he reached the Quarterfinals at Bronx, Glenbrooks, UK, Ridge and Princeton, Semifinals at Penn and Columbia, and championed the Scarsdale Invitational. He was ranked as high as 7th in the country in his senior year. As a coach for Hackley, his students have reached semifinals at Blake and Quarters at Penn.

# Champion Briefs

## January 2021

## Public Forum Brief



# General Information

# General Information

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

**Foreword:** We, at Champion Briefs, feel that having deep knowledge about a topic is just as valuable as formulating the right arguments. Having general background knowledge about the topic area helps debaters form more coherent arguments from their breadth of knowledge. As such, we have compiled general information on the key concepts and general areas that we feel will best suit you for in- and out-of-round use. Any strong strategy or argument must be built from a strong foundation of information; we hope that you will utilize this section to help build that foundation.

**What does the NSA do**

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 severalreports 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 passage 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.


THE NSA: EYES AND EARS ON THE WORLD
In 2013, the United States spent more than US$52 billion on 16 different spy agencies, about double what it spent in 2001. Nearly half the money went to the NSA and CIA.
CENTRAL INTELLIGENCE AGENCY
$14.7 BILLION
NATIONAL SECURITY AGENCY
$10.8 BILLION
NATIONAL RECONNAISSANCE OFFICE
$10.3 BILLION
OTHERS
$16.8 BILLION
1,700,000,000
THE NUMBER OF PHONE CALLS, EMAILS AND OTHER COMMUNICATIONS THE NSA INTERCEPTED EVERY DAY IN 2010
700,000
THE NUMBER OF "VOICE OVER IP" (VOIP) FILES THE NSA STORED EACH DAY IN 2013, INCLUDING INTERNET PHONE CALLS AND SKYPE SESSIONS
The U.S. intelligence budget exceeds the gross domestic product of more than 100 countries
By 2013, the NSA directly employed roughly 40,000 – and many more private contractors – compared to an estimated 14,000 employed by the CIA.
telesur
Sources: Edward Snowden, Washington Post, The Intercept, World Bank

**The now-infamous Snowden whistleblowing affair**

Seven years after former National Security Agency contractor Edward Snowden blew the whistle on the mass surveillance of Americans' telephone records, an appeals court has found the program was unlawful - and that the U.S. intelligence leaders who publicly defended it were not telling the truth.

In a ruling handed down on Wednesday, the U.S. Court of Appeals for the Ninth Circuit said the warrantless telephone dragnet that secretly collected millions of Americans' telephone records violated the Foreign Intelligence Surveillance Act and may well have been unconstitutional.

Snowden, who fled to Russia in the aftermath of the 2013 disclosures and still faces U.S. espionage charges, said on Twitter that the ruling was a vindication of his decision to go public with evidence of the National Security Agency's domestic eavesdropping operation.

"I never imagined that I would live to see our courts condemn the NSA's activities as unlawful and in the same ruling credit me for exposing them," Snowden said in a message posted to Twitter.

Evidence that the NSA was secretly building a vast database of U.S. telephone records - the who, the how, the when, and the where of millions of mobile calls - was the first and arguably the most explosive of the Snowden revelations published by the Guardian newspaper in 2013.

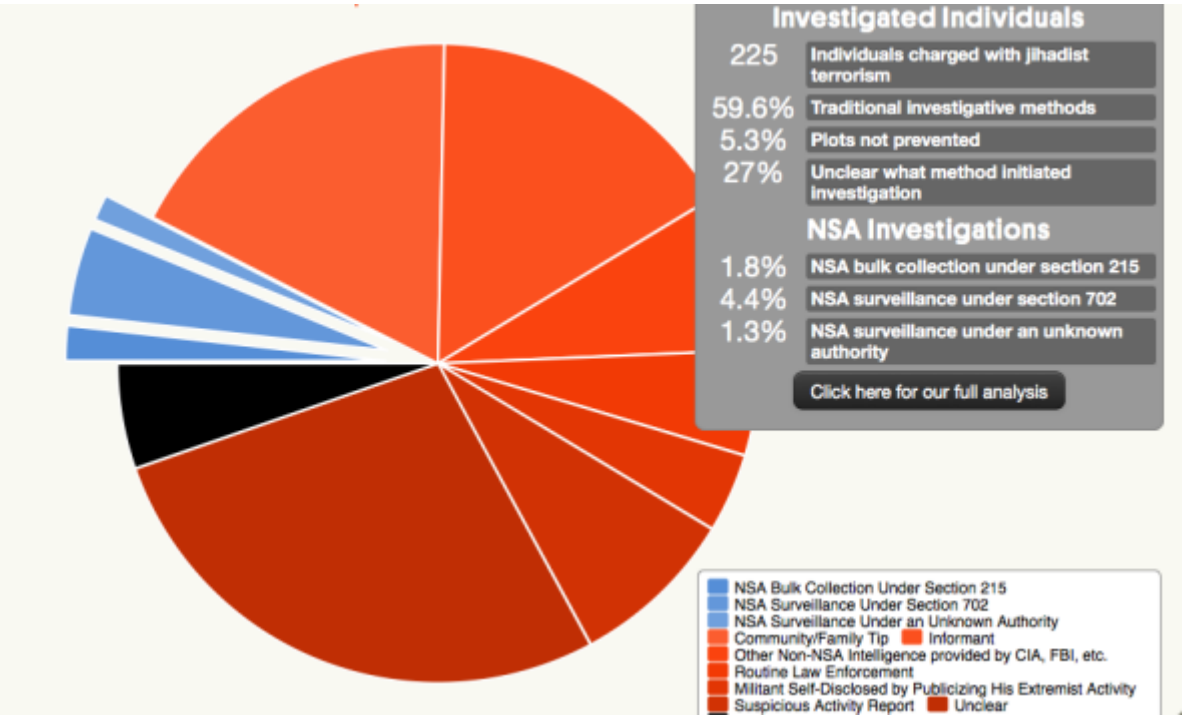

BREACHING THE NSA
How Edward Snowden did it and is your enterprise next?
SECURITY CLEARANCE: DELTA 7
Official Memorandum
10/9/2013
According to the NSA, Edward Snowden "fabricated keys" to obtain and exfiltrate top secret information. Here is how he did it.
Venafi invites the NSA or Edward Snowden to provide more details so enterprises can better secure their most sensitive data and intellectual property.
TOP SECRET
BASED ON A CLOSE ANALYSIS OF PUBLIC INFORMATION, YEARS OF CUSTOMER EXPERIENCE AND KILL-CHAIN ANALYSIS, EDWARD SNOWDEN'S ATTACKS CAN BE SUMMARIZED INTO THE FOLLOWING 3 KEY STEPS.
Military experts, and now IT Security Teams, are using Kill Chain Analysis to establish how an adversary can attack or has attacked an organization
THE KILL CHAIN
1 Research Target
2 Initial Intrusion
3 Exfiltrate Data
Just like any government contractor, Edward Snowden was issued a CAC smart card with digital certificates and keys. As an administrator, he was also issued SSH keys for systems he was required to administer. This allowed Snowden to have valid access to some data and understand what else was out there.
CAC SMARTCARD
SSH KEYS
UNAUTHORIZED
NEW & TRUSTED
SELF-SIGNED CERTIFICATES
As described in testimony by General Keith Alexander, Edward Snowden fabricated digital keys because of the NSA's failure to detect anomalies. He used his authorized access to create new keys, obtain unauthorized keys, and create trust for new keys.
To get data out unnoticed, Edward Snowden needed to transfer data between systems. The transfer needed to go undetected, so he encrypted his data transfer sessions using self-signed certificates.
DATA
WHAT ATTACKERS ARE LOOKING FOR
Wide Reach
17K
Keys and certificates per enterprise. 1
Low Visibility
51%
Over HALF of all enterprises don't know where keys and certificates are or how to use them. 1
Slow Response
60%
Have more than a 24 hour response time. 2
Trusted Status
10X
Increase in malware digitally signed with a compromised or stolen digital certificate. 3
You Are a Target AND CANNOT HIDE
100% OF ALL ENTERPRISES
Have had attacks on keys and certificates within the last two years. 1
& IF THE NSA WAS ATTACKED
Being the most secure organization in the world then YOU'RE NEXT
Basically "EVERY ENTERPRISE IS A SITTING DUCK."
– Forrester Consulting
LEARN HOW TO PROTECT YOUR ORGANIZATION
VENAFI
www.venafi.com/EdwardSnowden

**Do NSA surveillance efforts stop terrorism**

On June 5, 2013, the Guardian broke the first story in what would become a flood of revelations regarding the extent and nature of the NSA's surveillance programs. Facing an uproar over the threat such programs posed to privacy, the Obama administration scrambled to defend them as legal and essential to U.S. national security and counterterrorism. Two weeks after the first leaks by former NSA contractor Edward Snowden were published, President Obama defended the NSA surveillance programs during a visit to Berlin, saying: "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved." Gen. Keith Alexander, the director of the NSA, testified before Congress that: "the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world." Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that "54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives."

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of

the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.



**Do Americans support NSA surveillance?**

Fourteen years after the Sept. 11 terrorist attacks, and two years after Edward Snowden's revelations about extensive U.S. government surveillance of phone and internet data, Americans continue to have mixed – and sometimes conflicting – views about government surveillance programs.

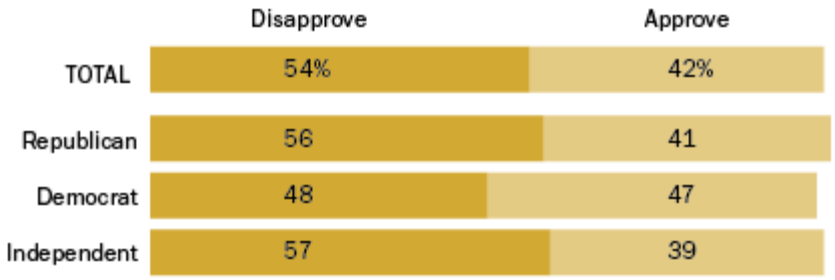
On the one hand, a majority of Americans oppose the government collecting bulk data on its citizens, and two-thirds believe there aren't adequate limits on what types of data can be collected. But at the same time, Americans generally support monitoring the communications activity of suspected terrorists. Here's a rundown of what we know about attitudes toward U.S. government surveillance, at home and abroad:

**A majority of Americans (54%) disapprove of the U.S. government's collection of telephone and internet data as part of anti-terrorism efforts**, while 42% approve of the program. Democrats are divided on the program, while Republicans and independents are more likely to disapprove than approve, according to a survey we conducted in spring 2014.

**More broadly, most Americans don't see a need to sacrifice civil liberties to be safe from terrorism**: In spring 2014, 74% said they should not give up privacy and freedom for the sake of safety, while just 22% said the opposite. This view had hardened since December 2004, when 60% said they should not have to give up more privacy and freedom to be safe from terrorism.

## Americans' Views of NSA Surveillance

*% who ___ of government's collection of phone and internet data*

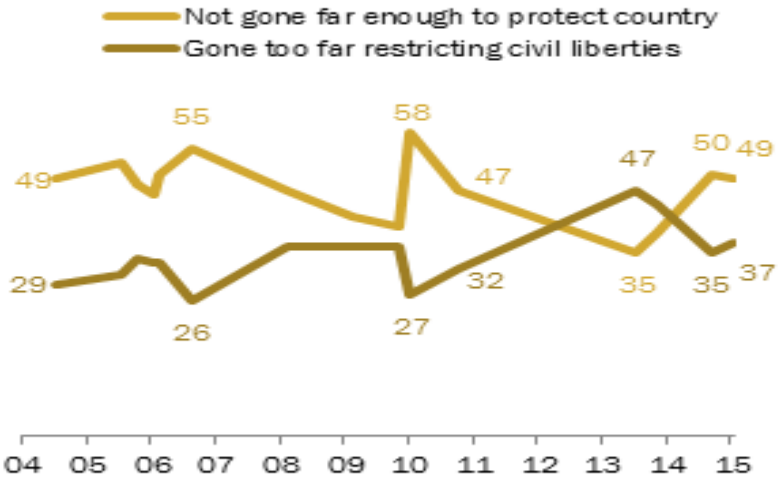



Note: Don't know/refused responses not shown.
Source: Spring 2014 Political Typology Survey

PEW RESEARCH CENTER

## More Continue To Be Concerned With Country's Protection Over Civil Liberties

*Bigger concern about gov't anti-terrorism policies? (%)*




Survey conducted Jan. 7-11, 2015.
Volunteered responses of Both/Neither/Don't know not shown.

PEW RESEARCH CENTER

**Works Cited**

Bocek, Kevin. “Infographic: How Snowden Breached the NSA” Venafi. 11/12/13. https://www.venafi.com/blog/infographic-how-snowden-breached-nsa

Cahill, Bailey. “Do NSA’s bulk surveillance programs stop terrorists?” New America. 1/13/14. https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

“FAQ: What you need to know about the NSA’s surveillance programs.” ProPublica. 8/5/13. https://www.propublica.org/article/nsa-data-collection-faq

Gao, George. “What Americans think about NSA surveillance, national security, and privacy.” Pew Research Center. 5/29/15. https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

Satter, Rachel. “U.S. court: Mass surveillance program exposed by Snowden was illegal.” Reuters. 9/2/20. https://www.reuters.com/article/us-usa-nsa-spying/u-s-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK

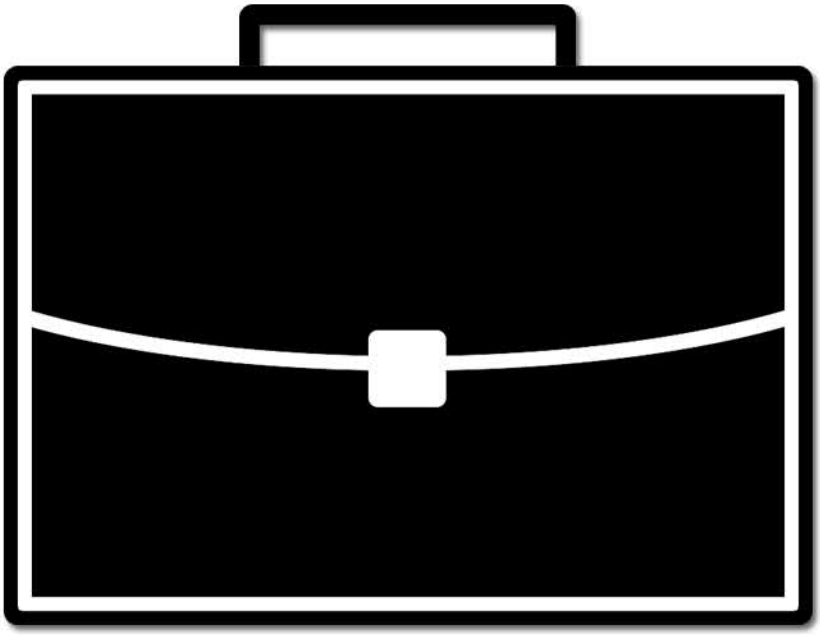
Sterman, David. “Infographic: How the government exaggerated the successes of NSA surveillance.” Slate. 1/16/14. http://www.slate.com/blogs/future_tense/2014/01/16/nsa_surveillance_how_the_government_exaggerated_the_way_its_programs_stopped.html

“The US National Security Agency: Eyes and Ears on the World.” TeleSur. No date. https://www.telesurenglish.net/news/Infographic-The-NSA---Eyes-and-Ears-on-the-World-20151118-0038.html

# Champion Briefs

## January 2021

## Public Forum Brief



# Pro Arguments

## PRO: The NSA surveillance program amounts to authoritarianism

**Argument:** Government surveillance of citizens and lawful permanent residents is an authoritarian abuse of power.

**Warrant:** Authoritarian abuse "slippery slope" is a real concern.

Townsend, Mark, and Anushka Asthana. "Put young children on DNA list, urge police." The Observer, March 16, 2008: 1. https://www.theguardian.com/society/2008/mar/16/youthjustice.children

"In addition, **allowing surreptitious surveillance of one form**, even limited in scope and for a particular contingency, **encourages government to expand such surveillance programs in the future.** It is our view that **the danger of a "slippery slope" scenario cannot be dismissed as paranoia** - as a prominent example, **the collection of biometric has expanded immensely in the past several years. Many schools in the UK collect fingerprints of children as young as six without parental consent** (Doward 2006), **and fingerprinting in American schools has been widespread since the mid-eighties** (NYT National Desk 1983). Now, **the discussion has shifted towards DNA collectio**; **British police are now pushing for the DNA collection of children who "exhibit behavior indicating they may become criminals in later life**"

**Warrant**: Government surveillance doesn't just include phone calls or digital data. New York City mayor Rudy Giuliani has even encouraged the collection of data of newborns.

Lambert, Bruce. "Giuliani Backs DNA Testing Of

Newborns for Identification." New York Times. December 17, 1998. https://www.nytimes.com/1998/12/17/nyregion/giuliani-backs-dna-testing-of-newborns-for-identification.html

"**When asked whether all children should have DNA tests at birth, the Mayor said**: ''I don't know that that's the proposal, but I **would have no problem with that, or fingerprinting all children. We go through a massive effort to try to fingerprint large numbers of children**'' now, he said, **''so in case they are lost they can be found again or in case if they are kidnapped they can be found again. There is absolutely no reason why people should be afraid of being identified.''**

**Warrant**: Even surveillance through our ID cards is potentially a huge risk for authoritarian abuses.

eGov Monitor Weekly. "Government ID Card claims deflated." The Register. March 15, 2006/ Web. http://www.theregister.co.uk/2006/03/15/biometric_data_open_to_abuse

"**Biometric data employed for identification purposes could be misused and lead to "function creep",** the European Data Protection Supervisor has warned**.** In a comment this week, **the EDPS**, **who monitors the use of public data, said the ease with which biometric information, such as fingerprints, could be shared with other databases across the EU would leave it open to abuse.** The EDPS **Peter Hustinx said the accuracy of biometric data in uniquely identifying a person is "overestimated", and could in fact "facilitate the unwarranted interconnection of databases".**

**Warrant:** Abuse is and over reach has already occurred at the Federal Levels.

Aaronson, Trevor. "A DECLASSIFIED COURT RULING SHOWS HOW THE FBI ABUSED NSA MASS SURVEILLANCE DATA: By abusing the NSA's mass surveillance data, the FBI may have violated the rights of millions of Americans, a federal judge ruled.". 10 Oct 2019. https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/

**"THE FOREIGN INTELLIGENCE Surveillance Court found that the FBI may have violated the rights of potentially millions of Americans — including its own agents and informants — by improperly searching through information obtained by the National Security Agency's mass surveillance program. "These opinions reveal devastating problems with the FBI's backdoor searches, which often resembled fishing expeditions through Americans' personal emails and online messages**," said Patrick Toomey, a staff attorney for the American Civil Liberties Union's National Security Project**. "**But the court did not go nearly far enough to fix those abuses. **The Constitution requires FBI agents to get a warrant before they go combing through our sensitive communications."**

**Warrant:** Even after the Freedom Act was passed, the Federal Government surveillance has continued surveillance of citizens illegally.

**"**US: New Evidence Suggests Monitoring of Americans: **Documents Point to Warrantless Surveillance". ** October 25, 2017 https://www.hrw.org/news/2017/10/25/us-new-evidence-suggests-monitoring-americans

**"Newly released documents reveal a US Defense Department policy that appears to authorize warrantless monitoring of US citizens and green-card holders whom the executive branch regards as "homegrown violent extremists,"** Human Rights Watch

said today. Separately**, the documents also reinforce concerns that the government may be gathering very large amounts of data about US citizens and others without warrants.** Both issues relate to a longstanding executive order that is shrouded in secrecy and should be a focus of congressional inquiry.**"**

**Warrant:** The current pandemic has highlighted ongoing and egregious abuses of government surveillance.

Gebrekidan, Selam. "For Autocrats, and Others, Coronavirus Is a Chance to Grab Even More Power." New York Times. 14 April 2020. https://www.nytimes.com/2020/03/30/world/europe/coronavirus-governments-power.html?auth=login-google

**"We could have a parallel epidemic of authoritarian and repressive measures following close if not on the heels of a health epidemic,"** said Fionnuala Ni Aolain, the United Nations Special Rapporteur on counterterrorism and human rights**. As the new laws broaden state surveillance, allow governments to detain people indefinitely and infringe on freedoms of assembly and expression, they could also shape civic life, politics and economies for decades to come."**

**Impact:** Continued Government Surveillance of citizens and lawful permanent residents is a danger to democracy.

**Warrant:** Real solutions for digital era necessary to democracy survival.

Adrian Shahbaz. "Fake news, data collection, and the challenge to democracy." Freedom House.org. 2020. https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy

**"If democracy is to survive the digital age, technology companies, governments, and civil society must work together to find real solutions to the problems of social media manipulation and abusive data collection.** Multilateral and cross-sectoral coordination is required to promote digital literacy, identify malicious actors, and deny them the tools to fraudulently amplify their voices. **When it comes to protecting data, users must be granted the power to ward off undue intrusions into their personal lives by both the government and corporations. Global internet freedom can and should be the antidote to digital authoritarianism. The health of the world's democracies depends on it."**

**Warrant:** Government Surveillance abuses are clear and violate human rights.

St. Vincent, Sarah. "NSA's Domestic Spying Program Needs to End---Permanently." Progressive.org. 18 Mar 2019. https://progressive.org/op-eds/nsa-domestic-spying-must-end-st.vincent-190318/

"The Section 215 phone records program, it seems, was from the beginning a large-scale fishing expedition. **Letting government stockpile sensitive information about individuals, 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 insufficient to end the human rights violations this domestic spying entailed.** If this program is indeed dormant, the government should let it stay that way until the law underpinning it expires**.** 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."**

**Warrant:** Public trust in the government is at an all time low.

"Americans' Views of Government: Low Trust, but Some Positive Performance Ratings" Pew Research Center. 14 Sept 2020. https://www.pewresearch.org/politics/2020/09/14/americans-views-of-government-low-trust-but-some-positive-performance-ratings/

**"For years, public trust in the federal government has hovered at near-record lows. That remains the case today, as the United States struggles with a pandemic and economic recession. Just 20% of U.S. adults say they trust the government in Washington to "do the right thing" just about always or most of the time."**

**Warrant:** Ending Government surveillance will go a long way to restore the balance of power in government and restore the public trust.

WU, Edieth Y. "DOMESTIC SPYING AND WHY AMERICA SHOULD AVOID THE SLIPPERY SLOPE". Review of Law and Social Justice. Vol 16.1. https://gould.usc.edu/students/journals/rlsj/issues/assets/docs/Wu_Final.pdf

**"The war on terror has led the American people into a quagmire—** whether to maintain confidence in the president or to question whether he "is crafting an imperial presidency unfettered by constitutional checks and balances." **On the one hand, most Americans are willing to sacrifice certain civil liberties for national security.** In the wake of September 11, **Americans became increasingly tolerant of government intrusion into private affairs; particularly with respect to state action targeting potential security threats. On the other hand, Americans remain wary of warrantless domestic surveillance because of the threat it poses to civil liberties.** As we move further from the tragedy of September 11, there is a mounting sentiment that the president has overstepped his authority. **Many Americans "have concluded that**

**defeating Islamic fundamentalism cannot be accomplished by abandoning basic American values." And members of Congress are taking a stand against warrantless surveillance by asking for an investigation into Bush's decision to spy on U.S. citizens without court orders. "**

**Analysis:** While the United States has attempted to curb the unlimited and warrantless surveillance of its citizens and lawful permanent residents, the fact remains that there are clear abuses already and continuing to occur. Public trust in our government is at an all time low and the continued abuse of powers does not help. The slippery slope is real, and we do not want to end up with fully authoritarian regime over our citizens, even if it is in the name of public good

## PRO: The NSA surveillance program can be hacked

**Argument:** Government surveillance of citizens and lawful permanent residents is at a high risk of being hacked.

**Warrant:** The Government collects and stores massive amounts of phone call data every year.

Savage, Charlie. "N.S.A. Triples Collection of Data From U.S. Phone Companies." New York Times. 4 May 2018. https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

WASHINGTON — **The National Security Agency vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year — more than three times what it collected in 2016,** a new report revealed on Friday. **Still, the large and growing volume of data gathered shows that the N.S.A. continues to collect significant amounts of information about Americans' phone and text messages after changes made by Congress in a 2015 law, the USA Freedom Act, which overhauled how the N.S.A. can gain access to domestic telecom data.**

**Warrant:** The government currently is storing personal information of its citizens.

ProPublica. "FAQ: What You Need to Know About the NSA's Surveillance Programs" Propublica.org. 5 Aug 2013. https://www.propublica.org/article/nsa-data-collection-faq

**"The collected information covers "nearly everything a user does on the Internet,"** according to a presentation on the XKEYSCORE system. **The slides specifically mention**

**emails, Facebook chats, websites visited, Google Maps searches, transmitted files, photographs, and documents of different kinds. It's also possible to search for people based on where they are connecting from, the language they use, or their use of privacy technologies such as VPNs and encryption, according to the slides.** This is a massive amount of data. **The full contents of intercepted Internet traffic can only be stored for up to a few days, depending on the collection site, while the associated "metadata" (who communicated with whom online) is stored up to 30 days. Telephone metadata is smaller and is stored for five years. NSA analysts can move specific data to more permanent databases when they become relevant to an investigation."**

**Warrant:** The government is collecting and storing a myriad of types of personal information.

Bump, Phillip. "How Big Is the NSA Police State, Really?." The Atlantic. 11 June 2013. https://www.theatlantic.com/national/archive/2013/06/nsa-datacenters-size-analysis/314364/

Early last month, even while he was finalizing his discussions with Edward Snowden, ***The Guardian*'s Glenn Greenwald reported on a conversation between Tim Clemente, a former FBI agent,** and CNN host Carol Costello. **In the interview about the Boston Marathon investigation**, as seen at right, **Clemente makes the claim that "all digital communications are — there's a way to look at digital communications in the past." Costello refers to a previous appearance in which Clemente claimed the government could access phone calls, even "exactly what was said in that conversation. "This is an important claim for two reasons. The first is that Clemente, who also served on the FBI's Joint Terrorism Task Force, suggests a massive breadth of information collection.** The second is that he doesn't say who is actually collecting the data, which we'll come back to. **Clemente indicates that entire phone calls are being recorded and stored,**

**which is a far stronger claim than that Verizon is sharing metadata with the government.** So **if Clemente is right, and the government has access to "all digital communications" — videos, calls, audio recordings, emails, photos** — that's taking up a lot of physical space somewhere. Which brings us to the second reason Clemente's claim is important, and to our second question.

**Warrant:** The government has been hacked several times by even just one small group.

Goodin, Dan. “Database hacking spree on US Army, NASA, and others costs gov’t millions.” ARS Technica. 28 Oct 2013. https://arstechnica.com/information-technology/2013/10/database-hacking-spree-on-us-army-nasa-and-others-cost-gov-millions/

"**Using the stolen administrator's password, the co-conspirators obtained data belonging to the Army Corps, including information regarding the planned demolition and disposal of certain military facilities,"** prosecutors wrote in the indictment. "The attack was launched from a computer server located in or around Romania, which was leased by defendant Love.” **The indictment went on to detail at least nine additional hacks on government and military networks. Other government agencies Love allegedly breached included the Department of Energy, the Department of Health and Human Services, the US Sentencing Commission, and the Regional Computer Forensics Laboratory, according to the criminal complaint filed in Virginia.** To cover his tracks, Love allegedly used the Tor privacy service to conceal his IP address and used a series of pseudonyms**. He and his colleagues allegedly used pseudonyms on social media sites to publicize the breaches.** Despite the effort to remain anonymous, Love allegedly originated at least one attack from an Internet domain that was registered using a PayPal account associated with his lauri.love@gmail.com account.

**Warrant:** The government has failed to ensure that collected information is protected from hackers.

Davis, Julie. "Hacking of Government Computers Exposed 21.5 Million People." New York Times. 9 July 2015. https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

**The Obama administration** on Thursday **revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including Social Security numbers and some fingerprints. Every person given a government background check for the last 15 years was probably affected,** the Office of Personnel Management said in announcing the results of a forensic investigation of the episode, whose existence was known but not its sweeping toll. **The agency said hackers stole "sensitive information," including addresses, health and financial history, and other private details, from 19.7 million people who had been subjected to a government background check, as well as 1.8 million others, including their spouses and friends. The theft was separate from, but related to, a breach revealed last month that compromised the personnel data of 4.2 million federal employees,** officials said.

**Warrant: US** Citizens deserve their right to have their information protected.

Meehan, Michael. "The Need for Unified Data Protection in the U.S." Nextgov. 21 Sept 2020. https://www.nextgov.com/ideas/2020/09/need-unified-data-protection-us/168643/

**"Having a single federal data privacy law would allow companies to focus their efforts on compliance and protection of individuals' rights, and not on a complex and shifting**

**set of requirements that would differ depending on the jurisdiction(s) at play for each individual or piece of data.** The more complex the tapestry of laws that apply to personal data, the harder compliance will be. **Europe learned this lesson and has implemented General Data Protection Regulation as an European Union-wide privacy law. We should do the same."**

**Impact:** Citizens are at risk of their personal information being attained by hacking into the government databases.

**Warrant:** Citizens are at harmed by criminal data breaches.

Pallone, Frank; Schakowsky, Jan; DeGette, Diana. "Range of Consumer Risks Highlights Limitations of Identity Theft Services Report to Congressional Requesters United States." Government Accountability Office. https://www.gao.gov/assets/700/697985.pdf

**Individuals' sensitive personal information can be lost, stolen, or given away. Once exposed, individuals' information can be misused to commit identity theft, fraud, or inflict other types of harm**. Identity theft occurs when individuals' information is used without authorization in an attempt to commit fraud or other crimes. **In 2016,** according to the Bureau of Justice Statistics, **an estimated 26 million people—10 percent of U.S. residents aged 16 or older—reported that they had been victims of identity theft in the previous year**. **One potential source of identity theft is a data breach at an organization that maintains large amounts of sensitive personal information. The harms caused by exposure of personal information or identity theft can extend beyond tangible financial loss, including the following: Lost time. Victims of identity theft or fraud may spend significant amounts of time working to restore their identities. In 2016,** according to the Bureau of Justice Statistics survey of identity

victims**, most victims resolved issues in 1 day or less but about 1 percent of victims spent 6 months or more resolving their identity theft issues.** Emotional distress and reputational harm. **Exposed information also can cause emotional distress, a loss of privacy, or reputational injury. In 2016,** according to the Bureau of Justice Statistics, **about 10 percent of those who experienced identity theft reported suffering severe emotional distress**. Harm from state-based actors**. State-sponsored espionage can cause harm to individuals when nations use cyber tools as part of information-gathering, espionage, or other nefarious activities.**

**Warrant:** Lives are ruined from hacked information.

Johansen, Alison. "4 Lasting Effects of Identity Theft." Lifelock. 13 Mar 2018. https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html

"**Identity theft's negative impacts often involve finances, but there can be other consequences, as well, including an emotional toll.** For example, if a thief commits a crime and provides your name to police—something known as criminal identity theft—and authorities arrest you as a result, well, you can imagine the resulting stress, as well as disruption to your life until you're able to resolve the situation. **While you clean up the messy trail of ID theft, the emotional stress can disrupt your sleeping and eating, and lead to depression and isolation. And what about the emotional stress of receiving calls from debt collectors?** When someone else racks up debt in your name, it can be challenging to prove the debt isn't yours. **Plus, you need to take steps so the businesses and collections agencies stop reporting the debt as yours. In its 2016 ITRC survey, 23 percent of ID theft victims surveyed feared for their physical safety, 39 percent experienced an inability to focus, 29 percent reported new physical illnesses such as body pain, sweating, and heart and stomach issues, 41 percent had sleep issues, and 10 percent couldn't go to work due to resulting physical issues.**

**Warrant:** Millions of dollars are spent on victims after government hacked accounts occur.

Koyame-Marsh, Rita & Marsh, John. (2014). Data Breaches and Identity Theft: Costs and Responses Rita O. Koyame-Marsh and John L. Marsh. IOSR Journal of Economics and Finance (IOSR-JEF). 5. 36-45. 10.6084/m9.figshare.1284635.

"**Identity theft is also becoming increasingly costly to American people. It was estimated,** on the basis of a 2006 FTC's Identity Theft Survey, **that the total amount stolen in 2005 by identity thieves from victims was about $15.6 billion** with 8.3 million of U.S. adults becoming victims of some types of identity theft the same year (Synovate, 2007). **The amount stolen rose to about $18 billion in 2013** with 13.1million of U.S. adult becoming victims of identity fraud in that same year (Javelin, 2014). "

**Analysis:** Government surveillance of citizens data is not secure. The US government has shown that it cannot adequately protect its systems from being hacked and with the mass amounts of various types of personal sensitive data that it collects, they have an obligation to protect their citizens. The only way to ensure that this data cannot be hacked to harm individuals' lives is to end the surveillance of its citizens and lawful permanent residents. This will not only protect individuals, but save the government money in recovery after the fact, while living up to the human rights we value.

# PRO: The NSA surveillance program should be ended by the Freedom Act

**Argument:** Ending Government surveillance of citizens and lawful permanent residents is necessary to fulfill the Freedom Act.

**Warrant:** The United States Government already passed the Freedom Act, limiting the Government in its surveillance practices.

Liu, Jodi. "So What Does the USA Freedom Act Do Anyway? ". Law Fare. 3 June 2015. https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway

"Under Title I, **the bill bans the current system of bulk collection under Section 215.** Instead, **it requires that the government base any applications** for call detail records **on a "specific selection term"—**a term **that "specifically identifies a person, account, address, or personal device" in a way that "limit[s], to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things."**

**Warrant:** Government surveillance should already be ended with the Freedom Act, however, it is still ongoing through loopholes.

Franklin, Sharon. "Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records." Just Security.org. 28 Mar 2019. https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/

"**The USA Freedom Act was supposed to end bulk surveillance of Americans. It amended Section 215 to replace the highly controversial bulk telephone meta data collection program with a much narrower authority for collecting "call detail records"** (CDRs). CDRs consist of metadata that show "session-identifying information" for which phone numbers or other identity numbers are contacting with other numbers and when. **The New Section 215 CDR program authorizes the collection of the same time of metadata as the former bulk collection program, but the program is narrower than the previous one in several respects. Most significantly, the government can no longer collect all the CRs generated by any communications providers in bulk.** Rather, the telephone metadata is stored by providers and the government can only obtain calling records associated with particular targeted numbers that have been approved by the FISA court. As explained further below, the government now sends its "query" terms to the providers and they run the queries in their databases and send back the query results. But even with the providers holding the data and conducting queries **the replacement CDR programs still permits to collect vast amounts of data, including the calling patterns of people who are not suspected of any wrongdoing.** What's more**, a series of recent disclosures indicates that the new programs is no more valuable than the ineffective former bulk collection program that it replaced.** These revelations should demonstrate to Congress that as the December 2019 sunset date for Section 215 approaches, **it should start by carrying out the promise of the USA Freedom Act, by eliminating the CDR program and truly ending bulk collection of Americans' Records**.

**Warrant:** Congress' renewal of the Freedom Act has not fulfilled the original intent to end mass surveillance of citizens.

Robertson, Adi. "Senate passes surveillance bill without ban on web history snooping" The Verge. 14 May 2020 https://www.theverge.com/2020/5/14/21257782/surveillance-bill-congress-senate-pass-usa-freedom-reauthorization-act

**"The Senate has voted to reauthorize the USA Freedom Act, bringing the surveillance bill closer to becoming law.** The USA Freedom Reauthorization Act restores government powers that expired in March with Section 215 of the Patriot Act. **While the Senate adopted an amendment to expand oversight, it shot down a proposal that would have restricted warrantless collection of internet search and web browsing data. Conversely, Sens. Ron Wyden (D-OR) and Steve Daines (R-MT) failed by one vote to pass a rule prohibiting warrantless surveillance of internet search and browsing records.** Wyden ultimately voted against the reauthorization. **"The legislation hands the government power for warrantless collection of Americans' web browsing and internet searches, as well as other private information, without having to demonstrate that those Americans have done anything wrong,"** he said in a statement**. "Without further reform of these vague and dangerous Patriot Act authorities, Congress is inviting more secret interpretations of the law and more abuses."**

**Warrant:** The government's mass collection of internet surveillance is even more concerning given that more are at home and online than ever.

Reed, Kevin. "US Senate reauthorizes domestic surveillance, allows access to internet histories". WSWS.org. 16 May 2020. https://www.wsws.org/en/articles/2020/05/16/surv-m16.html

**"**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."**

**Impact:** Government surveillance violates the original Freedom act suppressing individuals and democracy

**Warrant:** Government surveillance is tantamount to thought policing and should require a warrant.

Morrison, Sara. The Senate voted to let the government keep surveilling your online life without a warrant." Vox. 14 May 2020. https://www.vox.com/recode/2020/5/13/21257481/wyden-freedom-patriot-act-amendment-mcconnell

**"The vote was for an amendment to the controversial Patriot Act, which would have expressly forbidden internet browsing and history from what the government is allowed to collect through the approval of a secret court. Currently, there is no such provision, which means there's nothing stopping the government from doing so. The government has an established history of using this method to collect certain types of data about millions of Americans without their knowledge. "There is little information that is more personal than your web browsing history," Sen. Ron Wyden, a Democrat who sponsored the amendment, told Recode. "If you know that a person is visiting the website of a mental health professional, or a substance abuse support group, or a particular political organization, or a particular dating site, you know a tremendous amount of private and personal information about that individual. Getting access to**

**somebody's web browsing history is almost like spying on their thoughts," Wyden added. "This level of surveillance absolutely ought to require a warrant."**

**Warrant:** Government Surveillance suppresses social progress through free exchange of ideas and information.

Richards, Neil M. "The Dangers of Surveillance." Harvard Law Review. 20 May 2013**. https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/**

"At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state over-sight or interference, we need what I have elsewhere called "intellectual privacy." A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance."

**Warrant:** The government has an obligation to uphold its own laws and continue to protect citizens from their own overreach.

Lamont, Keir. "Rightsizing U.S. Surveillance Authority: Delivering on the USA Freedom Act Reforms". Disruptive Competition Project. 11 May 2020. https://www.project-disco.org/privacy/051120-

rightsizing-u-s-surveillance-authority-delivering-on-the-usa-freedom-act-reforms/

"**As the technical capabilities to collect and analyze personal data grow more advanced, it will be tempting for governments to conduct invasive surveillance over their citizens. Countries that value democratic principles must ensure that intelligence tools are carefully scoped to respect personal freedom and protect civil liberties.** While the USA Freedom Act took a critical step forward in restoring public transparency and accountability over U.S. surveillance activities, **Congress must remain vigilant in its oversight function to ensure that the intelligence community has the tools to protect U.S. citizens without violating personal liberties. Given what is now known about the operation of USA Freedom Act reforms, lawmakers should take additional steps to ensure that domestic intelligence gathering capacities are balanced, accountable, and transparent.**"

**Analysis:** The United State Congress has attempted to resolve the issues with the Patriot Act in passing the Freedom Act. However, their continued violations of their own laws, as well as the failure of congress to renew and enhance the full intentions of the Freedom Act to protect citizens is a violation of their obligations as leaders in our nation. If our own government cannot uphold their own laws, then how can they expect anyone else to, or to take them seriously as leaders.

## PRO: The NSA surveillance program harms mental health

**Argument:** Ending Government surveillance of citizens and lawful permanent residents will help with the mental health epidemic in our country.

**Warrant:** The United States has been and is in the midst of a Mental Health Crisis.

Wellness Network. "Treating American's Mental Health Crisis." The Wellness Network.net. 14 Mar 2019. https://www.thewellnessnetwork.net/health-news-and-insights/mental-health-crisis/

It's almost a certainty that you know someone suffering from a mental health disorder. While much of the medical profession is focused on physical diseases like heart disease and diabetes, **America is also in the grip of a less visible, but no less traumatic epidemic: mental health disorders.** Look at just a few numbers: **Anxiety is the most common mental health disorder in the United States, affecting more than 18% of the adult population, or more than 40 million people.** In the past year**, an estimated 16.2 million adults in the United States suffered from at least one major depressive episode.** Of these**, as many as 10 million suffered a "severe impairment" from their depression. As many as two-thirds of people diagnosed with generalized anxiety disorder also suffer from depression or another type of anxiety disorder,** complicating treatment**. Depression and anxiety,** together or separately**, are known to raise the risk of suffering from certain diseases, such as heart disease,** and can also make patients less likely to follow their treatment plan. While less common, bipolar disorder and schizophrenia affect about 2.6% and 1% of the U.S. adult population respectively**. These disorders can cause significant impairment and,** in many cases**, interfere with a patient's ability to work or enjoy a normal life. Mental illness is linked to**

**homelessness, higher risk of incarceration, and substance abuse.** In fact, **serious mental illness is estimated to cost America $193.2 billion every year in lost wages, not including the cost of treatment and the personal difficulties caused by mental illness.**

**Warrant:** The pandemic and other stressors are compounding the mental health crisis.

Bethune, Stephanie. "Stress in America 2020 Survey Signals a Growing National Mental Health Crisis." American psychological Association. October 20, 2020. https://www.apa.org/news/press/releases/2020/10/stress-mental-health-crisis

"**Nearly 1 in 5 adults (19%) say their mental health is worse than it was at this time last year.** By generation, 34% of Gen Z adults report worse mental health, followed by Gen X (21%), millennials (19%), boomers (12%) and older adults (8%). **Gen Z adults are the most likely to report experiencing common symptoms of depression, with more than 7 in 10 noting that in the prior two weeks they felt so tired that they sat around and did nothing (75%), felt very restless (74%), found it hard to think properly or concentrate (73%), felt lonely (73%), or felt miserable or unhappy (71%). "This survey confirms what many mental health experts have been saying since the start of the pandemic: Our mental health is suffering from the compounding stressors in our lives,"** said Arthur C. Evans Jr., PhD, APA's chief executive officer. **"This compounding stress will have serious health and social consequences if we don't act now to reduce it. We're already seeing this with some of the youngest members of our nation, who just seven months into this crisis are beginning to show signs of serious mental health issues, such as depression and anxiety."**

**Warrant:** Mental health is a second pandemic that will continue past COVID.

Heale, Roberta. "Is a Crisis in Mental Health the Next Pandemic?" BMJ:

Evidence Based Nursing. 4 Oct 2020. https://blogs.bmj.com/ebn/

**"The resulting mental health issues arising from COVID-19 have created a second pandemic–**one which has yet to be fully recognized**. In fact**, rather than an increase in mental health supports, **the need to distance and isolate has resulted in the amalgamation or closure of amenities and has resulted in fewer or less accessible mental health services in an already underserviced and stigmatized sector.** It's important for health care systems to recognize mental health as a significant issue and put strategies in place to address it. The COVID-19 pandemic has changed the world. As we all work to contain the virus, to keep as many people as possible safe, **we mustn't forget the mental health repercussions of this time. COVID-19 will last in our memories long after a vaccine has been found and the virus contained, but the mental health crisis it brought may be with us for a much longer time."**

**Warrant:** Government surveillance of citizens and lawful permanent residents is exacerbating the mental health crisis in the United States.

Stanley, Jay. "Does Surveillance Affect Us Even When We Can't Confirm We're Being Watched? Lessons From Behind the Iron Curtain." ACLU. 15 OCT 2012 . https://www.aclu.org/blog/national-security/privacy-and-surveillance/does-surveillance-affect-us-even-when-we-cant

"Of course, **the point is not that the FISA Amendments Act is equivalent to the kind of surveillance that took place behind the Iron Curtain**. Rather, it's that there are things we can learn from the experience of extreme surveillance in Eastern Europe. In particular, that experience makes especially clear a point that the government is trying to obfuscate in this case: **the negative effects of surveillance flow not just from direct observation, but equally from uncertainty over whether and when one might be under observation. Even a person who was never actually spied upon could have his or her life drastically curbed by the threat of such spying. That is a dynamic that operates in**

**all times and places where such a threat is present. The brief also includes a succinct rundown of studies that have shown how perceptions of surveillance** (not just surveillance**) cause psychological stress and altered behavior:** For example, **a workplace study** conducted statewide in New Jersey **found a direct correlation between workers' perceptions of surveillance and negative sentiments concerning privacy, role in the work place, self-esteem, and workplace communication.… Similarly, a study of seven urban centers in New Zealand supported the conclusion that a perceived lack of privacy is directly associated with psychosomatic stress."**

**Warrant:** Government Surveillance suppresses free expression which contributes to mental health issues and revictimization.

Jillian York. THE HARMS OF SURVEILLANCE TO PRIVACY, EXPRESSION AND ASSOCIATION. Global Information Society watch. 2014 https://www.giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and-association

"In a 2013 report, **Frank La Rue**, **Special Rapporteur to the United Nations** on the promotion 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." 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 metadata 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."**

**Warrant:** Government surveillance increases stress, anxiety, and other dangerous mental health issues.

Villnes, Zawn. "Watch Out: The Psychological Effects of Mass Surveillance" Good Therapy. 16 Sept 2013. https://www.goodtherapy.org/blog/watch-out-psychological-effects-of-mass-surveillance-0910137

"**A sense of privacy can play a significant role in the control people feel over their lives. We all have private thoughts and behaviors that we'd rather keep under wraps, but mass surveillance makes this much more challenging. A hastily typed email message or unfortunate Facebook update can suddenly become public knowledge. As far back as 1996, researchers found that people felt a loss of control when they knew they were being watched.** The mental health effects don't end there, though**. Researchers have found that as surveillance increases, so does anxiety. Anxiety can lead to a host of health conditions, including high blood pressure, obesity, respiratory problems, gastrointestinal problems, and even cancer.** Social networking, email, and text messaging play major roles in helping to maintain relationships with friends and family, especially across geographic distances. **When people know they're being watched,** though, **they tend to be more circumspect with their communications. What was once**

**a sarcastic inside joke might become something that, taken out of context, reads like a threat. As the zone of privacy around a relationship diminishes, so too might people's willingness to foster real intimacy and shared understandings."**

**Impact:** Ending government surveillance could help alleviate the mental health crisis facing the nation.

**Warrant:** We need to address mental health now to save our citizens and communities.

Mental Health America. "New State Rankings Shines Light on Mental Health Crisis, Shows Differences in Blue, Red States." Mental Health National.org 18 Oct 2016. https://www.mhanational.org/new-state-rankings-shines-light-mental-health-crisis-show-differences-blue-red-states

**"This is ultimately about policy decisions we make.** It isn't just about what states are red and what states are blue**," Gionfriddo added, "**because there are some of each near the top and the bottom. But political environments in states do seem to matter. **Those that invest more in mental health clearly have to throw away less money on jails and prisons. "It's time to act—we must invest in the overall physical and mental well-being of our citizens—every day," concluded Gionfriddo. "We must address these mental health concerns before crisis and tragedy strikes—before Stage 4."**

**Warrant:** Not acting now to help the mental health of our citizens will lead to a worse crisis.

Ornstein, Norm. "The Coming Mental-Health Crisis Congress must rethink the American approach to mental-health care during the pandemic." The Atlantic. 14 May 2020. https://www.theatlantic.com/ideas/archive/2020/05/coming-mental-health-crisis/611635/

**"The challenge is daunting—and not just for those who already face mental-health and substance-abuse issues and those at risk because of the changes in their life caused by the pandemic. Recent suicides and increased calls to crisis lines dedicated to health professionals and other essential workers underscore the size of the unaddressed problem.** The coronavirus has laid bare the failings of American health care and public health. **Without immediate action, it will do the same to America's fragile mental-health system.** Investment in that system will pay off, not just in terms of lives saved and bettered, but in monetary savings as well. **The demands for money to ease economic, medical, and social problems will accelerate when the coronavirus pandemic ebbs. The United States cannot allow the needs of mental health to be pushed aside by other priorities. If that happens, the price we will pay as a society will be fearsome."**

**Warrant:** Treatment alone is not enough, government policies for prevention are crucial.

Walrath, Christine. "The Mental Health Crisis is Spreading Faster Than Our Infrastructure Can Support: Here's what needs to change." Govexec.com. 24 July 2020. https://www.govexec.com/management/2020/07/mental-health-crisis-spreading-faster-our-infrastructure-can-support/167197/

**"Treatment alone, however, is not enough. We also need stronger prevention infrastructure. That requires creating the policies and programs to prevent things like substance abuse and suicide. Bolstering prevention offerings, coupled with more treatment options, will allow the United States to address both current and future issues."**

**Analysis:** The United States has already been facing a mental health crisis. Government Surveillance contributes to anxiety, stress, and mental health issues. With the current pandemic highlighting and worsening this crisis, the Government can control its own contributions to this by protecting the US citizens from the unwarranted surveillance policies currently in place.

## PRO: The NSA surveillance program runs contrary to the right to be forgotten

**Argument:** Government surveillance of citizens and lawful permanent residents takes away our Right to be Forgotten.

**Warrant:** More effective collection of data is necessary to protect citizens' rights to privacy..

Guariglia, Matthew. "Too much surveillance makes us less free. It also makes us less safe." Washington Post. 18 July 2017. https://www.washingtonpost.com/news/made-by-history/wp/2017/07/18/too-much-surveillance-makes-us-less-free-it-also-makes-us-less-safe/

"Since 1946, **the amount of retained information on individuals has increased from airplane hangars full of filing cabinets to massive National Security Agency data centers and algorithms combing through yottabytes of information.** But the same problems remain. Even as computer programs purport to solve the century-old problem of human errors, like misfiling and misidentifying, these mechanisms have also proved to be flawed and imprecise. **Dragnet surveillance tactics have accumulated 250 trillion household compact discs worth of data in a Utah data center. This mass data collection continues to pose a threat to Americans' safety, and has left some struggling to solve the problem of incidents of public violence. Since effective data analysis will always take time and energy, the solution today —** as it could have been in 1890 or 1920 — **is not to create a more technologically savvy means of combing through information, but to be far more selective in which data to collect. Doing so will not only protect Americans' right to privacy, but also their lives."**

**Warrant:** Government surveillance violates our 4th Amendment rights and right to our own levels of privacy.

Guariglia, Matthew . “NSA Spying.” Electronic Frontier Foundation. 2020 https://www.eff.org/nsa-spying

**“In September of 2014, EFF, along with the American Civil Liberties Union (ACLU) and the American Civil Liberties Union of Idaho, joined the legal team for Anna Smith, an Idaho emergency neonatal nurse, in her challenge of the government's bulk collection of the telephone records of millions of innocent Americans.** In Smith v. Obama**, we are arguing the program violated her Fourth Amendment rights by collecting a wealth of detail about her familial, political, professional, religious and intimate associations. In particular, we focus on challenging** the applicability of the so-called “third party doctrine,” **the idea that people have no expectation of privacy in information they entrust to others.”**

**Warrant**: The Human Rights Council has determined that individuals have a right to privacy that businesses but government are recognizing.

Damen, Juliane. “The Huma Right of Privacy in the Digital Age”. Semanticscholar.org. 2017. https://www.semanticscholar.org/paper/The-Human-Right-of-Privacy-in-the-Digital-Age-Damen Koehler/c9c238838f07a0541626c0c236fc038d4e40df31?p2df

“The Right to privacy in the digital age generates new challenges for the international jurisdiction. The following article deals with such challenges. Therefore, it firstly defines the term privacy in general and presents and international legal framework. **With whistleblower Snowden a huge political discourse was initiated and the article gives insights into its further development. In 2015 the Human Rights Council for the first time announced a special rapporteur on the right to privacy. However the discourse is**

**not only taking place on a political level, also civil society organizations advocate more stringent regulations and prosecutions against violations of the right to privacy. Moreover, the importance of the technology sector becomes clear. Companies like Microsoft are increasingly taking responsibility to protect digital media against unjustified data misuse, surveillance, collection and storate. But whereas the IT secor is developing very quickly, legislative processes do so rather slowly.** Lastly, the individual is also hold to account. To protect oneself against data misuse is to a great extent acting self-responsible. Still, therefore information on protection must be clear and accessible for everyone."

**Warrant:** A majority of American's believe that part of the right to privacy is also the right to be forgotten.

Auxier, Brooke. "Most Americans support right to have some personal info removed from online searches". Pew Research. 27 Jan 2020. https://www.pewresearch.org/fact-tank/2020/01/27/most-americans-support-right-to-have-some-personal-info-removed-from-online-searches/

**"Nearly nine-in-ten Americans (87%) agree with this idea when it comes to potentially embarrassing photos and videos. Majorities also think Americans should have a right to have personal financial data collected by a tax preparer (79%) and personal medical data collected by a health care provider (69%) deleted by the organization or person who holds the information.** Far fewer (36%) think personal data collected by law enforcement – like criminal records or mugshots – should be able to be deleted, which tracks with the findings around the removal of such data from public online search results. **Across several of these types of information, white Americans, older adults, those with higher annual household incomes and those higher levels of educational attainment are more likely to say all Americans should have the right to have their**

**personal information deleted. However, when it comes to views about data collected by law enforcement, black adults (47%) and Hispanic Americans (45%) are more likely than white adults (32%) to say the deletion of such information should be a right for all Americans."**

**Warrant:** US Government Mass surveillance has been found to violate right to be forgotten laws in the EU.

O'Brien, Danny. "EU Court Again Rules That NSA Spying Makes U.S. Companies Inadequate for Privacy". Electronic Frontier Foundation. 16 July 2020. https://www.eff.org/deeplinks/2020/07/eu-court-again-rules-nsa-spying-makes-us-companiesinadequateprivacy#:~:text=EU%20Court%20Again%20Rules%20That%20NSA%20Spying%20Makes%20U.S.%20Companies%20Inadequate%20for%20Privacy,Share%20It%20Share&text=The%20European%20Union's%20highest%20court,privacy%20rights%20of%20EU%20citizens.

**"The European Union's highest court today** made clear—once again—**that the US government's mass surveillance programs are incompatible with the privacy rights of EU citizens.** The judgment was made in the latest case involving Austrian privacy advocate and EFF Pioneer Award winner Max Schrems. **It invalidated the "Privacy Shield," the data protection deal that secured the transatlantic data flow, and narrowed the ability of companies to transfer data using individual agreements** (Standard Contractual Clauses, or SCCs). Whatever the initial reaction by EU regulators, companies and the Commission, **the real solution lies, as it always has, with the United States Congress. Today's decision is yet another significant indicator that the U.S. government's foreign intelligence surveillance practices need a massive overhaul.**

**Congress half-heartedly began the process of improving some parts of FISA earlier this year—a process which now appears to have been abandoned. But this decision shows, yet again, that the U.S. needs much broader, privacy-protective reform, and that Congress' inaction makes us all less safe, wherever we are."**

**Warrant:** The United State Should follow the EU with their own right to be forgotten laws.

Grachis, George. "Global Data Protection and the right to be forgotten.". CSO. 17 Oct 2019.

https://www.csoonline.com/article/3446446/global-data-protection-and-the-right-to-be-forgotten.html

"About data protection, **the EU directive states "obliges member states to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"** If you are a US citizen you probably know that the US Constitution does even mention the right to privacy, it's addressed in the 4th amendment under Search and Seizure:
**It's pretty simple: EU citizens have a right to be forgotten. All US corporations that store and process any EU citizen's personal information must comply with the right to be forgotten law and be fully compliant with GDPR.** In the meantime, **the US is still trying to figure out if it will continue with its siloed approach of state laws or finally land on a single federal privacy law like the EU's GDPR.** Whatever happens, it will impact all of us one way or another. As a lawyer colleague of mine recently shared with me, **whenever the federal government makes a law that applies to all states, then those states lose their individual rights in that area."**

**Impact:** The Right to be Forgotten protects individuals against government surveillance abuse and misuse.

**Warrant:** Stored and collected data could be used for malicious intent.

Stallman, Richard. “How Much Surveillance Can Democracy Withstand?”.GNU. 10 6 2020. https://www.gnu.org/philosophy/surveillance-vs-democracy.en.html

“In addition, **the state's surveillance staff will misuse the data for personal reasons. Some NSA agents used U.S. surveillance systems to track their lovers—past, present, or wished-for—in a practice called “LOVEINT.”** The NSA says it has caught and punished this a few times; we don't know how many other times it wasn't caught. But these events shouldn't surprise us, because **police have long used their access to driver's license records to track down someone attractive, a practice known as “running a plate for a date.” This practice has expanded with new digital systems. In 2016, a prosecutor was accused of forging judges' signatures to get authorization to wiretap someone who was the object of a romantic obsession.** The AP knows of many other instances in the US. **Surveillance data will always be used for other purposes, even if this is prohibited. Once the data has been accumulated and the state has the possibility of access to it, it can misuse that data in dreadful ways,** as shown by examples from Europe, the US, and most recently Turkey. (Turkey's confusion about who had really used the Bylock program only exacerbated the basic deliberate injustice of arbitrarily punishing people for having used it.) **Personal data collected by the state is also likely to be obtained by outside crackers that break the security of the servers, even by crackers working for hostile states.”**

**Warrant:** Personal digital data should not be allowed to ruin or end lives.

Garsd, Jasmine. “Internet Memes And 'The Right To Be Forgotten'”. NPR. 3 Mar 2015. HTTPS://WWW.NPR.ORG/SECTIONS/ALLTECHCONSIDERED/2015/03/03/390463119/INTERNET-MEMES-AND-THE-RIGHT-TO-BE-FORGOTTEN

"But for others, it's a nightmare. **Perhaps one of the most notable cases is Ghyslain Raza, "Star Wars Kid," who in 2003 became one of the first viral memes. This was before YouTube launched, and Raza did not even post the video. He simply taped himself doing *Star Wars*-style fighting for a school video club. His classmates secretly posted the video online, and it spread like wildfire. By the end of 2006, it had been clicked on more than 900 million times. It has more than 27 million views on YouTube and was parodied on *Family Guy*, *The Colbert Report* and *South Park*. For Raza, it was a teenage nightmare. He was bullied incessantly, to the point that he became depressed and dropped out of school to go to a children's psychiatric ward.** Raza's family initiated a lawsuit against the families of the four students who posted the video online. The family eventually dropped one of the cases and settled out of court for an undisclosed amount**."**

**Warrant:** Government surveillance overreaches is ruining lives and individuals should have the right to have their privacy protected.

Page, Carter. "FBI Spying Ruined My Good Name." WSJ. 10 Dec 2019. https://www.wsj.com/articles/fbi-spying-ruined-my-good-name-11576022322

**"My name is Carter Page, and I wish you were hearing it for the first time. If you were, I could introduce myself—a former naval officer who has worked for political figures from both parties. But my identity has been reduced to a series of false accusations**. If something isn't done to prevent future abuses of power by intelligence agencies, I won't be the last to lose his good name this way. **In 2016-17 the government I once served investigated me on suspicion of being an intermediary between the Trump campaign and the Russian government. This week Inspector General Michael Horowitz detailed how officials committed troubling errors over the course of the probe. From the day news of the investigation broke, I have faced threats to my life and have been forced**

> **to live like a fugitive. I still don't feel safe enough to establish a fixed residence.** I still have many questions about the FBI investigation that ruined my life. **If you value your privacy, reputation and right to political expression, you should too."**

**Analysis:** Government surveillance of citizens and lawful permanent residents breaches their right to privacy and even further with their right to be forgotten. The mass storage of information from phone calls, texts, and internet search histories, etc are a direct violation of 4th amendment search and seizure as well as unable to be accessed by the individuals to be erased if they so choose. Individuals make mistakes, say and do things on the internet that they may regret or that may potentially be used by the government and others to ruin their lives, careers, etc. Ending mass surveillance by the government is necessary to protect the rights of their citizens as is their primary responsibility.

## PRO: NSA Surveillance hurts U.S. credibility

**Argument:** NSA surveillance kills U.S. credibility in the eyes of the world making it more difficult to condemn other countries' human rights violations.

**Claim:** NSA surveillance hurts U.S. credibility

Kim Zetter, 7-29-2014, "Personal Privacy Is Only One of the Costs of NSA Surveillance," Wired, https://www.wired.com/2014/07/the-big-costs-of-nsa-surveillance-that-no-ones-talking-about/

THERE IS NO doubt the integrity of our communications and the privacy of our online activities have been the biggest casualty of the NSA's unfettered surveillance of our digital lives. But **the ongoing revelations of government eavesdropping have had a profound impact on the economy, the security of the internet and the credibility of the U.S. government's leadership when it comes to online governance.** These are among the many serious costs and consequences the NSA and those who sanctioned its activities---including the White House, the Justice Department and lawmakers like Sen. Dianne Feinstein---apparently have not considered, or acknowledged, according to a report by the New America Foundation's Open Technology Institute. "Too often, we have discussed the National Security Agency's surveillance programs through the distorting lens of a simplistic 'security versus privacy' narrative," said Danielle Kehl, policy analyst at the Open Technology Institute and primary author of the report. "But if you look closer, the more accurate story is that in the name of security, **we're trading away not only privacy, but also the U.S. tech economy, internet openness, America's foreign policy interests and cybersecurity**." Over the last year, **documents leaked by NSA whistleblower Edward Snowden, have disclosed numerous NSA spy operations that have gone beyond what many considered acceptable surveillance activity**. These included infecting the computers of network administrators working for a Belgian

telecom in order to undermine the company's routers and siphon mobile traffic; working with companies to install backdoors in their products or network infrastructure or to devise ways to undermine encryption; intercepting products that U.S. companies send to customers overseas to install spy equipment in them before they reach customers. The Foundation's report, released today, outlines some of the collateral damage of NSA surveillance in several areas, including: Economic losses to US businesses due to lost sales and declining customer trust. The deterioration of internet security as a result of the NSA stockpiling zero-day vulnerabilities, undermining encryption and installing backdoors in software and hardware products. **Undermining the government's credibility and leadership on "internet freedom" and governance issues such as censorship.**

**Warrant:** specifically, NSA degrades U.S. leadership online

Capital Flows, 12-20-2013, "NSA Snooping's Negative Impact On Business Would Have The Founding Fathers 'Aghast'," Forbes, https://www.forbes.com/sites/realspin/2013/12/20/nsa-snoopings-negative-Impact:on-business-would-have-the-founding-fathers-aghast/

Second, what will this mean for the future of Internet governance? Since its earliest days, **the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) has governed the web. As the Internet has expanded, several nations, especially China, have been pressing to end American dominance and transfer control of Internet** governance to the International Telecommunication Union (ITU), a specialized agency within the United Nations. Worse still for prospects of continued American dominance**, the NSA revelations have prompted calls for extensive regional control of the Internet. For example, Brazil, which has long called for such regional control, will host an important Internet governance conference in April that could challenge America's role. Unless the U.S. government takes steps to restore some degree of**

**trust, the groundswell of international interest in a new approach to Internet governance could undermine or end U.S. Internet leadership. This could leave management of the Internet to nations like China or Russia that do not share America's commitment to safety, openness, competition, and growth. Recommendations for change are coming from many corners.** President Obama's advisory group on NSA reform is calling for an end to bulk collection of Americans' metadata and other steps to restore protections abroad. Major Internet companies have called for greater restrictions on surveillance activities, saying the balance has tipped too far from the individual. The government should heed these calls for reflection and reform. Without understanding the economic implications of our security policies and taking reasonable steps to restore trust in America's surveillance efforts, our Internet dominance and our economy could pay the price.

**Impact:** NSA spying revelations boost oppressive regimes' power

Kenneth Roth, 11-18-2013, "The NSA's Global Threat to Free Speech," Human Rights Watch, https://www.hrw.org/news/2013/11/18/nsas-global-threat-free-speech

But the NSA's overreaching endangers free speech in more direct ways as well**. Consider the not-uncommon situation in which a repressive government such as China's asks an Internet company for information on a user.** The most notorious request of this kind involved the Chinese journalist Shi Tao, who just completed eight years in prison for "leaking state secrets"—sending a human rights group information about media restrictions for the fifteenth anniversary of the 1989 Tiananmen Square uprising and the ensuing massacre**. At China's request, Yahoo turned over Shi's email information, contributing to his conviction. One of the best defenses against such requests is for Internet companies to store user information in servers located outside the country in question.** That approach is not foolproof—governments have many ways to pressure Internet companies to cooperate—but it can help to fend off such requests. **US Internet**

**companies currently opt to repatriate to servers in the United States most information on users in foreign countries. However, after the revelations about NSA surveillance, many countries have said they may require Internet companies to keep data about their citizens on servers within their own borders. If that becomes standard practice, it will be easier for repressive governments to monitor Internet communications.** Weak as US privacy safeguards are, those in many other countries are no better. For example, while outraged at the NSA's snooping, many privacy activists in Brazil oppose their own government's proposed requirement to store data locally because they fear their data protection laws are inadequate.

**Analysis -** this argument shows that the U.S. must lead by example and is based on perception rather than result (making it easier to prove solvency). However, many affirmatives may have difficulty generating unique impact scenarios and may use this as a time suck to catch cons off guard.

## PRO: NSA surveillance is unconstitutional

**Argument:** as the NSA surveillance is unconstitutional it should end

**Claim:** NSA Surveillance violates the fourth and first amendment

Rainey Reitman, 11-22-2017, "NSA Internet Surveillance Under Section 702 Violates the First Amendment," Electronic Frontier Foundation, https://www.eff.org/deeplinks/2017/11/nsa-internet-surveillance-under-section-702-violates-first-amendment

The Supreme Court found **that the "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**." In short, **we all have the right to engage in associate with one another and to join and communicate with political and religious groups free from government surveillance.** As our society has moved online, our associations have become digital in nature. Signing up for a membership or learning about an advocacy group often happens over a website or app. Members of modern political groups coordinate donations, activities, and information over social networks, email, and websites. **When the NSA—either by itself or by working with corporate "partners"—collects the digital communications and browsing history of countless individuals, it's also obtaining records of innocent Americans visiting activism websites, becoming members of advocacy groups, and coordinating social movements.** EFF also raised this argument in our case against the mass telephone records collection by the NSA (substantially narrowed in 2015) First Unitarian Church of Los Angeles v NSA. **The surveillance of our communications systems, and thereby the surveillance of our communications, infringes on the very rights of private association upheld by the Supreme Court in 1958. So while the Fourth Amendment concerns about 702 and mass surveillance are important, they are not the only problem created**

**by the law.** And as Alex Abdo, an attorney at the Knight First Amendment Institute at Columbia University, argues that **when it comes to confronting government surveillance, we shouldn't expect the Fourth Amendment alone to protect our First Amendment interests.** He recently wrote that "The Fourth Amendment, unlike the First, is blind to the cumulative effects of invasions of privacy that are small in isolation but substantial in combination." Those cumulative effects are especially felt when it comes to the right to publish and access information freely. While the government may be forbidden from censoring online speakers and readers, **the cumulative impact of pervasive digital surveillance has a chilling effect on online communities.** The specter of government surveillance quells engagement in online forums, social networks, and blogs that discuss controversial, political, or unpopular positions. Knowing that the government is keeping a digital dossier of comments we leave online and articles we digitally share creates an environment in which speakers hesitate to engage in online political advocacy.

**Warrant:** the PRISM program specifically is unconstitutional as it violates the fourth amendment

Patrick Toomey, Senior Staff Attorney, ACLU National Security Project, 8-22-2018, "The NSA Continues to Violate Americans' Internet Privacy Rights," American Civil Liberties Union, 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, internet 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 compani**es. PRISM Slide **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 communications, 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 review 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 government 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.

**Impact:** first amendment protections are needed for a functioning democracy

Kelsey Cora Skaggs, May 2016, "Surveilling Speech And Association: NSA Surveillance Programs And The First Amendment", University of Pennsylvania, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1610&context=jcl

Regardless of the outcome of the Fourth Amendment analysis, however, **mass surveillance programs separately implicate the First Amendment.** The First Amendment and Fourth Amendment protect different rights and serve different purposes. The Fourth Amendment protects privacy, primarily benefitting the individual whose privacy is at 45 issue. By contrast, the First Amendment protects the rights to

association and expression. **Though the First Amendment benefits individuals," it also benefits society as a whole by ensuring the freedom of political activity that is necessary for a functioning democracy.47 The First Amendment protects ideas and dissent in a way that the Fourth Amendment does not, and this protection is of fundamental importance for a free and democratic society.4 8**

**Analysis:** smart affirmative teams should build more on why protecting the constitution should be a priority and should pull other cards about the impacts of the chilling effect. However, it is unclear what parts of the NSA remain today.

## PRO: Ending NSA Surveillance ends surveillance on minorities

**Argument:** NSA Surveillance unjustly targets minority communities through racial profiling

**Claim:** the government surveils minority communities disproportionally

Andrea Dennis, John Byrd Martin Chair of Law, University of Georgia School of Law, 2-18-2020, "Mass Surveillance and Black Legal History," American Constitution Society, https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/

If anything today is different from historical Black experiences with government surveillance, it's that **21st century technology advances have made the practice far easier and more widespread. What was once limited to human, street-level surveillance or wiretaps has expanded to include Black people's online activities**.[16] From social platforms such as Facebook, Twitter, and Instagram to content-sharing sites such as YouTube, SoundCloud, and Spotify, **law enforcement can watch and listen to whole communities, all from the comfort of their removed, secure offices**.[17] **As a result, street gang police units and other intelligence-gathering entities have moved much of their policing online.** Today**, law enforcement spends substantial resources monitoring the online conversations, activities, and networks of young Black and Latino men, looking for evidence of crimes, sometimes before any crime or real threat has occurred.**[18] **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 American 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.

**Warrant:** surveillance is justified as being targeted and is used for predictive policing

Malkia Amala Cyril, 3-30-2015, "Black America's State of Surveillance," Progressive.org, https://progressive.org/magazine/black-america-s-state-surveillance-cyril/

In an era of big data, the Internet has increased the speed and secrecy of data collection. Thanks to new surveillance technologies, law enforcement agencies are now able to collect massive amounts of indiscriminate data. Yet **legal protections and policies have not caught up to this technological advance. Concerned advocates see mass surveillance as the problem and protecting privacy as the goal. Targeted surveillance** is an obvious answer—it **may be discriminatory, but it helps protect the privacy perceived as an earned privilege of the inherently innocen**t. The trouble is**, targeted surveillance frequently includes the indiscriminate collection of the private data of people targeted by race but not involved in any crime. For targeted communities, there is little to no expectation of privacy from government or corporate surveillance.** Instead, we are watched, either as criminals or as consumers. We do not expect policies to protect us. Instead, we've birthed a complex and coded culture—from jazz to spoken dialects—in order to navigate a world in which spying, from AT&T and Walmart to public benefits programs and beat cops on the block, is as much a part of our built environment as the streets covered in our blood. In a recent address, New York City Police Commissioner Bill Bratton made it clear: "2015 will be one of the most significant years in the history of this organization. It will be the year of technology, in which we literally will give to every member of this department technology that would've been unheard of even a few years ago." **Predictive policing, also known as "Total Information Awareness," is described as using advanced technological tools and data analysis to "preempt" crime. It utilizes trends, patterns, sequences, and affinities found in data to make determinations about when and where crimes will occur. This model is deceptive, however, because it presumes data**

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

**Warrant:** Muslims are specifically targeted by the NSA

Malkia Amala Cyril, 3-30-2015, "Black America's State of Surveillance," Progressive.org, https://progressive.org/magazine/black-america-s-state-surveillance-cyril/

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

**Warrant:** NSA Surveillance is rooted in slavery

Barton Gellman, 12-21-2017, "The Disparate Impact of Surveillance," Century Foundation, https://tcf.org/content/report/disparate-Impact:surveillance/?agreed=1

We do not need a unified theory of privacy to show that, in each of its meanings, marginal communities enjoy far less of it in practice. In some contexts**, poor people and people of color have legal rights to privacy, but no means to exercise them**; "paper rights," as Karl Llewellyn called them.27 In other contexts**, the government justifies extraordinary surveillance in superficially general language that applies exclusively, or close to exclusively, in minority neighborhoods. In still others, the government denies a disfavored class a privacy right, even in principle, that other Americans freely enjoy.** We focus most concretely in this report on excesses of surveillance in policing and in the interactions of the poor with the welfare state. **Policing Surveillance in America owes its origins, in part, to the slave economy. P**oet and media activist Malkia Cyril puts the point provocatively: "From colonial times to now, **surveillance technologies have been used to separate the citizen from the slave, to protect the citizen from the slave."28** Plantation ledger books served as proto-biometric databases, recording the slaves as physical specimens in fine detail. The slave pass, the slave patrol, and the fugitive slave poster—three pillars of information technology in their day—prefigured modern policing, tracking, and photo ID. Plantation space, by one historian's account, was organized to enable planters and overseers to "exercise surveillance and reinforce the subordinate status of enslaved people."29

**Warrant:** those in poverty cannot buy privacy, making them vulnerable to surveillance

Barton Gellman, 12-21-2017, "The Disparate Impact of Surveillance," Century Foundation, https://tcf.org/content/report/disparate-Impact:surveillance/?agreed=1

Policy has to comply with law, but it does much more than that. Policy makers are free to consider facts and values that judges do not. They may use policy to correct what Vanderbilt University law professor Christopher Slobogin calls the "poverty exception"44 that courts have carved out of the Fourth Amendment. Something is very

wrong when protection against "unreasonable search and seizure" depends on conditions that money can buy and the poor cannot hope to afford.45 Stuntz hypothesized **that poor neighborhoods are over-policed because the police face fewer constitutional limits there. Search and seizure and, therefore, arrest, are simply cheaper in budget and personnel.** Considering the example of drug markets, Stuntz writes, "In well-off neighborhoods, transactions are likely to take place in private dwellings through arranged meetings; in poorer neighborhoods, transactions take place on the street. Fourth Amendment law makes it much harder to police the former, and thereby pushes police to focus ever more on the latter."46 That explanation fits bureaucratic behavior in other contexts. But it does not seem likely to cover all, or even many, of the motives for law enforcement scrutiny in disfavored minorities. The causal relationship, in many respects, could as easily be reversed. **The law found more leeway to invade the Fourth Amendment rights in poor communities because the poor—especially the non-white poor—are perceived as uniquely menacing.** "The police are not picking on the urban poor because the rest of society is too hard to search," Slobogin writes. "[T]hey are simply going after the group they think, rightly or wrongly, is most crimogenic."47 Regardless of motive, **poor communities of color are policed not only more frequently but with a far heavier hand than whiter and wealthier ones.**48

**Impact:** NSA surveillance silences minority voices

Lauren C., 3-29-2016, "How The NSA Revelations Made Surveillance Worse For Minorities," ThinkProgress, https://archive.thinkprogress.org/how-the-nsa-revelations-made-surveillance-worse-for-minorities-f571218c49ab/

**"When individuals think they are being monitored and disapprove of such surveillance practices, they are equally as unlikely to voice opinions in friendly opinion climates as they are in hostile ones,**" researchers concluded. **Speaking out is highest "when one is the majority" and staying quiet is strongest when someone believes their online**

**activity is being monitored but thinks the government practice is justified.** One of the study's lead researchers, Elizabeth Stoycheff, told the Washington Post that people dismiss online surveillance because they don't have anything to hide. "So many people I've talked with say they don't care about online surveillance because they don't break any laws and don't have anything to hide. And I find these rationales deeply troubling," said Stoycheff, who is an assistant professor at Wayne State University. **Those same individuals who don't voice their opinions, she said, are "enabling a culture of self-censorship because it further disenfranchises minority groups."** Knowing that people are less inclined to state their opinions on the government's behavior is generally disturbing, but Stoycheff was right. **Dismissing online surveillance as no big deal, or self-censoring, deletes the voices of those most likely to be victimized by government misconduct. Racial and religious minorities in America are at an increased risk of being targeted by law enforcement. Surveillance programs** tossed around by Republican presidential **candidates advocate for illegal monitoring of Muslim communities. People of color are notoriously vulnerable to police harassment and brutality, but are particularly at risk online.** More than 70 percent of Blacks or Latinos online use Facebook, and are more likely to use Twitter and Instagram than their white counterparts, according to Pew Research. Those sites, particularly Twitter and Instagram, are often used to promote awareness for social movements such as Black Lives Matter, and have been monitored by law enforcement. On top of online monitoring, **minorities are disproportionately at risk of digital privacy violations through cellphone tracking and the physical confiscation of devices upon arrest or during travel because they are more likely to access the internet through mobile devices.**

**Analysis:** this argument would function well as a critical affirmative as it implies that all surveillance is racist thus voting pro is a positive measure to counter that racism. However, the impacts are difficult to quantify (yet are very real) making it difficult to persuade lay judges

especially in some circuits. If you run this argument, it would help to read up more on some of the philosophical theories of surveillance and the history of COINTEL

## PRO: NSA Surveillance is inefficient

**Argument:** NSA surveillance does more harm than good by being inefficient

**Claim:** NSA surveillance collects so much data it's inefficient

Zack Whittaker, 4-27-2016, "NSA is so overwhelmed with data, it's no longer effective, says whistleblower," ZDNet, https://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/

"The data was all there**... the NSA is great at going back over it forensically for years to see what they were doing before that,**" he said. "But that doesn't stop it." Binney called this a "bulk data failure" -- in **that the NSA programs, leaked by Edward Snowden, are collecting too much for the agency to process**. He said **the problem runs deeper across law enforcement and other federal agencies, like the FBI, the CIA, and the Drug Enforcement Administration (DEA), which all have access to NSA intelligence**. The Future State of Endpoint Security Since COVID-19, on-site offices, devices and networks have shifted to remote work and workforces. This shift has propelled security to the forefront as protecting work-anywhere employees is paramount to organizational success. But how do companies assess their current security state? What factors go into selecting hardware and software to maintain security compliance while protecting the end-user experience? White Papers provided by Jamf **Binney left the NSA a month after the September 11 attacks in New York City in 2001, days after controversial counter-terrorism legislation was enacted -- the Patriot Act -- in the wake of the attacks**. Binney stands jaded by his experience leaving the shadowy eavesdropping agency, but impassioned for the job he once had. He left after a program he helped develop was scrapped three weeks prior to September 11, replaced by a system he said was more expensive and more intrusive. Snowden said he was inspired by Binney's case, which in part inspired him to leak thousands of classified documents to journalists. Since then**,**

**the NSA has ramped up its intelligence gathering mission to indiscriminately "collect it all."** Binney said the NSA is today not as interested in phone records -- such as who calls whom, when, and for how long. Although the Obama administration calls the program a "critical national security tool," the agency is increasingly looking at the content of communications, as the Snowden disclosures have shown.

**Warrant:** new programs further increase the amount collected

Geoffrey Ingersoll, 10-30-2013, "'Numerous' NSA Analysts Don't Like The Google Cloud Hack, And For Good Reason," Business Insider, https://www.businessinsider.com/the-nsa-is-collecting-too-much-data-2013-10

**The National Security Agency has found a way to circumvent the encryption process between Yahoo/Google's public Internet and cloud encryption through a program codenamed MUSCULAR**, reports Barton Gelmann of the Washington Post. Presumably, that would be awesome for the NSA, but **multiple analysts have complained about being awash in too much information. According to the Post's NSA slides, "Numerous S2 [intelligence] analysts have complained of its [MUSCULAR] existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4 of the total data collect)." The slide goes on, "Numerous offices have complained about this collection diluting their workflow**." The complaints jibe with what NSA whistleblower William Binney said about NSA Chief Keith Alexander's claim that you need the "haystack" in order to find the needle.

**Warrant:** Collective from U.S citizens continued to increase

Charlie Savage, 5-4-2018, "N.S.A. Triples Collection of Data From U.S. Phone Companies (Published 2018)," New York Times,

https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

WASHINGTON — **The National Security Agency vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year — more than three times what it collected in 2016, a new report revealed on Friday.** Intelligence analysts are also more frequently searching for information about Americans within the agency's expanding collection of so-called call detail records — telecom metadata logging who contacted whom and when, but not the contents of what they said. The new report — an annual set of surveillance-related statistics issued by the Office of the Director of National Intelligence — did not explain why the number of records increased so dramatically. But in an interview, Alex Joel, the office's chief civil liberties officer, said the N.S.A. had not reinterpreted its legal authorities to change the way it collects such data. He cited **a variety of factors** that **might have contributed to the increase, potentially including changes in the amount of historical data companies are choosing to keep, the number of phone accounts used by each target and changes to how the telecommunications industry creates records based on constantly shifting technology and practices. "**Based on what we have learned from this data, we expect it will continue to fluctuate from year to year," Mr. Joel said. Still, **the large and growing volume of data gathered shows that the N.S.A. continues to collect significant amounts of information about Americans' phone and text messages after changes made by Congress in a 2015 law, the USA Freedom Act, which overhauled how the N.S.A. can gain access to domestic telecom data. .**

**Impact:** NSA Surveillance costs $100 million without producing results

Charlie Savage, 2-25-2020, "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads," New York Times, https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

**N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads** A disputed program that allowed the National Security Agency to gain access to logs of Americans' domestic calls and texts yielded only one significant investigation, according to a newly declassified study**. 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 technical headaches,** halting a counterterrorism effort that has touched off disputes about privacy and the rule of law since the Sept. 11, 2001, attacks.

**Analysis:** this argument is nice, straightforward, and gives the pro a two impact scenario of (1) inefficiency leads to national security risks and (2) money. This argument could also be incorporated as a rebuttal overview that removes solvency while creating independent offense.

## PRO: NSA Surveillance hurts the economy

**Argument:** NSA surveillance hurts the economy by discrediting U.S businesses.

**Warrant:** differences in laws put businesses at risk

Caren Morrison, Associate Professor of Law, Georgia State University, 10-20-2015, "Ruling shows Europe still vexed over NSA spying, leaving US companies in legal limbo," Conversation, https://theconversation.com/ruling-shows-europe-still-vexed-over-nsa-spying-leaving-us-companies-in-legal-limbo-48938

**Large businesses are operating as usual, only with armies of lawyers behind the scenes redrafting contracts and figuring out next moves.** Some are speeding up plans to build European data-storage facilities, even though it's not clear that geographical siloing of data will really protect against NSA surveillance. **The situation is even more daunting for smaller companies, which represent 60% of the users of Safe Harbor. Data service and storage companies working for US multinationals risk being replaced by European companies if data can't be transferred.** The European Commission has promised new guidance soon, but negotiations between Europe and the United States for a new data transfer pact have been dragging on for two years. Worse, **any agreement will have to address the fundamental incompatibility between European and American laws. If US companies pledge to keep data safe, they could find themselves in violation of NSA demands for "compelled assistance," potentially exposing them to fines as high as $250,000 a day.** But **if US companies comply with NSA requests for user data, they might be violating Europe's privacy laws and face fines from their European hosts. So what's a company to do?** For now, the US Department of Commerce is "continuing to administer the Safe Harbor program, including processing submissions for self-certification." It does add, however, that companies might want to call a lawyer.

**Warrant:** NSA Surveillance weakened cyber security

Denver Nicks, 7-8-2014, "NSA Spying Hurts Cybersecurity for All of Us Say Privacy Advocates," Time, https://time.com/2966463/nsa-spying-surveillance-cybersecurity-privacy-advocates-schneier

"**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 referenced 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. In the year since former NSA contractor Edward Snowden's first leaks, attention has focused on the Agency's surveillance itself, fueling debates over whether it is legal and ethical to spy on American citizens or to eavesdrop on the leaders of allied countries. **NSA policies that intentionally undermine cybersecurity too often get left out of the debate, said** panelists Monday at a New American Foundation event titled "National Insecurity Agency: How the NSA's Surveillance Programs Undermine Internet Security."

**Impact:** NSA surveillance may have costs billions

Zack Whittaker, 2-25-2015, "It's official: NSA spying is hurting the US tech economy," ZDNet, https://www.zdnet.com/article/another-reason-to-hate-the-nsa-china-is-backing-away-from-us-tech-brands/

**China is no longer using high-profile US technology brands for state purchases, amid ongoing revelations about mass surveillance and hacking by the US government**. A new report confirmed key brands, including Cisco, Apple, Intel, and McAfee -- among

others -- have been dropped from the Chinese government's list of authorized brands, a Reuters report said Wednesday. **The number of approved foreign technology brands fell by a third, based on an analysis of the procurement list. Less than half of those companies with security products remain on the list. Although a number of reasons were cited, domestic companies were said to offer "more product guarantees" than overseas rivals in the wake of the Edward Snowden leaks. Some reports have attempted to pin a multi-billion dollar figure on the impact of the leaks. In reality, the figure could be incalculable**. The report confirms what many US technology companies have been saying for the past year: the activities by the NSA are harming their businesses in crucial growth markets, including China.

**Quantification:** NSA surveillance cost $180 billion

Jon Swartz, 2-28-2014 "NSA surveillance hurting tech firms' business," USA TODAY, https://www.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/

The National Security Agency, and revelations about its extensive surveillance operations — sometimes with the cooperation of tech firms — have undermined the ability of many U.S. companies to sell products in key foreign countries, creating a fissure with the U.S. government and prompting some to scramble to create "NSA-resistant" products. The fallout could cost the tech industry billions of dollars in potential contracts, which has executives seething at the White House. "Suspicion of U.S. vendors is running at an all-time high," says Andrew Jaquith, chief technology officer at cloud-security firm SilverSky. Cisco, IBM, Microsoft and Hewlett-Packard have reported declines in business in China since the NSA surveillance program was exposed. The Information Technology & Innovation Foundation estimates the NSA imbroglio will cost U.S. businesses $22 billion through 2016. Forrester Research pegs potential losses at $180 billion, which includes tech firms and managed service providers The

> conflagration took on political tones this month when German Chancellor Angela Merkel — whose mobile phone was tapped by U.S. spy agencies — said she would press France President Francois Hollande to back a push for EU-based alternatives to the current U.S.-dominated Internet infrastructure.

**Analysis:** this argument is easy to prove that past NSA surveillance cost business, especially if you set up the argument as “the next Snowden will cost us”. In addition, this evidence would work well with an impact to the argument that NSA surveillance weakened cyber security.

## PRO: The NSA spies on activists and protestors

**Argument**: The NSA spies on activists and protestors under the guise of national security.

**Warrant**: The NSA can collect vast amounts of data on disfavored communities.

Yachot, Noa. "History shows activists should fear the surveillance state." ACLU. 10/27/17. https://www.aclu.org/blog/national-security/privacy-and-surveillance/history-shows-activists-should-fear-surveillance

Under Section 702 of the Foreign Intelligence Surveillance Act, the National Security Agency collects vast amounts of phone calls, emails, text messages, and more from Americans communicating with people overseas, often sweeping up domestic communications in the process — all without individualized warrants from a court. Government agencies can then search through that data for information about anyone, in a subversion of judicial protections meant to prevent abuse of government powers. The threat that these protections guard against isn't theoretical. Recent history clearly shows that the burden of overzealous surveillances falls on disfavored communities who powerful actors believe threaten the status quo. While 20th century reforms were designed to curtail precisely these abuses, surveillance hawks continue to fight tooth and nail to retain their ability to use Section 702 to search for information about American residents without ever needing to make a case before a judge.

**Evidence**: The NSA and other government organizations are already spying on activists around the country.

Gibbons, Chip. "Government surveillance of activists and labor organizers is alive and well." Jacobin Magazine. June 2006.

https://jacobinmag.com/2020/06/government-surveillance-activists-labor-organizers-pinkertons

In February 2020, University of California–Santa Cruz graduate student workers refused to turn in final grades unless their demand for a Cost of Living Adjustment (COLA) to match the cost of housing was met. As the administration refused to meet this demand, the graduate student workers' protest became a wildcat strike.

Emails recently obtained by Vice as part of a public records request reveal the lengths the administration was willing to go to to thwart the strike. Rather than meeting their demands, the administration worked with campus police, the Alameda County Sheriff's Office, the California National Guard, and the California Office of Emergency Services to police the strike.

These agencies also turned to the California State Threat Assessment Center, a "state fusion center." Fusion centers are affiliated with the Department of Homeland Security and share intelligence between state, federal, and private entities. According to a 2012 Congressional investigation, fusion centers produce intelligence of "uneven quality — oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."

**Evidence**: NSA software developed by Lockheed Martin was used against labor activists.

Gibbons, Chip. "Government surveillance of activists and labor organizers is alive and well." Jacobin Magazine. June 2006.
https://jacobinmag.com/2020/06/government-surveillance-activists-labor-organizers-pinkertons

The FBI had already used its counterterrorism authorities to spy on Occupy. In fact, before the first protesters had ever gathered in Lower Manhattan, the FBI was not only

keeping tabs on the movement, but also relaying that information to the New York Stock Exchange and private businesses.

Walmart didn't merely have to rely on state actors. The company has its own global security division, which is headed by a former FBI agent. And when it first learned of the organizing effort, Walmart hired Lockheed Martin. While it is best known as a weapons producer, Lockheed Martin also has been "involved in surveillance and information processing for the CIA, the FBI, the Internal Revenue Service (IRS), the National Security Agency (NSA), the Pentagon, the Census Bureau, and the Postal Service."

In the service of Walmart, Lockheed Martin monitored activists' social media accounts. Lockheed Martin also monitored the movement of a "Caravan of Respect," a group of workers traveling to Walmart's annual shareholder meetings.

**Impact**: Suppressing activism squashes dissent and ignores individual right to protest.

Gibbons, Chip. "Government surveillance of activists and labor organizers is alive and well." Jacobin Magazine. June 2006. https://jacobinmag.com/2020/06/government-surveillance-activists-labor-organizers-pinkertons

Both public and private intelligence have partial origins in attempts to suppress domestic labor radicalism. Just as private detective agencies tried to foil strikes, some of the earliest police intelligence units were "Red Squads." One of the earliest intelligence units of the FBI was its "Radical Division," responsible for founding up leftists during the Palmer Raids. Since 9/11, intelligence-gathering has reemerged as the FBI's top priority. Given that such intelligence-gathering has long been used to spy on leftists and labor organizing, this is bad news for civil liberties.

> In the past, abuses like this galvanized civil libertarians to defend working-class free speech from the monied interests seeking to squash dissent. Those who purport to care about free speech should be no less concerned about our modern-day Pinkertons.

**Analysis**: The NSA is a tool of the state, meaning that it's often used by the state to stop things that would upset the status quo. Examples of this include labor protestors, who have been spied on with NSA technology that bleeds into the private sector. Squashing dissent and intimidating protestors is certainly not a good use of government money.

## PRO: NSA spying is unpopular among Americans

**Argument**: Most Americans are uncomfortable with the notion of a surveillance state, and therefore are opposed to the NSA on principle.

**Warrant**: Public opinion polls reveal that a cross-section of Americans dislike the NSA.

> **Gao, George. "What Americans think** about **NSA surveillance, national security, and privacy." Pew Research Center. 5/29/15. https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/**
>
> **A majority of Americans (54%) disapprove of the U.S. government's collection of telephone and internet data as part of anti-terrorism efforts**, while 42% approve of the program. Democrats are divided on the program, while Republicans and independents are more likely to disapprove than approve, according to a survey we conducted in spring 2014.

**Evidence**: Americans are not willing to trade liberty for security, in the context of surveillance.

> **Gao, George. "What Americans think** about **NSA surveillance, national security, and privacy." Pew Research Center. 5/29/15. https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/**
>
> **More broadly, most Americans don't see a need to sacrifice civil liberties to be safe from terrorism**: In spring 2014, 74% said they should not give up privacy and freedom for the sake of safety, while just 22% said the opposite. This view had hardened since

December 2004, when 60% said they should not have to give up more privacy and freedom to be safe from terrorism.

**Warrant**: Ending NSA surveillance has bipartisan and third party support.

Staff. "Protesters march in Washington against NSA spying." Reuters. 10/26/13. https://www.reuters.com/article/us-usa-security-protest/protesters-march-in-washington-against-nsa-spying-idUSBRE99P0B420131026

People carried signs reading: "Stop Mass Spying," "Thank you, Edward Snowden" and "Unplug Big Brother" as they gathered at the foot of the Capitol to demonstrate against the online surveillance by the National Security Agency.
Estimates varied on the size of the march, with organizers saying more than 2,000 attended. U.S. Capitol Police said they do not typically provide estimates on the size of demonstrations.
The march attracted protesters from both ends of the political spectrum as liberal privacy advocates walked alongside members of the conservative Tea Party movement in opposition to what they say is unlawful government spying on Americans.

**Impact**: Unrepresentative policy leads to unrest and protests.

Staff. "Protesters march in Washington against NSA spying." Reuters. 10/26/13. https://www.reuters.com/article/us-usa-security-protest/protesters-march-in-washington-against-nsa-spying-idUSBRE99P0B420131026

"Over the past several months, we have learned so much about the abuses (of privacy) that are going on and the complete lack of oversight and the mass surveillance into every detail of our lives. And we need to tell Congress that they have to act," said another protester, Jennifer Wynne.

> The event was organized by a coalition known as “Stop Watching Us” that consists of some 100 public advocacy groups and companies, including the American Civil Liberties Union, privacy group Electronic Frontier Foundation, Occupy Wall Street NYC and the Libertarian Party.

The groups have been urging Congress to reform the legal framework supporting the NSA’s secretive online data gathering since Snowden’s disclosure of classified information about the programs that are designed to gather intelligence about potential foreign threats.

**Analysis**: The NSA was empowered at a time when the United States chose to prioritize security, but in 2020, most citizens believe the tradeoff of security for liberty is simply not worth making. Democratic policies are supposed to represent the people, and as we have seen, unrest and protests can arise when representation is disregarded.

## PRO: The NSA is subject to leaks

**Argument**: The NSA, an organization responsible for immense amounts of private collected data, is notorious for its loss of data and history of leaks.

**Warrant**: Edward Snowden revealed the extent of NSA surveillance.

Starr, Barbara. "Man behind NSA leaks says he did it to safeguard privacy, liberty." CNN. 6/23/13. https://www.cnn.com/2013/06/10/politics/edward-snowden-profile/index.html

He's a high school dropout who worked his way into the most secretive computers in U.S. intelligence as a defense contractor -- only to blow those secrets wide open by spilling details of classified surveillance programs.

Now, Edward Snowden might never live in the United States as a free man again. Where he may end up was a source of global speculation Sunday after he flew from Hong Kong to Russia, his ultimate destination unknown to most. Snowden has revealed himself as the source of documents outlining a massive effort by the U.S. National Security Agency to track cell phone calls and monitor the e-mail and Internet traffic of virtually all Americans.

Snowden, 29, said he just wanted the public to know what the government was doing.

**Evidence**: New information is still being exposed from the original NSA leak.

Riechmann, Deb. "Costs of Snowden leak still mounting 5 years later." AP News. 6/4/18. https://apnews.com/article/797f390ee28b4bfbb0e1b13cfedf0593

The top U.S. counterintelligence official said journalists have released only about 1

percent taken by the 34-year-old American, now living in exile in Russia, “so we don’t see this issue ending anytime soon.”

“This past year, we had more international, Snowden-related documents and breaches than ever,” Bill Evanina, who directs the National Counterintelligence and Security Center, said at a recent conference. “Since 2013, when Snowden left, there have been thousands of articles around the world with really sensitive stuff that’s been leaked.”

On June 5, 2013, The Guardian in Britain published the first story based on Snowden’s disclosures. It revealed that a secret court order was allowing the U.S. government to get Verizon to share the phone records of millions of Americans. Later stories, including those in The Washington Post, disclosed other snooping and how U.S. and British spy agencies had accessed information from cables carrying the world’s telephone and internet traffic.

**Warrant**: Leaks are still being addressed, and often the NSA can’t find the source of the leak.

Abdolleh, Tami. “Mystery of NSA leak lingers as stolen document case winds up.” AP News. 7/6/19. https://apnews.com/article/f84c3f7f9cb54ef7aaab16acbbc6f61a

Federal agents descended on the suburban Maryland house with the flash and bang of a stun grenade, blocked off the street and spent hours questioning the homeowner about a theft of government documents that prosecutors would later describe as “breathtaking” in its scale.

The suspect, Harold Martin, was a contractor for the National Security Agency. His arrest followed news of a devastating disclosure of government hacking tools by a mysterious internet group calling itself the Shadow Brokers . It seemed to some that the United States might have found another Edward Snowden, who also had been a contractor for the agency.

“You’re a bad man. There’s no way around that,” one law enforcement official conducting the raid told Martin, court papers say. “You’re a bad man.”

> Later this month, about three years after that raid, the case against Martin is scheduled to be resolved in Baltimore's federal court. But the identity of the Shadow Brokers, and whoever was responsible for a leak with extraordinary national security implications, will remain a public mystery even as the case concludes.

**Impact**: Leaks hurt privacy and put Americans at risk.

> Riechmann, Deb. "Costs of Snowden leak still mounting 5 years later." AP News. 6/4/18. https://apnews.com/article/797f390ee28b4bfbb0e1b13cfedf0593

> The top U.S. counterintelligence official said journalists have released only about 1 percent taken by the 34-year-old American, now living in exile in Russia, "so we don't see this issue ending anytime soon."
> "This past year, we had more international, Snowden-related documents and breaches than ever," Bill Evanina, who directs the National Counterintelligence and Security Center, said at a recent conference. "Since 2013, when Snowden left, there have been thousands of articles around the world with really sensitive stuff that's been leaked."
> On June 5, 2013, The Guardian in Britain published the first story based on Snowden's disclosures. It revealed that a secret court order was allowing the U.S. government to get Verizon to share the phone records of millions of Americans. Later stories, including those in The Washington Post, disclosed other snooping and how U.S. and British spy agencies had accessed information from cables carrying the world's telephone and internet traffic.

**Analysis**: The NSA is an organization dedicated to security, yet it has historically not been a very secure organization itself. The Snowden leak is well known, but it's unclear how much information was originally leaked, and how much more information has been leaked in subsequent incidents. The NSA is jeopardizing American security and privacy by handling this information in such an insecure manner.

## PRO: The NSA antagonizes China and Chinese Americans

**Argument**: The NSA has been used to spy on China, and Americans of Chinese descent. This has created tensions with China, and has been a justification for discriminatory practices.

**Warrant**: The NSA has historically been used to spy on China, even going back to the Obama administration.

Aid, Mathew. "Inside the NSA's ultra-secret China hacking group." South China Morning Post. 6/12/13. https://www.scmp.com/news/china/article/1259175/inside-nsas-ultra-secret-china-hacking-group

Last weekend, US President Barack Obama sat down for a series of meetings with China's newly appointed leader, Xi Jinping. We know that the two leaders spoke at length about the topic du jour – cyber-espionage – a subject that has long frustrated officials in Washington and is now front and centre with the revelations of sweeping US data mining. The media has focused at length on China's aggressive attempts to electronically steal US military and commercial secrets, but Xi pushed back at the "shirt-sleeves" summit, noting that China, too, was the recipient of cyber-espionage. But what Obama probably neglected to mention is that he has his own hacker army, and it has burrowed its way deep, deep into China's networks.

When the agenda for the meeting at the Sunnylands estate outside Palm Springs, California, was agreed to several months ago, both parties agreed that it would be a nice opportunity for President Xi, who assumed his post in March, to discuss a wide range of security and economic issues of concern to both countries. According to diplomatic sources, the issue of cyber-security was not one of the key topics to be discussed at the summit. Sino-American economic relations, climate change, and the growing threat posed by North Korea were supposed to dominate the discussions.

**Evidence**: Today, the government surveils Chinese Americans suspected of spying.

Waldman, Peter. "Mistrust and the hunt for spies among Chinese Americans." Bloomberg. 12/10/19. https://www.bloomberg.com/news/features/2019-12-10/the-u-s-government-s-mistrust-of-chinese-americans

Su's ordeal reflects how the U.S. government's distrust of China, which flared during the Obama administration and erupted openly during President Donald Trump's trade war, has mutated into distrust of Chinese Americans. Signs of this heightened scrutiny emerged in July when FBI Director Christopher Wray told the Senate Judiciary Committee that the bureau is investigating more than 1,000 cases of attempted theft of U.S. intellectual property, with "almost all" leading back to China. Last year the U.S. National Institutes of Health, working with the FBI, started probes into some 180 researchers at more than 70 hospitals and universities, seeking undisclosed ties to China. Some of the suspected scientists were instructed by their associates in China to conceal their connections to the country while in the U.S., says Ross McKinney, chief scientific officer for the Association of American Medical Colleges. "The presumption of trust is blown by the fact that there's a systematic approach to lying," he says.

**Warrant**: The government has been known to use the surveillance state to keep track of Chinese Americans.

Hvistendahl, Mara. "The FBI's China obsession." The Intercept. 2/2/20. https://theintercept.com/2020/02/02/fbi-chinese-scientists-surveillance/

As Chinese American scientists returned to visit long-lost friends and relatives, the bureau closely tracked them.
In 1972, Jen led a delegation of Chinese American scientists and their families to China. Katherine Yih, who joined her father on the trip, recalled a highly orchestrated

tour that included visiting agricultural communes and watching children's dance performances. "We were being shown the successes of the revolution," she said. The visitors were seen as important enough that they were also taken to meet Premier Zhou Enlai, a development that almost certainly heightened the suspicions of U.S. counterintelligence operatives.

**Impact**: The surveillance state engages in discriminatory, harmful practices when handling cases with Chinese Americans.

Hvistendahl, Mara. "The FBI's China obsession." The Intercept. 2/2/20. https://theintercept.com/2020/02/02/fbi-chinese-scientists-surveillance/

Lieu told me that in his view, institutional racism, not individual bias, is to blame for these encounters. "Most of the people who are doing the investigations are just following the guidance of the top boss," he said. "Everything is coming down, and they're just getting their marching orders to do this." The message from leadership, he said, is that "Chinese Americans are being weaponized as a tool by foreign nationals." FBI training materials obtained by the American Civil Liberties Union under the Freedom of Information Act in 2012 reveal approaches that are at best inadequate and at worst offensive. One presentation is sourced from "The Idiot's Guide" — presumably "The Complete Idiot's Guide to Modern China" — and titled "The Chinese."

**Analysis**: The government has been known to spy on its citizens, but the extent to which some are spied on more than others is largely unknown. Disproportionately, the NSA has been used to spy on those considered national security threats. Unfortunately, as the United States continues its relatively antagonistic relationship with China, this has resulted in Chinese Americans being treated as second class citizens by the surveillance state.

## PRO: NSA surveillance is an invasion of privacy.

**Argument**: While the right to privacy is not explicitly written out in the American constitution, it has become accepted as a foundation of American liberty. The NSA ignores that foundational right, and chooses to surveil on the basis of security.

**Warrant**: Newly released documents confirm that the NSA is violating our priacy,

> "Documents confirm how the NSA's surveillance procedures threaten Americans' privacy." ACLU. No date. https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy#:~:text=The%20Procedures%20allow%20the%20surveillance,foreigners%20outside%20the%20United%20States.&text=Because%20they%20have%20no%20right,including%20their%20communications%20with%20Americans.

Newly released documents confirm what critics have long suspected—that the National Security Agency, a component of the Defense Department, is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

The FISA Amendment Act, signed into law by President Bush in 2008, expanded the government's authority to monitor Americans' electronic communications. Critics of the law feared the NSA would use the law to conduct broad surveillance of Americans' international communications and, in the process, capture an unknown quantity of purely domestic communications. Government officials contended that the law authorized surveillance of foreign nationals outside the United States—not of Americans—and that it included robust safeguards to protect Americans' privacy. Last

year, in a successful effort to derail a constitutional challenge to the law, the Obama administration made these same claims to the U.S. Supreme Court.

**Evidence**: The NSA is lying about not listening to our calls or reading our emails.

"Documents confirm how the NSA's surveillance procedures threaten Americans' privacy." ACLU. No date. https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy#:~:text=The%20Procedures%20allow%20the%20surveillance,foreigners%20outside%20the%20United%20States.&text=Because%20they%20have%20no%20right,including%20their%20communications%20with%20Americans.

The NSA "is not listening to Americans' phone calls or monitoring their emails," the Chairman of the House Intelligence Committee recently said, and many other government officials, including the president himself, have made similar assurances. But these statements are not true. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. Indeed, in advocating for the Act, government officials made clear that these "one-end-domestic" communications were the ones of most interest to them. The Procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

**Warrant**: The government does not need probable cause or even suspicion to spy through the NSA.

> "Documents confirm how the NSA's surveillance procedures threaten Americans' privacy." ACLU. No date. https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy#:~:text=The%20Procedures%20allow%20the%20surveillance,foreigners%20outside%20the%20United%20States.&text=Because%20they%20have%20no%20right,including%20their%20communications%20with%20Americans.
>
> One of the fundamental problems with the Act is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who aren't even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." That term, though, is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The Procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA seems to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

**Impact**: Information is stored in a knowledge database, meaning

"Documents confirm how the NSA's surveillance procedures threaten Americans' privacy." ACLU. No date. https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy#:~:text=The%20Procedures%20allow%20the%20surveillance,foreigners%20outside%20the%20United%20States.&text=Because%20they%20have%20no%20right,including%20their%20communications%20with%20Americans.

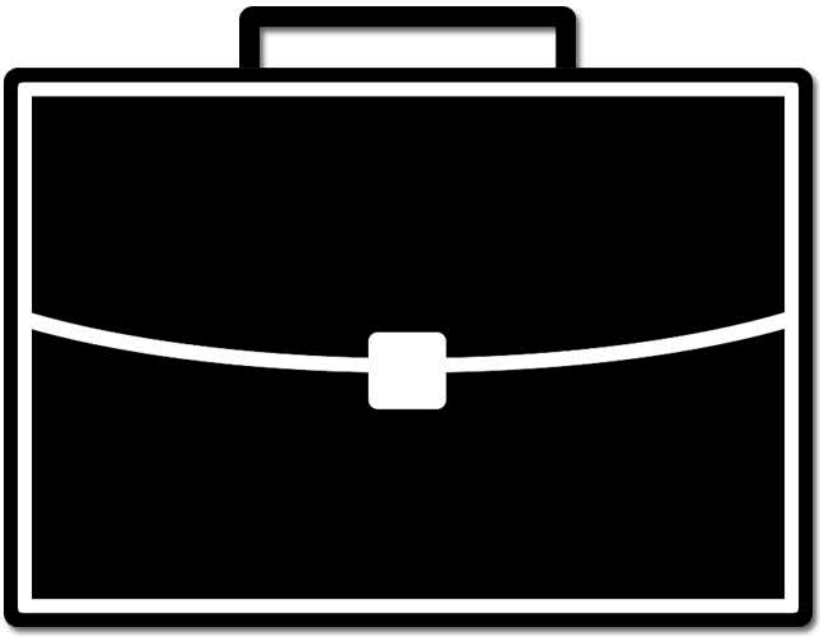
To determine whether a target is a foreigner abroad, the Procedures contemplate that the NSA will consult various NSA databases containing information collected by it and other agencies through signals intelligence, human intelligence, law enforcement, and other means. These databases—referred to as "NSA content repositories" and "knowledge databases"—apparently house internet data, including metadata that reveals online activities, as well as telephone numbers and email addresses that the agency has reason to believe are being used by U.S. persons. The Procedures' reference to "Home Location Registers," which receive updates whenever a phone "moves into a new service area," suggests that the NSA also collects some form of location information about millions of Americans' cellphones. The Procedures do not say what limits apply to these databases or what safeguards, if any, are in place to protect Americans' constitutional rights.

**Analysis**: The right to privacy holds value in and of itself, as a fundamental aspect of American liberty. The NSA chooses to ignore that under the veil of security, and Americans are left without any means of recourse.

# Champion Briefs

## January 2021

## Public Forum Brief



# Pro Responses to Con Arguments

## A/2: NSA will be critical to stopping cyber attacks

**Warrant:** America is already behind many other countries in cyberpreparedness.

O'Hanlan, Michael. 06-14-2017. "Cyber Threats and How the US Should Prepare." The Brookings Institute. 14 Jun. 2017. Web. 7 Dec. 2020. https://www.brookings.edu/blog/order-from-chaos/2017/06/14/cyber-threats-and-how-the-united-states-should-prepare/#

Cybersecurity is now at the forefront of policy discussions and planning for future conflicts. In many ways, the cyber threat has leveled the playing field, and that presents unique concerns to the United States and its allies**. The Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, released in February, concluded that cyber capabilities of other nations exceed U.S. ability to defend systems, and argued that this will continue to be the case for at least another five to 10 years.** With this in mind, a cyber strategy that can credibly deter potential foes is increasingly necessary, as are ways to keep critical systems defended. In both cases, progress has been slow and irregular

**Mitigation:** America is already experiencing the most cyberattacks of any country. Why haven't terrible impacts happened yet?

Specops Team. 07-13-2020. "The Countries Experiencing the Most Significant Cyber Attacks." Specops. 13 Jul. 2020. Web. 7 Dec. 2020. https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

**Specops Software found that the United States of America has experienced the most significant cyber-attacks, totalling 156 between the period of May 2006 and June 2020. In this time frame, 2018 was the worst year for cyber-attacks, with 30 incidents alone occurring throughout the year. One of the USA's most recent breaches, in May 2020, was brought to light by the National Security Agency (NSA), who found that Russian hackers were exploiting a bug in a commonly used email server to infiltrate sensitive data from American organisations.** Following the USA is the United Kingdom who have experienced the second-highest number of attacks between May 2006 and June 2020. Our research can reveal that the UK experienced 47 cyber-attacks classified as "significant" during this time, which included the large-scale cyber-attacks deployed across the Labour Party's digital platforms during the 2019 general election. India ranks in third place, falling prey to 23 significant cyber-attacks. In their latest cyber-attack, in June 2020, the country experienced a high-profile attack where malware was deployed against nine human rights activists to log their keystrokes, record their audio, and steal their personal credentials.

**Warrant:** Despite its efforts, the NSA still experiences frequent security breaches

Ken Dilanian, 6-30-2017, "Can the CIA and NSA be trusted with cyber hacking tools?," NBC News. 30 Jun. 2017. Web. 7 Dec. 2020. https://www.nbcnews.com/news/us-news/can-cia-nsa-be-trusted-cyber-hacking-tools-n778731

Some people would like the NSA to alert industry to every software hole it finds. But then, the former official said, the NSA would lose avenues for spying and attack. And hackers would still find holes to exploit, because such holes are inevitable. "We do have software vulnerabilities out there, and why shouldn't the NSA be in the business of helping to protect us by exploiting those things when necessary?" a second former official asked. **But one thing neither former official could answer is why the NSA has**

**continued to experience major breaches of classified material. First former NSA contractor Edward Snowden leaked some of the most sensitive secrets ever made public**. Then another contractor, Harold Martin, was accused of taking home reams of classified documents. Then the Shadow Brokers obtained the software flaws. Through it all, the same person, Kemp Ensor, has been head of security at the agency, according to his LinkedIn profile. The NSA did not respond to a request to make him available, and he did not respond to a message sent through LinkedIn. The success of the cyber attacks can't be blamed entirely on the U.S. government. After it learned of the Shadow Brokers leak, the NSA warned Microsoft and other companies, the former officials said. Microsoft released a patch in March designed to fix the flaw. But many companies and individuals failed to patch their systems. Those running outdated software may not even have been be able to.

**Warrant:** The threat of cyber attacks is not that large (study)

Jensen, Benjamin. 04-20-2018. "Cyber Warfare May Be Less Dangerous Than We Think." The Washington Post. 20 Apr. 2018. Web. 8 Dec. 2020. https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/26/what-can-cybergames-teach-us-about-cyberattacks-quite-a-lot-in-fact/

"Frankly, the United States is under attack." This February 2018 warning to the Senate from Director of National Intelligence Dan Coats included a message that "there should be no doubt" that Russia, emboldened by its 2016 cyberattacks and informational warfare campaign, will target the U.S. midterm elections this year. We agree. **However, our research suggests that, although states like Russia will continue to engage in cyberattacks against the foundations of democracy (a serious threat indeed), states are less likely to engage in destructive "doomsday" attacks against each other in cyberspace**. Using a series of war games and survey experiments, we found that cyber

operations may in fact produce a moderating influence on international crises. **Here's why: Cyberspace offers states a way to manage escalation in the shadows. Thus, cyber operations are more akin to the Cold War-era political warfare than a military revolution.**

**Analysis:** There are several strong ways to oppose this argument. The most compelling narrative is probably going to be forcing aff to prove when a cyber attack has been that harmful if they have been happening. If cyber attacks happen frequently with no consequence, then there really is not a benefit of keeping the NSA. Teams also may want to look more into the details of who exactly is responsible for cyber warfare. The Department of Defense is involved with some cyberoperations so there is a possibility that the NSA isn't totally relied upon for cyber protection.

## A/2: The NSA Prevents Terrorist Attacks

**Warrant:** Claims that NSA has prevented many terrorist attacks are overblown.

Cahall, Bailey. 6-5-2013, "Do NSA's Bulk Surveillance Programs Stop Terrorists?," New America. 5 Jun. 2013. Web. 8 Dec. 2020. https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

**However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading**. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and **NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.**

**Specific Response:** Coleman, Zari, and New York Stock Exchange examples are overblown

Cahall, Bailey. 6-5-2013, "Do NSA's Bulk Surveillance Programs Stop Terrorists?," New America. 5 Jun. 2013. Web. 8 Dec. 2020. https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

Additionally, **a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange.** In 28 percent of the cases we reviewed, court records and public reporting do not identify which specific methods initiated the investigation. These cases, involving 62 individuals, may have been initiated by an undercover informant, an undercover officer, a family member tip, other traditional law enforcement methods, CIA- or FBI-generated intelligence, NSA surveillance of some kind, or any number of other methods. In 23 of these 62 cases (37 percent), an informant was used. However, we were unable to determine whether the informant initiated the investigation or was used after the investigation was initiated as a result of the use of some other investigative means. Some of these cases may also be too recent to have developed a public record large enough to identify which investigative tools were used.

**Warrant: Study shows that the NSA does not prevent terrorist threats**

Nakashima, Ellen. 01-12-2014. “NSA phone record collection does little to prevent terrorist attacks, group says.” The Washington Post. 12 Jan. 2014. Web. 9 Dec. 2020. https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html

**An analysis of 225 terrorism cases inside the United States since the Sept. 11, 2001, attacks has concluded that the bulk collection of phone records by the National Security Agency "has had no discernible impact on preventing acts of terrorism."** In the majority of cases, traditional law enforcement and investigative methods provided the tip or evidence to initiate the case, according to the study by the New America Foundation, a Washington-based nonprofit group. The study, to be released Monday, corroborates the findings of a White House-appointed review group, which said last month that the NSA counterterrorism program "was not essential to preventing attacks" and that much of the evidence it did turn up "could readily have been obtained in a timely manner using conventional [court] orders."

**Warrant**: It is clear- Mass surveillance does not prevent terrorist attacks

Patrick G., 1-27-2015, "No, Mass Surveillance Won't Stop Terrorist Attacks," Cato Institute. 27 Jan 2015. Web. 9 Dec. 2020. https://www.cato.org/publications/commentary/no-mass-surveillance-wont-stop-terrorist-attacks

**But would more mass surveillance have prevented the assault on the Charlie Hebdo office? Events from 9/11 to the present help provide the Response:**

- **2009: Umar Farouk Abdulmutallab—i.e., the "underwear bomber"—nearly succeeded in downing the airline he was on over Detroit because, according to then-National Counterterrorism Center (NCC) director Michael Leiter, the federal Intelligence Community (IC) failed "to connect, integrate, and fully understand the intelligence" it had collected.**
- 2009: Army Major Nidal Hasan was able to conduct his deadly, Anwar al-Awlaki-inspired rampage at Ft. Hood, Texas, because the FBI bungled its Hasan investigation.
- **2013: The Boston Marathon bombing happened, at least in part, because the CIA, Department of Homeland Security (DHS), FBI, NCC, and National Security Agency**

**(NSA) failed to properly coordinate and share information about Tamerlan Tsarnaev and his family, associations, and travel to and from Russia in 2012. Those failures were detailed in a 2014 report prepared by the Inspectors General of the IC, Department of Justice, CIA, and DHS.**

- 2014: The Charlie Hebdo and French grocery store attackers were not only known to French and U.S. authorities but one had a prior terrorism conviction and another was monitored for years by French authorities until less than a year before the attack on the magazine. **No, mass surveillance does not prevent terrorist attacks**

**Analysis:** The most effective way to counter this argument is by directly countering the claim that the NSA has stopped terrorist attacks. There are many sources that suggest government accounts of how many terrorist threats the NSA has stopped are exaggerated at best and factually incorrect at worst. If neg teams can prove that aff's claims are untrue, then they strip aff of any proof of efficacy from their argument, meaning that they are arguing for an organization that has never proved to be effective against what it works against.

## A/2: NSA Surveillance Maintains Safety

**Warrant:** Government surveillance leads to over surveillance

K.N.C., 12-13-2019, "Open Future," The Economist. 13 Dec. 2019. Web. 9 Dec. 2020. https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

**Perhaps the most recognizable danger inherent to overt surveillance is that it causes individual inhibition and self-censorship. When people are aware that they are being watched, they tend to alter their behavior to fit what they believe to be general expectations of "normal behavior" so as not to draw attention to themselves.** This self-censorship often occurs even if a person is not doing anything wrong. […] Physical surveillance gives watchers access to a subject's speech or acts, which technology allows them to reproduce. In this regard it differs from data surveillance. People take more care in their writing than they do with their impromptu speech and actions. Casual speech often includes offhand comments, partial observations, sarcasm, and false sentiments to either avoid argument or draw a subject out. To have such conversations made public is potentially catastrophic to an individual's reputation.

**Turn:** NSA risks safety of Americans

Hooper, Charles 1-6-2014, "NSA Surveillance: A Cost/Benefit Analysis," Econlib. 6 Jan. 2014. Web. 8 Dec. 2020. https://www.econlib.org/library/Columns/y2014/Hoopersurveillance.htm

The benefit of the NSA's surveillance is a reduction in the small probability of high-cost events. **Ironically, the NSA's spying activities introduce other low-probability, high-cost events, including the following:**

**1. People with evil intentions, such as spammers, scam artists, hackers, and members of foreign governments, might eventually tap into and abuse the data the NSA has meticulously collected and organized.**

2. The NSA itself might abuse this sensitive data: we already know that at least a dozen NSA employees have abused secret surveillance programs in the past decade, most often to spy on their significant others.**6**

3. The data could be used for political advantage. The IRS recently harassed various Tea Party groups. Indeed, the IRS has been repeatedly used for political persecution since at least FDR's presidency.**7** If the IRS can be used as a political weapon, so can the NSA.

4. Freedom of the press could be at stake. In May, the Justice Department admitted that it secretly seized phone records from The Associated Press.**8** Certainly, it's not hard to imagine the NSA handing over personal information about reporters to the Justice Department or even intimidating reporters who write critically about the NSA or the government as a whole.

5. The NSA's spying might lead to anti-American reactions abroad—some of which has already happened after the spying on German Chancellor Angela Merkel—hurting this country both politically and economically.

6. Revelations about NSA spying could spur the splintering of the Internet. American and foreign companies, along with numerous foreign governments, are alarmed at the depth of the U.S. government's penetration into the Internet and the cell phone network. Concern about the possible abuse of this power has spurred talk of a "splinternet" in which the Internet is Balkanized.**9** In the vanguard of this effort is Brazilian President Dilma Rouseff, who was surprised to learn that the NSA had been reading her private emails.**10**

**Mitigation:** There is not that high of a risk associated with threats

Hooper, Charles L. 1-6-2014, "NSA Surveillance: A Cost/Benefit Analysis," Econlib. 6 Jan, 2014. Web. 9 Dec. 2020. https://www.econlib.org/library/Columns/y2014/Hoopersurveillance.htm

Back to that other alphabet agency, the NSA. The question of NSA spying is intertwined with the issue of terrorism. **If terrorism poses a huge threat to Americans, then spying might be justified. But, in reality, how dangerous is terrorism? Not very, according to John Mueller: Even with the September 11 attacks included in the count, the number of Americans killed by international terrorism since the late 1960s (which is when the State Department began counting) is about the same as the number of Americans killed over the same period by lightning, accident-causing deer, or severe allergic reaction to peanuts.3** Still, many Americans persist in their fear of flying even though, statistically, one September 11-like disaster would need to occur each month for the risk of flying to equal the risk of driving—something we do daily without much concern.**4 And a September 11-like hijacking is much less likely now that flight crews and passengers have learned that passivity equals death.In addition to airplane hijackings, other possible terrorist techniques are also ineffective against a large number of American**s. For all the fear they induce in the population, radiological, chemical, and biological bombs are unlikely to kill large numbers of people.**5**

**Warrant:** NSA harms internet privacy

Patrick Toomey,, 8-22-2018, "The NSA Continues to Violate Americans' Internet Privacy Rights,"AmericanCivilLibertiesUnion.22Aug2018.Web.9Dec2020.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 systematically combs through its 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 — i**ncluding 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, 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 Americans' online communications receive the full protection of the Fourth Amendment.

**Analysis:** There is a bounty of information for neg teams to use if aff teams claim that the NSA protects citizens. You can counter it in many ways: mitigate the offense, try to turn it, or use link defense. Just about every specific example of NSA benefits has a response about how that claim is overblown. Strategic neg teams should listen carefully to aff teams who read this argument to find the most compelling and responsive arguments to read in rebuttal.

## A/2: The NSA is good for the economy

**Warrant:** The NSA costs an obscene amount of money

Jeanne Sahadi, 6-7-2013, "What the NSA Costs Taxpayers" CNNMoney. 7 Jun. 2013. Web. 9 Dec. 2020. https://money.cnn.com/2013/06/07/news/economy/nsa-surveillance-cost/index.html

As a result, it's impossible to say exactly how much money the NSA is given to conduct its surveillance efforts -- which Americans learned this week has recently included collecting phone call data and monitoring online activities. That's because the NSA, a Defense Department agency created in 1952, falls under the category of a "black" program in the federal budget, a term applied to classified efforts. The NSA is one of at least 15 intelligence agencies, and combined the total U.S. intelligence budget in 2012 was $75 billion, said Steve Aftergood, director of the government secrecy program at the Federation of American Scientists, a nonpartisan think tank that analyzes national and international security issues. **The intelligence budget includes funding for both classified and unclassified activities. Funding for classified programs has tracked the upward trend in defense spending over the past decade,** according to an analysis of fiscal year 2012 Defense Department budget request by Todd Harrison of the Center for Strategic and Budgetary Assessments. **Aftergood estimates about 14% of the country's total intelligence budget -- or about $10 billion -- goes to the NSA.**

**Warrant:** There is no way the NSA formulas are cost effective

Hooper, Charles 1-6-2014, "NSA Surveillance: A Cost/Benefit Analysis," Econlib. 6 Jan. 2014. Web. 8 Dec. 2020. https://www.econlib.org/library/Columns/y2014/Hoopersurveillance.htm

**For every true terrorist uncovered, the NSA would incorrectly flag 475,50014 innocent American residents. With the NSA budget of $5 million per terrorist ($5 billion divided by 1,000) and a follow-up cost of $30,000 per accused, the marginal cost per real terrorist is over $14 billion, which is far above the marginal value per terrorist of $100 million.** Notice that even if one assumes a zero budget for the NSA, the marginal cost per real terrorist is still over $14 billion. The big driver of costs is not the NSA budget, but the cost of incorrectly flagging 475,500 innocent American residents for every true terrorist. To put this into perspective, if the goal were to find all 1,000 terrorists, 475.5 million innocent people would be flagged as terrorists, and the total follow-up costs would equal $14 trillion. **There are not enough American residents to accuse—there are only 317 million of us—and the U.S. GDP is only $15.7 trillion. Simply accusing everyone in the country would achieve the same result and allow the federal government to save $5 billion per year on the NSA's budget.** In other words, if the NSA persists in using inaccurate tests that, because of their high false-positive rates, end up accusing every American of being a terrorist, then we can simply accuse everyone right away and avoid the suspense and hassle. Perhaps the NSA's tests are more accurate. With a sensitivity and specificity of 80 percent and the other assumptions unchanged, the PPV is 0.00126 percent. That means that for every true terrorist uncovered, the tests would incorrectly flag 79,250 innocent Americans. The total follow-up costs would be almost $2.4 billion, which is still far above the value per terrorist of $100 million. The NSA budget per terrorist would still be rounding error.

**Warrant:** The NSA loses money and directly harms foreign business

Danielle Kehl, 07-31-2014, "How the NSA Hurts Our Economy, Cybersecurity, and Foreign Policy," Slate Magazine. 31 Jul. 2014. Web. 9 Dec. 2020. https://slate.com/technology/2014/07/usa-freedom-act-update-how-the-nsa-hurts-our-economy-cybersecurity-and-foreign-policy.html

Meanwhile, evidence of the costs continues to pile up. This week, two new reports were published that demonstrate how surveillance reform is needed to protect fundamental rights here in the U.S. An in-depth study conducted by the American Civil Liberties Union and Human Rights Watch documents how mass surveillance undermines press freedom, the right to legal counsel, and other essential elements of a healthy democracy**. And a separate report from New America's Open Technology Institute examines how the NSA's programs are bad for the U.S. economy,** American foreign policy, and the security of the Internet as a whole. (Full disclosure: I am the primary author of the second paper; Future Tense is a partnership of Slate, New America, and Arizona State University.) It's easy to get caught up in the simplistic debate that often dominates the surveillance conversation: that this is about balancing national security and individual privacy. But the binary argument over security vs. privacy ignores the other negative impacts of NSA surveillance on our national interests. **The U.S. cloud computing industry—a fast-growing and American-dominated market—could lose anywhere from $22 billion to $180 billion in the next few years as companies lose customers abroad and here at home. U.S. tech companies are facing declines in overseas sales due to the backlash, while foreign governments are blaming the NSA for decisions to drop American companies from huge contracts, as we've witnessed with Boeing in Brazil and Verizon in Germany.**

**Warrant:** A recent NSA investigation cost serious many and yielded almost no benefits.

Charlie Savage, 2-25-2020, "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads," The New York Times, 25 Feb. 2020. Web. 9 Dec. 2020. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html?auth=login-email&login=email

**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, w**hich 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.

**Analysis:** Once again, the difficulty in responding to this argument is in selecting what to read. Neg teams should be ready to contest the idea that) the NSA prevents terrorist attacks and therefore saves money long term and b) if any small communities that benefit from the NSA outweigh all the others. Teams should focus on forming a cohesive narrative that is ready for judges to understand.

## A/2: Surveillance can stop the spread of COVID-19

**Nonunique:** Vaccines are already solving for the pandemic.

**Warrant:** Pfizer's COVID vaccine was recently approved by the FDA.

Thomas, Katie, et al. "F.D.A. Advisory Panel Gives Green Light to Pfizer Vaccine." The New York Times, 10 Dec. 2020, www.nytimes.com/2020/12/10/health/covid-vaccine-pfizer-fda.html.

**Pfizer's Covid-19 vaccine passed a critical milestone on Thursday when a panel of experts formally recommended that the Food and Drug Administration authorize the vaccine.** The agency is likely to do so within days, giving health care workers and nursing home residents first priority to begin receiving the first shots early next week. The F.D.A.'s vaccine advisory panel, composed of independent scientific experts, infectious disease doctors and statisticians, voted 17 to 4, with one member abstaining, in favor of emergency authorization for people 16 and older. With rare exceptions, the F.D.A. follows the advice of its advisory panels.

**Warrant:** If the vaccine is successful, there could be normalcy by summer.

Thomas, Katie, et al. "F.D.A. Advisory Panel Gives Green Light to Pfizer Vaccine." The New York Times, 10 Dec. 2020, www.nytimes.com/2020/12/10/health/covid-vaccine-pfizer-fda.html.

The initial shipment of 6.4 million doses will leave warehouses within 24 hours of being cleared by the F.D.A., according to federal officials. About half of those doses will be sent across the country, and the other half will be reserved for the initial recipients to receive their second dose about three weeks later. **The arrival of the first vaccines is**

> **the beginning of a complex, monthslong distribution plan coordinated by federal and local health authorities, as well as large hospitals and pharmacy chains, that if successful, will help return a grieving and economically depressed country back to some semblance of normal, maybe by summer.** "With the high efficacy and good safety profile shown for our vaccine, and the pandemic essentially out of control, vaccine introduction is an urgent need," Kathrin Jansen, a senior vice president and the head of vaccine research and development at Pfizer, said at the meeting.

**Analysis:** This argument can be weighed on timeframe as a prerequisite. If the vaccine results in herd immunity and people no longer contract COVID in mass numbers, there won't be any need for contact tracing through government surveillance.

**Delink:** The U.S. has greater respect for privacy than other countries and wouldn't turn to the same surveillance techniques to contact trace.

**Warrant:** 71% of Americans say they won't use COVID-19 contact tracing apps.

> Jercich, Kat. "Survey Says Majority of Americans Won't Use COVID-19 Contact-Tracing Apps." Healthcare IT News, 16 June 2020, www.healthcareitnews.com/news/survey-says-majority-americans-wont-use-covid-19-contact-tracing-apps.

> **According to a study commissioned by the security software vendor Avira, 71% of Americans say they won't use COVID-19 contact-tracing apps, with many citing potential privacy and security issues.** Government and healthcare professionals were the least likely to say they'd download the apps, and about three-quarters of people surveyed believed their digital privacy would be at risk if data were stored centrally so the government and other authorities could access it.

**Warrant:** Disease surveillance can chill the public's willingness to seek treatment and breed mistrust.

> Domino, Albert Fox Cahn and Alyssa. "Tracking Everyone's Whereabouts Won't Stop COVID-19." Fast Company, 6 Apr. 2020, www.fastcompany.com/90486342/tracking-everyones-whereabouts-wont-stop-covid-19.
>
> And even if some types of surveillance did help abroad, it's not certain that broad-based cellphone tracking or other invasive measures would be effective in the U.S. For example, it's unknown how broad-based surveillance impacts voluntary compliance with social distancing and quarantine requirements. As the government seeks greater visibility into the public's movements, many Americans will seek to evade public monitoring for reasons wholly unrelated to COVID-19. **These tools can backfire, driving people into the shadows and chilling the public's willingness to seek medical treatment. And just as importantly, draconian surveillance tools can foster an adversarial dynamic between the public and health authorities, undermining public support for, and compliance with, social distancing mandates.**

**Analysis:** This argument can be weighed on probability. The pandemic has been going on for months and months, yet the government hasn't turned to surveillance yet. The likelihood that the Biden administration decides to roll out a controversial surveillance program with a vaccine already on the way is low.

## A/2: Reforming NSA surveillance is preferable to ending it

**Delink:** Meaningful reform hasn't been enacted.

**Warrant:** Reforms have not reined in mass surveillance.

Pitter, Laura. "US: It's Been a Year Since Snowden, and Nothing's Really Changed." Human Rights Watch, 5 June 2014, www.hrw.org/news/2014/06/05/us-its-been-year-snowden-and-nothings-really-changed.

What we've seen far too little of over the past year is any real change. In the wake of the Edward Snowden leaks, the United States has denied some of the allegations, and disclosed -- under pressure -- a tiny bit of information about some of its programs. But **very little has been done to rein in the surveillance itself. The few proposed reforms we have seen have been so watered down that none come close to adequately restraining the government's capacity for mass electronic surveillance.** But first, a brief review: In the past year, we've learned that not only is our telephone data collected -- our Internet communications are under watch. Stunning amounts of data are being collected under the government's interpretation of the Foreign Intelligence Surveillance Act (FISA). U.S. Internet companies turn over the content of communications like texts, emails, videos, and chat messages, under Section 702 of FISA, which authorizes the warrantless collection -- inside American borders -- of communications containing "foreign intelligence information," a term defined to include essentially anything about the foreign affairs of the United States -- so long as at least one person on the end of the communication is located outside the country.

**Warrant:** Some reforms have had the opposite of their intended effect.

Hattem, Julian. "Spying after Snowden: What's Changed and What Hasn't." TheHill, 25 Dec. 2016, thehill.com/policy/technology/310457-spying-after-snowden-whats-changed-and-what-hasnt.

Snowden's leaks can be directly connected to only one new law, which ended the NSA's bulk collection of Americans' phone records, among other changes. However, b**y requiring the NSA to go to private phone companies when seeking data, Congress likely ended up expanding the information available to the spy agency, as lawmakers such as Sen. Ted Cruz (R-Texas) have argued. Under the previous system, the NSA reportedly had trouble acquiring records from cellphones. Now it is able to obtain them with a court order**. The records detail the numbers involved in a phone call, when it occurred and how long it lasted, but do not include the content of the conversations. Overseas, the legal response to Snowden has been more pronounced — although in some places, the movements have been to solidify government surveillance powers, not undo them.

**Analysis:** This response can be weighed on probability. If meaningful reform hasn't been enacted in the years since Snowden, the likelihood that it will be now is slim to none. NSA spying also hasn't been in the news cycle lately, making it unlikely the Biden administration will feel pressured to make changes.

**Response:** The NSA cannot be held accountable.

**Warrant:** Classified material gets in the way of holding the NSA accountable.

Tien, Lee. "Why The NSA Can't Be Trusted to Run U.S. Cybersecurity Programs." Electronic Frontier Foundation, 30 July 2012, www.eff.org/deeplinks/2012/07/why-nsa-cant-be-trusted-run-us-cybersecurity-programs.

For example, last month a federal judge in California threw out a case challenging the agency's bulk collection of Internet data after finding that the plaintiffs' version of significant operational details of the Upstream collection process was inaccurate. But **the judge said he couldn't reveal what the inaccuracies were because that would harm national security. In effect the court ruled that even though the plaintiffs' communications may have been intercepted, the case couldn't proceed unless they could show how the surveillance worked — something they could not know since that information is classified. Such slippery conundrums seem to keep popping up to block every effort to hold the NSA accountable for its activities**, which doesn't bode well for the ACLU's latest lawsuit. Nonetheless, it's an effort that must be made if we are ever to enforce limits on what data the government can collect in our name.

**Warrant:** The NSA is exempt from the Freedom of Information Act.

The Baltimore Sun. "Can the NSA Be Checked?" Www.Govtech.com, 12 Mar. 2015, www.govtech.com/opinion/Can-the-NSA-be-Checked.html.

NSA keeps much of what it does classified and secret. Because cybersecurity policy is inescapably tied to our online civil liberties, it's essential to maximize government transparency and accountability here. The NSA may be the worst government entity on this score. **Much of the NSA's work is exempt from Freedom of Information Act (FOIA) disclosure because Congress generally shielded NSA activities from FOIA2. Even aside from specific exemption statutes, much information about NSA activities is classified on national security grounds.** The NSA has also stonewalled organizations trying to bring public-interest issues to light by claiming the "state secrets" privilege in court. EFF has been involved in lawsuits challenging the NSA's warrantless surveillance program since 2006. Despite years of litigation, the government continues to maintain that the

"state secrets" privilege prevents any challenge from being heard. Transparency and accountability simply are not the NSA's strong suit.

**Analysis:** This response can be weighed on probability. Because of the NSA's numerous exemptions from typical accountability measures due to its dealings with classified information, the likelihood that it will ever truly be held accountable without completely abolishing domestic surveillance programs is low.

## A/2: NSA surveillance is preferable to FBI surveillance

**Nonunique:** The FBI can already access surveillance data.

**Warrant:** The FBI has facial recognition technology.

The American Civil Liberties Union. "The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database." American Civil Liberties Union, 2019, www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through.

1. **The FBI's massive facial recognition apparatus continues to expand and can now match against over 640 million photos.** The FBI now has the ability to match against or request matches against over 640 million photos — a number that Rep. Jim Jordan (R-Ohio) noted is larger than the total population in the US. This includes driver's license photos from 21 states, including states that do not have laws explicitly allowing their driver's license repositories to be used in this way. **These numbers show that the FBI is moving closer to having the capability to run face recognition searches against photos of virtually every American.**

**Warrant:** The FBI already has access to NSA data.

Lindsey, Nicole. "FISA Court Ruled That FBI Improperly Used NSA Surveillance Data to Snoop on Americans." CPO Magazine, 15 Oct. 2019, www.cpomagazine.com/data-privacy/fisa-court-ruled-that-fbi-improperly-used-nsa-surveillance-data-to-snoop-on-americans/.

According to a new declassified ruling from the U.S. Foreign Intelligence Surveillance Court (FISC), **FBI personnel systematically abused National Security Agency (NSA) mass**

**surveillance data in both 2017 and 2018.** The 138-page ruling, which dates back to October 2018, was only unsealed 12 months later in October 2019. It offers a rare look at how the Federal Bureau of Investigation (FBI) has been abusing the constitutional privacy rights of U.S. citizens with alarming regularity. The court ruling is also a stinging rebuke to the FBI's overreach of its ability to search surveillance intelligence databases.

**Analysis:** This response can be used to mitigate the con's impact. If the FBI already has access to surveillance data, there's not much more that can be done to increase their power.

**Response:** The NSA is no better than the FBI.

**Warrant:** NSA analysts have deliberately ignored restrictions.

Gallagher, Ryan. "Obama Was Wrong: NSA Employees Have Deliberately 'Abused' Their Power." Slate Magazine, 23 Aug. 2013, slate.com/technology/2013/08/bloomberg-report-nsa-employees-have-deliberately-abused-their-power.html.

On Friday, Bloomberg reported that **NSA analysts have "deliberately ignored restrictions on their authority to spy on Americans multiple times in the past decade."** According to Bloomberg, an average of one case of intentional abuse per year has been documented in internal reports. Given that the NSA intercepts billions of communications weekly, the number of reported deliberate abuses is small. However, that there are any documented cases at all is highly significant because of how this contradicts statements made by both current and former senior officials in the aftermath of a series of stories about vast NSA spy programs based on leaked secret documents.

**Warrant:** The NSA uses PRISM as a backdoor into Americans' private communications.

"The NSA Continues to Violate Americans' Internet Privacy Rights." American Civil Liberties Union, 2018, www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

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 communications, 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 review 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 government has admitted to the spying.

**Analysis:** This response can be weighed on probability. We already know the NSA has abused its power to invade privacy in the past; the likelihood they do so again in the future — especially without the checks and balances of other government agencies — is high.

## A/2: Ending NSA surveillance props up Big Tech

**Response:** Big Tech wants to protect customer privacy.

**Warrant:** Repeated stories on privacy invasions have heightened customers attention to security.

Telang, Rahul. "In FBI versus Apple, Government Strengthened Tech's Hand on Privacy." The Conversation, 25 Feb. 2016, theconversation.com/in-fbi-versus-apple-government-strengthened-techs-hand-on-privacy-55353.

Not too long ago, everyone seemed to be bemoaning that companies aren't doing enough to protect customer security and privacy. The White House, for example, published a widely cited report saying that the lack of online privacy is essentially a market failure. It highlighted that users simply are in no position to control how their data are collected, analyzed and traded. Thus, a market-based approach to privacy will be ineffective, and regulations were necessary to force firms to to protect the security and privacy of consumer data. **The tide seems to have turned. Repeated stories on data breaches and privacy invasion, particularly from former NSA contractor Edward Snowden, appears to have heightened users' attention to security and privacy. Those two attributes have become important enough that companies are finding it profitable to advertise and promote them. Apple, in particular, has highlighted the security of its products recently and reportedly is doubling down and plans to make it even harder for anyone to crack an iPhone.** Whether it is through its payment software or operating system, Apple has emphasized security and privacy as an important differentiator in its products. Of course, unlike Google or Facebook, Apple does not make money using customer data explicitly. So it may have more incentives than others to incorporate these features. But it competes directly with Android and naturally plays

an important role in shaping market expectation on what a product and service should look like.

**Warrant:** Trust and profit go hand-in-hand.

Whittaker, Zack. "Should Tech Giants Slam the Encryption Door on the Government?" TechCrunch, 22 Jan. 2020, techcrunch.com/2020/01/22/should-tech-giants-slam-the-encryption-door-on-the-government/.

Tech companies are within their rights — both legally and morally — to protect their customers' data from any and all adversaries, using any legal methods at their disposal. **Apple is a great example of a company that doesn't just sell products or services, but one that tries to sell you trust — trust in a device's ability to keep your data private. Without that trust, companies cannot profit.** Companies have found end-to-end encryption is one of the best, most efficient and most practical ways of ensuring that their customers' data is secured from anyone, including the tech companies themselves, so that nobody other than the owner can access it. That means even if hackers break into Apple's servers and steal a user's data, all they have is an indecipherable cache of data that cannot be read.

**Analysis:** This response mitigates the probability of the con's link. If Big Tech is not incentivized to share information with the government because of a financial incentive to protect customer privacy, privacy violations will be lessened when the NSA ends its surveillance programs.

**Delink:** Big Tech has not historically cooperated with the government.

**Warrant:** Big Tech has been pushing back on government overreach through litigation.

Margaret Jane Radin. "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance." Harvardlawreview.org, 10 Apr. 2018, harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

These are just a few examples of major face-offs between surveillance intermediaries and the government, demonstrating the existence of a resistant band of technology companies fighting against perceived government overreach. **The rise of intermediary-initiated litigation paints a much more optimistic picture of surveillance intermediaries. It indicates that major technology companies are critically reviewing the legal orders they receive from the government and pushing back on government overreach when necessary.** This resistance might make us foster confidence in our data stewards and the surveillance intermediary system.

**Warrant:** Apple refused to unlock iPhones for the government.

Margaret Jane Radin. "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance." Harvardlawreview.org, 10 Apr. 2018, harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

A third incentive behind intermediary decisionmaking lies in the business model of each company. A surveillance intermediary will be incentivized to act in a way that promotes its own business model — and, better yet, a way that distinguishes its business model from that of its competitors. **Consider Apple's 2016 challenges to the government's use of the All Writs Act to compel Apple's assistance in unlocking iPhones for two government investigations.** Because Apple encrypts all iPhone data, unlocking an iPhone is the only expedient way for the government to gain access to its contents.The All Writs Act is used to "fill[] gaps where Congress has been silent," allowing a court to

issue writs it “might need to effectuate its judgments.” Nonetheless, it successfully challenged the use of the All Writs Act in the Eastern District of New York for a narcotics case, Although Apple’s challenge in the Central District of California was cut short when the government obtained an alternate means of unlocking the iPhone in question, the case generated significant publicity and started a nationwide conversation about the balance between privacy and security.

**Analysis:** This response also mitigates the probability of the con’s link. Big Tech has not historically shared information with the government. The likelihood that they do so when the government ends its own surveillance programs is low.

## A/2: NSA surveillance enables offensive cyber operations

**Turn:** Offensive Cyber Operations trigger retaliation and escalate conflict.

**Warrant:** U.S. attacks could trigger a response on a previously unseen scale.

Olejnik, Lukasz. "Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations, 2019, www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict.

Domestically, Russia is currently already in the process of isolating its networks from the outside internet. Russia's official justification for the action is to lower the risk of external cyberattacks; however, in reality the goal is to increase control over the networks, including strict traffic filtering, reminiscent of the China's Great Firewall. While Russia's narrative rings hollow, U.S. reports of cyberattacks on Russia may be exploited internally to justify the changes. **There is also the danger of a retaliation. While Russia could simply limit its response to a diplomatic message, the standard previously followed by the United States, escalation in response to the November action might follow, potentially on a previously unseen scale.** Intensifying cyber conflict would not only seriously impact national security, but also increase geopolitical risk for businesses.

**Warrant:** A preemptive or disproportionate attack could easily escalate.

Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired, WIRED, 18 June 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/.

But security wonks tend to agree, at least, that **there's one way not to prevent a cyberwar: launching a preemptive or disproportionate cyberattack on an opponent's**

> **civilian infrastructure. As the Trump administration increasingly beats its cyberwar drum, some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it.** Over the past weekend, The New York Times reported that US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.

**Analysis:** This turn can be weighed on probability. The likelihood that our adversaries sit idly by in the face of offensive cyber operations, rather than retaliate, is low. Countries like Russia and China are incentivized to retaliate because they derive legitimacy from attacking and scapegoating the U.S.

**Turn:** Offensive Cyber Operations erode international cyber norms.

**Warrant:** U.S. offensive operations allow other countries to claim their offensive hacking is acceptable.

Marks, Joseph. “Analysis | The Cybersecurity 202: Trump Gave the Military Freer Rein for Offensive Hacking. Security Experts Say That’s a Good Idea.” The Washington Post, 11 Feb. 2019, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/11/the-cybersecurity-202-trump-gave-the-military-freer-rein-for-offensive-hacking-security-experts-say-that-s-a-good-idea/5c607a571b326b66eb098678/.

More broadly, former White House cybersecurity coordinator Michael Daniel worried that **U.S. cyber strikes would allow adversary nations to claim their offensive hacking is acceptable behavior. "We don't have a monopoly on these capabilities and any offensive action we take legitimizes such actions -- meaning another nation could take the same action against us. We are especially vulnerable to disruption through cyberspace,**" said Daniel who is now president of the Cyber Threat Alliance, a cybersecurity information sharing group. "Therefore, we need to use this tool carefully and judiciously[.]"

**Warrant:** U.S. hypocrisy makes norms unenforceable.

Farrell, Henry. "Why It's so Hard to Create Norms in Cyberspace." The Washington Post, 6 Apr. 2015, www.washingtonpost.com/news/monkey-cage/wp/2015/04/06/why-its-so-hard-to-create-norms-in-cyberspace/.

**Second – the U.S.'s own commitment to many of its values has been called into question.** The Snowden revelations appear to show, for example, that the NSA has tried to compromise basic cryptographic standards that are required for an open and robust Internet to work. **This makes it hard for the U.S. to be an effective advocate for its norms. Some degree of hypocrisy is tolerable in international politics when others can turn a blind eye to it. However, when one's secrets have been leaked, other states may neither want to, nor be able to, ignore the difference between the U.S.'s lofty normative aspirations, and its self-interested behavior. The result, all too often, is battles over norms where neither side is likely to persuade the other.** For example, the U.S. and China are facing off over commercial cyber-espionage aimed to grab the trade secrets of firms located in other countries, and pass them on to one's own businesses.

**Analysis:** This argument can be weighed on scope and magnitude. The erosion of cyber norms has global impacts on cyberspace. Cyberwarfare will also be significantly worse in a world without clearly established norms.

## A/2: The NSA surveillance program is well regulated

**Response:** Regulations placed upon the NSA are simply not enough – the organization has proven that it can't safely handle personal data.

**Warrant:** Hacking from other governments into US data bases is on the rise.

Sobers, Rob. "Hacking Exploits, Examples and Prevention Tips". Varonis. 8 Sept 2020. https://www.varonis.com/blog/government-hacking-exploits/

> **"Government hacking exploits, unfortunately, pose a very real threat for organizations of all kinds,** and those of us working in cybersecurity need to be aware of it. **A decade ago, the majority of government-sponsored attacks were launched against other governments, and most aimed at demonstrating a state's capabilities rather than causing real disruption.** There are now signs that this is changing**: governments around the world have ramped up cyber operations** and are increasingly targeting commercial organizations. **In just the last few months, we have seen many government hacking attempts. July 2020. Canada, the UK, and the U.S. announced that hackers associated with Russian intelligence had attempted to steal information related to COVID-19 vaccine development. July 2020. Media reports say a 2018 Presidential finding authorized the CIA to cyber operations against Iran, North Korea, Russia, and China.** The operations included disruption and public leaking of information**. June 2020. Suspected North Korean hackers compromised at least two defense firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defense contractors."**

**Warrant:** US Citizens have little faith that the government can protect their information from being stolen.

Pew Research. "The State of Privacy in Post-Snowden America." Pewresearch.org. 21 Sept 2016. https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

**"Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them – particularly when it comes to the use of online tools. And they exhibited a deep lack of faith in organizations of all kinds, public or private, in protecting the personal information they collect.** Only tiny minorities say they are "very confident" that the records maintained by these organizations will remain private and secure."

**Analysis:** Even if the NSA imposes restrictions upon itself, that doesn't do anything to stop nefarious individuals who find the information. The NSA's security is simply not good enough to justify the risk.

## A/2: The NSA is essential to stopping Chinese cyberattacks

**Response:** Spying on permanent residents from China disproportionately is discrimination.

**Warrant**: The government has been known to use the surveillance state to keep track of Chinese Americans.

> Hvistendahl, Mara. "The FBI's China obsession." The Intercept. 2/2/20. https://theintercept.com/2020/02/02/fbi-chinese-scientists-surveillance/
>
> As Chinese American scientists returned to visit long-lost friends and relatives, the bureau closely tracked them.
> In 1972, Jen led a delegation of Chinese American scientists and their families to China. Katherine Yih, who joined her father on the trip, recalled a highly orchestrated tour that included visiting agricultural communes and watching children's dance performances. "We were being shown the successes of the revolution," she said. The visitors were seen as important enough that they were also taken to meet Premier Zhou Enlai, a development that almost certainly heightened the suspicions of U.S. counterintelligence operatives.

**Impact**: The surveillance state engages in discriminatory, harmful practices when handling cases with Chinese Americans.

> Hvistendahl, Mara. "The FBI's China obsession." The Intercept. 2/2/20. https://theintercept.com/2020/02/02/fbi-chinese-scientists-surveillance/
>
> Lieu told me that in his view, institutional racism, not individual bias, is to blame for these encounters. "Most of the people who are doing the investigations are just following the guidance of the top boss," he said. "Everything is coming down, and

> they're just getting their marching orders to do this." The message from leadership, he said, is that "Chinese Americans are being weaponized as a tool by foreign nationals." FBI training materials obtained by the American Civil Liberties Union under the Freedom of Information Act in 2012 reveal approaches that are at best inadequate and at worst offensive. One presentation is sourced from "The Idiot's Guide" — presumably "The Complete Idiot's Guide to Modern China" — and titled "The Chinese."

**Analysis**: Regardless of whether the government of China wishes to launch a cyber offensive against the United States, that would not justify ignoring individual liberties. Even if it was the case that some permanent residents are a threat, the majority are not and going after them simply because of their country of origin is discrimination.

## A/2: The NSA stops radical anti-government groups

**Response:** The NSA is also involved with surveillance of activists and organizers. For every extremist group they target, they also target many legitimate groups as well.

**Warrant**: The NSA can collect vast amounts of data on disfavored communities.

> Yachot, Noa. "History shows activists should fear the surveillance state." ACLU. 10/27/17. https://www.aclu.org/blog/national-security/privacy-and-surveillance/history-shows-activists-should-fear-surveillance
>
> Under Section 702 of the Foreign Intelligence Surveillance Act, the National Security Agency collects vast amounts of phone calls, emails, text messages, and more from Americans communicating with people overseas, often sweeping up domestic communications in the process — all without individualized warrants from a court. Government agencies can then search through that data for information about anyone, in a subversion of judicial protections meant to prevent abuse of government powers. The threat that these protections guard against isn't theoretical. Recent history clearly shows that the burden of overzealous surveillances falls on disfavored communities who powerful actors believe threaten the status quo. While 20th century reforms were designed to curtail precisely these abuses, surveillance hawks continue to fight tooth and nail to retain their ability to use Section 702 to search for information about American residents without ever needing to make a case before a judge.

**Evidence**: The NSA and other government organizations are already spying on activists around the country.

> Gibbons, Chip. "Government surveillance of activists and labor organizers is alive and well." Jacobin Magazine. June 2006.

https://jacobinmag.com/2020/06/government-surveillance-activists-labor-organizers-pinkertons

In February 2020, University of California–Santa Cruz graduate student workers refused to turn in final grades unless their demand for a Cost of Living Adjustment (COLA) to match the cost of housing was met. As the administration refused to meet this demand, the graduate student workers' protest became a wildcat strike.

Emails recently obtained by Vice as part of a public records request reveal the lengths the administration was willing to go to to thwart the strike. Rather than meeting their demands, the administration worked with campus police, the Alameda County Sheriff's Office, the California National Guard, and the California Office of Emergency Services to police the strike.

These agencies also turned to the California State Threat Assessment Center, a "state fusion center." Fusion centers are affiliated with the Department of Homeland Security and share intelligence between state, federal, and private entities. According to a 2012 Congressional investigation, fusion centers produce intelligence of "uneven quality — oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."

**Analysis**: It's true that the NSA has targeted radical right-wing organizations, but it has also been used to squash dissent from labor organizers and other legitimate causes. The NSA's ability to spy on political organizations is therefore a double edged sword – while it's useful for targeting dangerous organizations, it simultaneously spies on regular Americans as well.

## A/2: The NSA saves lives

**Response:** NSA surveillance has not stopped terror, or saved lives

**Warrant**: The government's claim that surveillance programs stop terrorists is overblown.

Cahill, Bailey. "Do NSA's bulk surveillance programs stop terrorists?" New America Foundation. 1/13/14. https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.

**Evidence**: A federal judge recently ruled that NSA surveillance has stopped 0 terrorist attacks in total.

> Holmes, Aaron. "The NSA phone-spying program exposed by Edward Snowden didn't stop a single terrorist attack, federal judge finds." Business Insider. 9/2/20. https://www.businessinsider.com/nsa-phone-snooping-illegal-court-finds-2020-9
>
> The National Security Administration's sweeping program to snoop on Americans' phone records was illegal and possibly unconstitutional — and there's no evidence it led to the arrests of any terrorism suspects — a federal appeals court ruled Wednesday.
> In its ruling, the 9th Circuit Court of Appeals said the NSA broke the law by collecting "phone metadata," or bulk records of Americans' phone-call history. The court upheld the convictions of four Somali immigrants who were charged with fundraising for terrorists, however, concluding that the NSA's phone-record collection was ultimately not relevant to their convictions.
> The NSA's program to collect phone records was first brought to light by the former NSA contractor Edward Snowden in 2013. Amid public outrage following the revelation, the agency defended the program by claiming it had helped thwart terrorist attacks.
> But the NSA could point to only one example: the case of Basaalay Moalin. On Wednesday, the appeals court ruled that not only was the collection of Moalin's phone records illegal, but it was ultimately irrelevant to the conviction.

**Analysis**: Con teams will likely point to government data that suggests that the NSA's efforts have been effective, yet it's crucial to point out the bias in those sources. Government sources have a reason to suggest that their own policies are working whereas independent review is far more likely to prove whether or not the NSA is working.

## A/2: The NSA is cost-efficient

**Response:** The NSA is not efficient with its spending.

**Warrant**: Over $100 million was invested in an NSA program that only produced 2 leads.

Savage, Charlie. "NSA phone program cost $100 million, but produced only two unique leads." New York Times. 2/25/20. https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

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."

**Response:** Analysts agree that the NSA's rewards are not worth the costs.

**Warrant**: The amount of spending does not justify the rewards: security experts.

Pramuk, Jacob. "NSA phone surveillance not worth the costs: Expert." CNBC. https://www.cnbc.com/2015/11/30/nsa-phone-surveillance-not-worth-the-costs-expert.html

> The National Security Agency's authority to collect bulk phone data has expired, and two experts disagreed Monday on whether intelligence officials need that power to thwart terror plots.
>
> Over the weekend, the NSA lost the legal approval to store phone records in one of the biggest changes to American intelligence since Edward Snowden revealed details about U.S. tactics two years ago. While some officials have called to reauthorize mass phone data collection, its effectiveness does not justify possible violations of civil rights, said David Chronister, founder of Parameter Security.
>
> "We really haven't seen where it's been effective ... the amount of money we're spending and the amount of civil liberties that are being violated just isn't worth it," he said on CNBC's "Closing Bell."

**Analysis**: There are two claims to beat back here: the first being cost and the second being the actual efficiency of the program. Either is sufficient to win the argument, but both prongs are pretty weak – the NSA's spending is pretty enormous all things considered, yet we haven't seen much in the way of payoff yet.

## A/2: The NSA surveillance program is justified under the constitution

**Response:** NSA surveillance violates the fourth amendment.

**Warrant:** the PRISM program specifically is unconstitutional as it violates the fourth amendment

Patrick Toomey, Senior Staff Attorney, ACLU National Security Project, 8-22-2018, "The NSA Continues to Violate Americans' Internet Privacy Rights," American Civil Liberties Union, 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, internet 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 compani**es. PRISM Slide **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 communications, 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 review 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 government 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.

**Impact:** Privacy protections are needed for a functioning democracy, freedom of speech.

Kelsey Cora Skaggs, May 2016, "Surveilling Speech And Association: NSA Surveillance Programs And The First Amendment", University of Pennsylvania, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1610&context=jcl

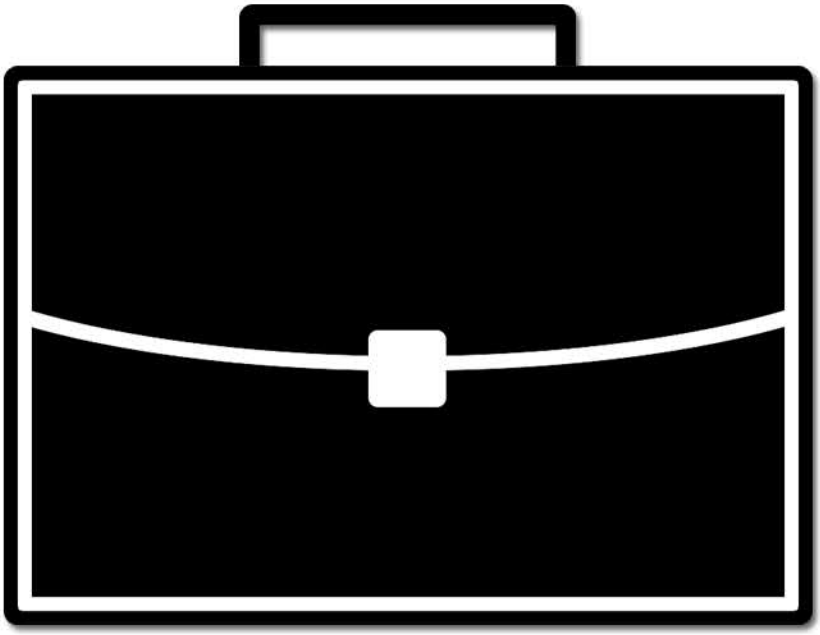
Regardless of the outcome of the Fourth Amendment analysis, however, **mass surveillance programs separately implicate the First Amendment.** The First Amendment and Fourth Amendment protect different rights and serve different purposes. The Fourth Amendment protects privacy, primarily benefitting the individual whose privacy is at 45 issue. By contrast, the First Amendment protects the rights to association and expression. **Though the First Amendment benefits individuals," it also benefits society as a whole by ensuring the freedom of political activity that is necessary for a functioning democracy.47 The First Amendment protects ideas and dissent in a way that the Fourth Amendment does not, and this protection is of fundamental importance for a free and democratic society.4 8**

**Analysis**: Ultimately, surveillance CAN be justified, but it's circumstantial. In many of the instances that the NSA has been known to spy on Americans, there isn't a legitimate justification hence why there have been lawsuits on the matter. Even if there is sometimes a justification for surveillance, that is outweighed by the violation of fundamental rights under the constitution.

# Champion Briefs

## January 2021

## Public Forum Brief



# Con Arguments

## CON - NSA will be critical to stopping cyber attacks

**Argument:** With an increasing number of countries developing their cyber attack capabilities, the NSA is more important than ever in order to protect this new threat.

**Warrant:** Many countries are developing cyber attack capability

Ranger, Steve. 05-01-2017. “US Intelligence: 30 countries building cyber attack capabilities.” ZD Net. 5 Jan. 2017. Web. 1 Dec. 2020. https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/

**More than 30 countries are developing offensive cyber attack capabilities, according to US intelligence chiefs. They warn that cyber attacks against critical infrastructure and information networks will give attackers a means of bypassing traditional defence measures.** The warning came in a joint statement by US director of National Security James Clapper, undersecretary of defense for intelligence Marcel Lettre, and NSA and US Cyber Command director Admiral Mike Rogers, at a hearing on foreign cyber threats by the Senate Armed Services Committee. **"Protecting critical infrastructure such as crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge,"** the written statement noted. It also warned that nations equipped with similar offensive cyber capabilities could be prone to preemptive attack and rapid escalation in a future crisis, "because both sides would have an incentive to strike first". The committee was meeting in the aftermath of what its chairman Senator John McCain called an "unprecedented attack on our democracy", referring to the hacking attacks during the recent Presidential election, which have been blamed by US intelligence on Russia.

**Uniqueness:** Surveillance is necessary to address cyber attacks

Goldsmith, Jack. 09-10-2013. "We Need an Invasive NSA." The New Republic. 9 Oct. 2013. Web. 1 Dec. 2020. https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks

Anyone anywhere with a connection to the Internet can engage in cyber-operations within the United States. **Most truly harmful cyber-operations, however, require group effort and significant skill. The attacking group or nation must have clever hackers, significant computing power, and the sophisticated software—known as "malware"—that enables the monitoring, exfiltration, or destruction of information inside a computer. The supply of all of these resources has been growing fast for many years—in governmental labs devoted to developing these tools and on sprawling black markets on the Internet.** Telecommunication networks are the channels through which malware typically travels, often anonymized or encrypted, and buried in the billions of communications that traverse the globe each day. The targets are the communications networks themselves as well as the computers they connect—things like the Times' servers, the computer systems that monitor nuclear plants, classified documents on computers in the Pentagon, the nasdaq exchange, your local bank, and your social-network providers.**To keep these computers and networks secure, the government needs powerful intelligence capabilities abroad so that it can learn about planned cyber-intrusions.** It also needs to raise defenses at home. An important first step is to correct the market failures that plague cybersecurity. Through law or regulation, the government must improve incentives for individuals to use security software, for private firms to harden their defenses and share information with one another, and for Internet service providers to crack down on the botnets—networks of compromised zombie computers—that underlie many cyber-attacks. More, too, must be done to prevent insider threats like Edward Snowden's, and to control the stealth introduction of vulnerabilities during

the manufacture of computer components—vulnerabilities that can later be used as windows for cyber-attacks.

**Warrant:** The threat of cyber attacks will mean that the public accepts and wants increasing surveillance measures.

Goldsmith, Jack. 09-10-2013. "We Need an Invasive NSA." The New Republic. 9 Oct. 2013. Web. 1 Dec. 2020. https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks

Alexander's domestic cybersecurity plans look like pumped-up versions of the NSA's counterterrorism-related homeland surveillance that has sparked so much controversy in recent months. That is why so many people in Washington think that Alexander's vision has "virtually no chance of moving forward," as the Times recently reported. "Whatever trust was there is now gone," a senior intelligence official told Times. There are two reasons to think that these predictions are wrong and that the government, with extensive assistance from the NSA, will one day intimately monitor private networks. The first is that the cybersecurity threat is more pervasive and severe than the terrorism threat and is somewhat easier to see. If the Times' website goes down a few more times and for longer periods, and if the next penetration of its computer systems causes large intellectual property losses or a compromise in its reporting, even the editorial page would rethink the proper balance of privacy and security. The point generalizes: **As cyber-theft and cyber-attacks continue to spread (and they will), and especially when they result in a catastrophic disaster (like a banking compromise that destroys market confidence, or a successful attack on an electrical grid), the public will demand government action to remedy the problem and will adjust its tolerance for intrusive government measures.**

**Urgency:** American Hospitals are at risk, especially during COVID.

Guardian Staff and Agencies. 10-29-2020, "US hospital systems facing 'imminent' threat of cyber-attacks, FBI warns," The Guardian. 29 Oct. 2020. Web. 7 Dec. 2020. https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi

**Federal agencies have warned that the US healthcare system is facing an "increased and imminent" threat of cybercrime, and that cybercriminals are unleashing a wave of extortion attempts designed to lock up hospital information systems, which could hurt patient care just as nationwide cases of Covid-19 are spiking.** In a joint alert on Wednesday, the FBI and two federal agencies warned that they had "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers". **The alert said malicious groups are targeting the sector with attacks that produce "data theft and disruption of healthcare services".** The cyber-attacks involve ransomware, which scrambles data into gibberish that can only be unlocked with software keys provided once targets pay up. Independent security experts say it has already hobbled at least five US hospitals this week, and could potentially affect hundreds more. The offensive by a Russian-speaking criminal gang comes less than a week ahead of the election, although there is no immediate indication they were motivated by anything but profit. "We are experiencing the most significant cybersecurity threat we've ever seen in the United States," Charles Carmakal, chief technical officer of the cybersecurity firm Mandiant, said in a statement.

**Impact: Cyber attack could cass mass deaths**

Struab, Jeremy. 08-18-2019. "A Major Cyber Attack Could be Just as Deadly as a Nuclear War." Science Alert. 18 Aug. 2019. Web. 1 Dec. 2020. https://www.sciencealert.com/a-major-cyber-attack-could-be-just-as-damaging-as-a-nuclear-weapon

In August 2017, a Saudi Arabian petrochemical plant was hit by hackers who tried to blow up equipment by taking control of the same types of electronics used in industrial facilities of all kinds throughout the world. Just a few months later, hackers shut down monitoring systems for oil and gas pipelines across the US This primarily caused logistical problems – but it showed how an insecure contractor's systems could potentially cause problems for primary ones. **The FBI has even warned that hackers are targeting nuclear facilities. A compromised nuclear facility could result in the discharge of radioactive material, chemicals or even possibly a reactor meltdown. A cyberattack could cause an event similar to the incident in Chernobyl. That explosion, caused by inadvertent error, resulted in 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.**

**Analysis:** This argument is strong if teams can prove two specific things. It will be important to first explain which countries threaten American cyber security at the moment and prove a clear motive to do so and capability to launch an attack, and second to prove how disastrous a cyber attack would be against America. Teams should look into specific threats against American cybersecurity in the squo and how exactly the NSA benefits cybersecurity threats.

## CON - The NSA Prevents Terrorist Attacks

**Argument:** The NSA is crucial to national security as it protects American cities from devastating terrorist attacks.

**Warrant:** Americans accept NSA surveillance to protect from terrorist attacks

Pew Survey. 06-10-2013."Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic." The Pew Research Center. 10 Jun. 2013. Web. 8 Dec. 2020. https://www.pewresearch.org/politics/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

**A majority of Americans – 56% – say the National Security Agency's (NSA) program tracking the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism,** though a substantial minority – 41% – say it is unacceptable. And while the public is more evenly divided over the government's monitoring of email and other online activities to prevent possible terrorism, **these views are largely unchanged since 2002, shortly after the 9/11 terrorist attacks.** The latest national survey by the Pew Research Center and The Washington Post, conducted June 6-9 among 1,004 adults, finds no indications that last week's revelations of the government's collection of phone records and internet data have altered fundamental public views about the tradeoff between investigating possible terrorism and protecting personal privacy.

**Quantification:** The NSA has prevented more than 50 terrorist attacks

Parkinson, John. 6-18-2013, "NSA: 'Over 50' Terror Plots Foiled by Data Dragnets," ABC News. 18 Jun 2013. Web. 8 Dec. 2020. https://abcnews.go.com/Politics/nsa-director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148

**The director of the National Security Administration today told Congress that more than 50 potential terrorist attacks have been thwarted by two controversial programs tracking more than a billion phone calls and vast swaths of Internet data each day.** T**he attacks on would-be targets such as the New York Stock Exchange were prevented by caching telephone metadata and Internet information, including from millions of Americans since Sept. 11, 2001,** Gen. Keith Alexander said during a hearing at the House Permanent Select Committee on Intelligence. Alexander had been less specific in testimony last week when he said "dozens" of possible attacks were foiled. He testified today: "**In recent years, these programs, together with other intelligence, have protected the U.S and our allies from terrorist threats across the globe to include helping prevent the potential terrorist events over 50 times since 9/11."** He appeared in a rare public hearing of the House Intelligence Committee with officials from the FBI and Justice Department to discuss the phone and Internet programs that were disclosed in June by former NSA contractor Edward Snowden in the British Guardian newspaper and also The Washington Post

**Warrant:** The data used by the NSA to uncover terrorist attacks does not harm citizens

Pierre Hines, 06-19-2013, "Here's how metadata on billions of phone calls predicts terrorist attacks," Quartz. 19 Jun. 2013. Web. 8 Dec. 2020. https://qz.com/95719/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/

**Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted**. Section 215 of the Patriot Act provides the legal authority to obtain "business records" from phone companies. Meanwhile, the NSA uses Section 702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases. One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. **As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists' planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack**. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat.

**Warrant: t**he NSA only need prevent one terrorist attack to be useful

Morrell, Michael. 12-27-2013. "Correcting the Record on NSA Recommendations." The

Washington Post. 27 Dec. 2013. Web. 9 Dec. 2020. https://www.washingtonpost.com/opinions/michael-morell-correcting-the-record-on-the-nsa-recommendations/2013/12/27/54846538-6e45-11e3-aecc-85cb037b7236_story.html?tid=a_inl_manual

Another misperception involved the review group's view of the efficacy of the Section 215 program; many commentators said it found no value in the program. The report accurately said that the program has not been "essential to preventing attacks" since its creation. But that is not the same thing as saying the program is not important to national security, which is why we did not recommend its elimination. **Had the program been in place more than a decade ago, it would likely have prevented 9/11. And it has the potential to prevent the next 9/11. It needs to be successful only once to be invaluable.** It also provides some confidence that overseas terrorist activity does not have a U.S. nexus. **The metadata program did exactly that during my last days at the CIA this summer, in the midst of significant threat reports emanating from Yemen. By examining the metadata, we were able to determine that certain known terrorists were most likely not in phone contact with anyone in the United States during this specific period of concern**. Personally, I would expand the Section 215 program to include all telephone metadata (the program covers only a subset of the total calls made) as well as e-mail metadata (which is not in the program) to better protect the United States. This is a personal view; it is not something the review group opined on or even discussed. Such an expansion should, of course, fall under the same constraints recommended by the review group.

**Impact:** Terrorism leads to increased probability of war which depletes resources for Americans

Sean Ross, 8-28-2020, "How Terrorism Damages the Global Economy," Investopedia. 28

Aug. 2020. Web. 8 Dec. 2020. https://www.investopedia.com/articles/markets/080216/top-5-ways-terrorism-impacts-economy.asp

There is an old saying in the study of political economy that reads "war is the health of the state." It means that during times of conflict, reactive governments and nervous citizens are far more inclined to give up economic and political freedoms in exchange for security.[10] This could result in higher taxes, higher government deficits, and higher inflation. **During wartime, the government often implements price controls and sometimes even the nationalization of industries. Governments are less effective at managing resources for productive economic activity than private individuals, especially when those resources are co-opted to achieve a strategic military objective. When governments militarize, the private economy suffers.** As economist and historian Robert Higgs demonstrated in his book "Crisis and Leviathan," many government controls stay in place long after

**Impact:** Terrorism causes long term economic impacts: xenophobia

Sean Ross, 8-28-2020, "How Terrorism Damages the Global Economy," Investopedia. 28 Aug. 2020. Web. 8 Dec. 2020. https://www.investopedia.com/articles/markets/080216/top-5-ways-terrorism-impacts-economy.asp

The final risk to the economy is a political risk. **This is already on display in the United States and Europe in 2016, where there has been a rise in skepticism of foreign cultures, businesses, immigrant workers, and refugees. Populist movements already won a victory of sorts in the United Kingdom, where anti-globalist and anti-trade sentiments helped pass Brexit. These kinds of major political events have an uncertain economic fallout on everything from currency to trade and diplomacy. Closing down**

**borders to trade and immigrant workers reduces the size and diversity of economic transactions and limits productive resources.** Economists as early as Adam Smith contended that the division of labor and gains from trade are limited to the size of available factors of production.[12] Just as a single household or town is less productive if it only relies on internal resources, so too do national economies limit themselves to the extent that they wall off external producers and consumers.

**Analysis:** This argument gives a clear reason that the NSA protects Americans. If you pair this argument with preemptive defense about how the NSA surveillance does not lead to concrete harms, then there is the potential for a large amount of offense. Teams thinking about running this argument should look into frontlines for arguments saying the NSA exaggerated claims about the amount of terrorist attacks stopped.

## CON - NSA Surveillance Maintains Safety

**Argument:** The NSA gathers information and uses it to keep America safe.

**Warrant:** Terrorist groups are willing to attack America

Tom Wither, 12-3-2015, "The NSA data collection program isn't criminal; ending it is," baltimoresun. 3 Dec. 2015. Web. 9 Dec. 2020. https://www.baltimoresun.com/opinion/op-ed/bs-ed-nsa-data-20151203-story.html

Throughout the nearly two years of public debate since the program was exposed, the Obama administration continued to apply for FISA Court warrants to compel multiple telecommunications service providers to give NSA their call records. The Obama administration obviously believed that the program was useful, and was permitted to continue to use it under the law, no matter what various critics might opine. Moreover, the FISA Court continued to approve these applications from the government. **The recent attacks in Paris remind us again that there are still organized and capable extremists willing to use violence and terror to attempt to advance their political agenda, be they from the Islamic State, al-Qaida, al-Shabaab, al-Nusrah Front, the Armed Islamic Group, the Moroccan Islamic Combatant Group or the relatively new "Revolutionary Organization 17 November.**

**Warrant:** Congressman believes NSA keeps America safe

Rogers, Michael. , 06-18-2013, "Rep. Mike Rogers: NSA keeps America safe," USA TODAY.

18 Jun. 2013. Web. 9 Dec. 2020. https://www.usatoday.com/story/opinion/2013/06/18/nsa-mike-rogers-house-intelligence-committee-editorials-debates/2436541/

**The gross distortion of two vital National Security Agency (NSA) programs is dangerous and unfortunate.** Neither program authorizes NSA to read e-mails or listen to phone calls of American citizens. Both are constitutional with numerous checks and balances by all three branches of government. **They have been authorized and overseen by Congress and presidents of both parties. And they have produced vital intelligence, preventing dozens of terrorist attacks around the world, including plots against New York City subways and the New York Stock Exchange. The first program allows NSA to preserve a limited category of business records. It preserves only phone numbers and the date, time and duration of calls. It doesn't include any names or the content of calls.** These records can only be accessed when NSA is investigating a foreign terrorist. If a foreign terrorist is found linked to an American, the tip is passed to the FBI and requires a court order before additional action can be taken**. This is a critical tool for connecting the dots between foreign terrorists plotting attacks in the U.S.**

**Warrant**: The amount of information the NSA gathers deters crime.

Michaels, Jim. 06-06-2013. "NSA data mining can help stop cybercrime, analysts say," USA TODAY. 6 Jun. 2013. Web. 8 Dec. 2020. https://www.usatoday.com/story/news/politics/2013/06/06/nsa-data-mining-cyber-crime-data/2397165/

**The huge volume of telephone records turned over to the U.S. government could help investigators identify and deter a range of terrorist acts, including cyberattacks, analysts say.** "Once you have this big chunk of data and you have it forever… you can do

all sorts of analytics with it using other data sources," said Joseph DeMarco, former head of the cybercrime unit in the U.S. attorney's office in New York City. "A data set like this is the gift that keeps on giving," said DeMarco, a partner at the law firm DeVore & DeMarco. The government obtained an order from the Foreign Intelligence Surveillance Court ordering a Verizon subsidiary to turn over phone records to the National Security Agency. The records do not include the content of phone calls and the order does not authorize eavesdropping.

**Warrant:** There has not been a major terrorist attack since 9/11

Dorell, Owen. 10-29-2013. "NSA chief defends its spying programs," USA TODAY. 29 Oct. 2013. Web. 9 Dec. 2020. https://www.usatoday.com/story/news/world/2013/10/29/nsa-spying-congress-testimony/3304221/

Under fire for even more revelations about the extent of its program, the NSA is now pushing back. In testimony before Congress, the director of the National Security Agency, General Keith Alexander, said that the agency's actions "bring back more U.S. soldiers, airmen and Marines" alive from a dangerous world. He also called "extremely false" the reports that the NSA has collected information on U.S. allies in Europe, and that they do not spy on Americans or "innocent civilians of any country." **Alexander was pointed in his defense arguing that despite major attacks elsewhere, there has been "not one major terrorist incident in the United States since 9/11," and that the NSA sees "what neither the CIA nor FBI could see" before 9/11.**

**Impact:** NSA is critical to protecting against terrorist attacks which can have deadly cost to lives

Miller, Erin.11-2017. "American Deaths in Terrorist Attacks" The University of

Maryland.Nov2017.Web.9Dec.2020. https://www.start.umd.edu/pubs/START_AmericanTerrorismDeaths_FactSheet_Nov2017.pdf

The following table presents statistics on the total number of terrorist attacks that took place in the United States, the total number of fatalities due to terrorist attacks in the United States (including perpetrators), the total number of U.S. fatalities due to terrorist attacks in the United States (including perpetrators), and the total number of U.S. fatalities due to terrorist attacks worldwide (including perpetrators, and excluding deaths in Afghanistan and Iraq), from 1995 to 2016. Effect of September 11, 2001 **Attacks: 3,222 Americans have been killed in terrorist attacks from 9/11/2001 through 12/31/2016, including perpetrators and excluding deaths in Afghanistan and Iraq. o 3,081 of these deaths occurred on American soil. o 2,902 of these deaths occurred during the attacks on September 11, 2001**

**Analysis:** This contention functions more broadly then a contention solely about prevention of one kind of attack, allowing more flexibility for teams running it. Teams interested in this argument should look into the various threats that the NSA addresses. A strong format for this contention would have several subpoints, all on different threats the NSA neutralizes.

## CON - The NSA is good for the economy

**Argument**: The NSA benefits the economy in several ways.

**Warrant:** The NSA employs a vast number of people

Elias Groll, 6-7-2013, "By the numbers: The NSA's super-secret spy program, PRISM," Foreign Policy. 7 Jun. 2013. Web. 9 Dec. 2020. https://foreignpolicy.com/2013/06/07/by-the-numbers-the-nsas-super-secret-spy-program-prism/

To put that debate in perspective, here's how PRISM stacks up by the numbers based on what we've learned today:

24,005: The number of PRISM-based reports issued in 2012 alone, which was a 27 percent increase from the previous year.

9: The number of tech companies whose servers NSA has access to via PRISM.

6: The number of years PRISM has been in operation.

2: The number of presidential administrations PRISM has operated under.

51 percent: The minimum confidence of a target's "foreignness" when an NSA analyst uses PRISM.

248 percent: The increase in 2012 in the number of Skype communications intercepted via PRISM

131 percent: The increase in 2012 in PRISM requests for Facebook data.

63 percent: The increase in 2012 in PRISM requests for Google data.

$20 million: The annual cost of PRISM.

$8 billion: The estimated annual budget of the NSA.

**35,000 to 55,000: The estimated number of employees at the NSA.**

0: The number of times Twitter has agreed to participate in PRISM.

1: The number of ad campaigns by Microsoft, the first company to agree to participate in PRISM, in which the company declares "your privacy is our priority."

**Warrant:** The NSA benefits telecom companies

Craig Timberg, 8-29-2013, "NSA paying U.S. companies for access to communications networks," Washington Post. 29 Aug. 2013. Web. 9 Dec. 2020. https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html

**The National Security Agency is paying hundreds of millions of dollars a year to U.S. companies for clandestine access to their communications networks, filtering vast traffic flows for foreign targets in a process that also sweeps in large volumes of American telephone calls, e-mails and instant messages. The bulk of the spending, detailed in a multi-volume intelligence budget obtained by The Washington Post, goes to participants in a Corporate Partner Access Project for major U.S. telecommunications providers.** The documents open an important window into surveillance operations on U.S. territory that have been the subject of debate since they were revealed by The Post and Britain's Guardian newspaper in June. New details of the corporate-partner project, which falls under the NSA's Special Source Operations, confirm that the agency taps into "high volume circuit and packet-switched networks," according to the spending blueprint for fiscal 2013. The program was expected to cost $278 million in the current fiscal year, down nearly one-third from its peak of $394 million in 2011.

**Warrant:** The NSA is crucial to helping the economic trauma after COVID.

Derek B. Johnson, 05-28-2020, "NSA's cyber wing looks to safeguard COVID research and expand outreach," FCW, 28 May 2020. Web. 9 Dec 2020. https://fcw.com/articles/2020/05/28/nsa-cyber-directorate-johnson.aspx

**The National Security Agency's cybersecurity directorate is focusing its resources on protecting medical research related to the COVID-19 pandemic and assisting critical infrastructure that can help speed up America's economic recovery,** according to the agency's Deputy Director George Barnes. Speaking on a webcast hosted by the Intelligence National Security Alliance, Barnes provided an update on the agency's cyber-focused directorate formed late last year. The rise of the COVID-19 pandemic has provided a whole host of additional challenges, increasing the collective digital threat surface as governments and businesses moved to mostly online operations and putting public health organizations and pharmaceutical companies working on a vaccine and other aspects of the response firmly in the crosshairs of nation-state hackers. Barnes said the fallout from the pandemic has pushed the directorate to ask "how do we protect critical activities that are vital to us getting back in a healthy state?" and enable Americans to get back to work and keep the economy moving. When it comes to protecting private and public medical research, the agency's bread and butter -- signals intelligence – can provide medical research organizations with insight into what information foreign governments are after as well as the tools and methods they're using to get it.

**Warrant:** NSA teams up with universities

NSA, 9-30-2009, "106 Universities Across U.S. Now Designated by NSA/DHS as National Centers of Academic Exc," National Security Agency Central Security Service. 30 Sep. 2009. Web. 9 Dec. 2020. https://www.nsa.gov/news-features/press-room/Article/1631507/106-universities-across-us-now-designated-by-nsadhs-as-national-centers-of-acad/

**The National Security Agency (NSA) has announced the designation of 29 additional U.S. colleges and universities as National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and/or Information Assurance Research (CAE-R). This brings the number of institutions participating in this highly regarded program to 106**, located in 37 states, the District of Columbia and the Commonwealth of Puerto Rico. Universities designated as National Centers of Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs. Graduates from Information Assurance programs at CAE institutions become the professional cyber security experts protecting national security information systems, commercial networks and critical information infrastructure. These professionals are helping to meet the increasingly urgent needs of the U.S. government, industry, academia and research.

**Impact:** Partnerships with colleges generate economic advantages

**Warrant:** The NSA partners with colleges

FLC Team, 2020 "NSA and the University of Texas: Supporting National Security and Economic Development Through Innovative Research Partnerships," FLC https://federallabs.org/successes/success-stories/nsa-and-the-university-of-texas-supporting-national-security-and-economic

**As part of its ongoing engagement with the University of Texas, NSA created in 2018 a first-of-its-kind CRADA that standardizes terms and conditions for specific joint work plans across the 14-institution UT System, resulting in significant improvements in the agility and responsiveness of collaborative research projects.** Under the umbrella CRADA, joint work plans can now be structured and approved within weeks, allowing

projects to be more responsive to Agency needs and more closely mirror the semester-by-semester cadence of higher education engagement. Much of the work to date has been concentrated at the University of Texas-San Antonio (UTSA), a national leader in cybersecurity that has fostered relationships with NSA and other federal agencies involved in intelligence and national security. Along with facilitating research within UTSA, NSA uses the umbrella CRADA to empower collaboration through the UTSA's National Security Collaboration Center (NSCC), a research center with more than 40 private and public-sector partners, to help a wide range of stakeholders meet shared national security needs. Many of these private and public partners specifically cited the importance of closer collaboration with NSA and other federal agencies in coordinating responses to shared threats and challenges. **The UTSA NSCC has provided a $100-million boost to the local technology ecosystem, which includes an excess of 1,000 technology businesses, 35,000 information technology workers, and an annual economic impact of approximately $12 billion.** Federal agency collaboration is a vital part of this ecosystem, with current federal cyber operations in San Antonio accounting for over 7,000 military and civilian jobs. It also supports broader regional and statewide economic development objectives, which identify cybersecurity as a key economic driver throughout the I-35 corridor. The umbrella CRADA and the collaborations it has facilitated also resulted in significant workforce benefits for NSA and the cybersecurity sector. Throughout the long term strategic relationship, more than 50 UTSA graduates have gone on to become NSA employees, and the Agency partnered with UTSA to create accelerated degree plans in cybersecurity and modern languages. Together, these efforts have helped the Agency and its federal and private sector partners "tackle some of America's toughest problems," said NSA Texas Commander Col. Gregory J. Gagnon.

**Analysis:** A good place to begin research on this argument is to figure out the cost of the NSA versus the cost of terrorist attacks. If teams can figure this out, then they can discuss the marginal benefit of having an NSA to prevent horrible economic consequences in the long term.

Teams would also be strategic to choose one way that the NSA helps the economy and base a whole contention over that specific thing.

## CON – Surveillance can stop the spread of COVID-19

**Argument:** Government surveillance is being used around the world for contact tracing to stop the spread of COVID-19. If the U.S. ends domestic surveillance, they rule out using the same technology to save lives.

**Uniqueness:** Surveillance to stop the spread of COVID has not been limited to authoritarian regimes.

> Rozenshtein, Alan. "Government Surveillance in an Age of Pandemics." Lawfare, 23 Mar. 2020, www.lawfareblog.com/government-surveillance-age-pandemics.
>
> But **increased surveillance has not been limited to authoritarian states. Other Asian countries, such as Taiwan, Singapore and South Korean, have also used aggressive surveillance and tracking to keep coronavirus infection rates low without resorting to mass lockdowns.** Perhaps taking notice, **liberal democracies are stepping up as well. Israel has repurposed its domestic spy agency's trove of cell phone data to notify individuals who may have come into contact with those infected with the coronavirus.** The United Kingdom is developing an app that would do the same thing, but on a voluntary basis. Even the European Data Protection Board, perhaps the world's strictest privacy regulator, has clarified that individualized phone-based tracking may be permissible, assuming legislative authorization and adequate safeguards.

**Uniqueness:** The U.S. is already moving toward using cellphone surveillance to track people who are infected.

> Deese, Kaelan. "US, Europe Turning to Cellphone Tracking Data to Slow Coronavirus Spread." TheHill, 3 Apr. 2020,

thehill.com/policy/technology/technology/490991-us-europe-cellphone-data-halt-coronavirus. Accessed 12 Dec. 2020.

**The U.S. and Europe are moving toward unprecedented cellphone surveillance strategies to track residents infected with the coronavirus as a way to slow the spread of the disease, The Wall Street Journal reported Friday.** The practice, which has been put in use in China, Singapore, Israel and South Korea, has faced a tougher audience in European countries and the U.S. because of privacy concerns. Still, more governments are looking into data surveillance as a way to keep coronavirus cases in check, as U.S. cases topped 257,000 on Friday, according to Johns Hopkins University data.

**Warrant:** Mass surveillance methods permit authorities to track and curb COVID-19.

Biddle, Sam. "Privacy Experts Say Responsible Coronavirus Surveillance Is Possible." The Intercept, 2 Apr. 2020, theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/.

IN LESS than a decade, whistleblowers like the NSA's Edward Snowden and Cambridge 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 another 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.

**Warrant:** The longer the pandemic goes on, the more likely the U.S. will turn to surveillance for solutions.

Rozenshtein, Alan. "Government Surveillance in an Age of Pandemics." Lawfare, 23 Mar. 2020, www.lawfareblog.com/government-surveillance-age-pandemics.

In the United States, which seems perennially behind the curve on all things coronavirus, there has not yet been (at least not publicly) an expansion in individual electronic surveillance to fight the pandemic. But **the longer it continues, the more likely that federal, state and local governments will turn to such technologies to enable a more targeted approach to coronavirus management. The federal government is already in talks with tech giants to use cell phone data to track the virus (though for now the discussion seems to be limited to anonymized data).** Strikingly, even the Electronic Frontier Foundation has conceded that more surveillance will be necessary, noting, "In the digital world as in the physical world, public policy must reflect a balance between collective good and civil liberties in order to protect the health and safety of our society from communicable disease outbreaks." When it comes to increased surveillance to fight the coronavirus, the question seems to be not if, but when.

**Impact:** COVID-19 fatalities in Korea are a third of the global average.

Fendos, Justin. "How Surveillance Technology Powered South Korea's COVID-19 Response." Brookings, 29 Apr. 2020, www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/.

Throughout the outbreak, the Korean public's opinions about surveillance have been overwhelmingly positive. **COVID-19 fatalities in Korea are a third of the global average, and Korea is one of very few countries to have flattened the curve and so far avoided a re-emergence of virus.** Despite these successes, there have been voices expressing concern about the level of detail released by health authorities. In one case, netizens

appear have to identified a couple engaged in an extramarital affair by matching their trace records. Such incidents are rare, but they have nonetheless motivated updates to surveillance guidelines, including the implementation of a petition process for rewording or withholding information deemed sensitive.

**Impact:** Worst-case scenario, global deaths from COVID-19 could exceed 3 million by January.

Mega, Emiliano Rodríguez. "COVID Has Killed More than One Million People. How Many More Will Die?" Nature, 30 Sept. 2020, www.nature.com/articles/d41586-020-02762-y, 10.1038/d41586-020-02762-y.

Nine months into the coronavirus pandemic, the official global death toll has now exceeded one million people. But researchers warn that this figure probably vastly underestimates the actual number of people who have died from COVID-19. And, **in a worst-case scenario, one group of modellers suggests that the number of deaths could exceed 3 million people by January.** The one-million milestone was hit on 28 September, according to the COVID case tracker maintained by Johns Hopkins University in Baltimore, Maryland.

**Analysis:** This argument can be weighed on timeframe. The midst of a global pandemic is not the right time to end domestic surveillance programs, as their use for legitimate matters of public health has never been more pressing. This argument can also be weighed on magnitude. The far-reaching impacts of the pandemic are likely more severe than any privacy concerns.

## CON – Reforming NSA surveillance is preferable to ending it

**Argument:** Some degree of domestic surveillance is necessary for national security. Since the Snowden leaks, there have been major efforts to reform the NSA and hold it accountable for unlawful spying. Ending surveillance is not the solution, but rather continued reform.

**Uniqueness:** Courts have condemned the NSA's old spying program as unlawful.

> Reuters. "NSA Surveillance Exposed by Snowden Was Illegal, Court Rules Seven Years On." The Guardian, 3 Sept. 2020, www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules.
>
> Seven years after the former National Security Agency contractor Edward Snowden blew the whistle on the mass surveillance of Americans' telephone records, an appeals court has found the program was unlawful – and that the US intelligence leaders who publicly defended it were not telling the truth. In a ruling handed down on Wednesday, t**he US court of appeals for the ninth circuit said the warrantless telephone dragnet that secretly collected millions of Americans' telephone records violated the Foreign Intelligence Surveillance Act and may well have been unconstitutional.** Snowden, who fled to Russia in the aftermath of the 2013 disclosures and still faces US espionage charges, said on Twitter that the ruling was a vindication of his decision to go public with evidence of the National Security Agency's domestic eavesdropping operation.

**Uniqueness:** The NSA suspended their controversial phone surveillance program.

> Lardieri, Alexa. "NSA Suspends Controversial Phone Surveillance Program." US News, 5 Mar. 2019, www.usnews.com/news/politics/articles/2019-03-05/nsa-suspends-controversial-phone-surveillance-program.

**THE NATIONAL SECURITY Agency has shut down the controversial program that tracks Americans' domestic calls and texts.** Luke Murry, national security adviser to House Minority Leader Kevin McCarthy, said during a Lawfare podcast that the NSA has not used the system in six months. The program is set to expire at the end of the year, and the Trump administration is unlikely to request an extension from Congress.

**Warrant:** Snowden forced the NSA to reform.

Edgar, Timothy. "Why the NSA Should Thank Edward Snowden." Fortune, 3 Oct. 2017, fortune.com/2017/10/03/edward-snowden-nsa-fisa-section-702/.

From 2006 to 2013, I worked inside the surveillance state as a privacy official, first in the Office of the Director of National Intelligence and later at the White House under President Barack Obama. While I helped put the NSA's programs on firmer legal ground and made some improvements in oversight, broader changes to protect privacy were elusive. **Obama's aides showed little interest in reforming mass surveillance until after I left, when the Snowden leaks forced their hands. It was Snowden who forced the NSA to be more transparent, accountable, and protective of privacy. The NSA took painful steps to open up.** It released thousands of pages of previously top-secret documents in a transparency drive intended to put the Snowden leaks in context. The head of the intelligence community now publishes an annual transparency report. Congress ended bulk collection of Americans' telephone records after an outside review found it to be of marginal value.

**Warrant:** Senators proposed a bill to drastically reform the NSA.

Coble, Sarah. "US Rolls Out New Bill to Reform NSA Surveillance." Infosecurity Magazine, 27 Jan. 2020, www.infosecurity-magazine.com/news/us-rolls-out-new-bill-to-reform/.

**US senators have proposed a bill that would drastically reform the surveillance practices of the National Security Agency (NSA) and increase oversight of government surveillance.** Titled The Safeguarding Americans' Private Records Act, the bill was introduced on Thursday by Senators Ron Wyden, Zoe Lofgren, Pramila Jayapal, Warren Davidson, and Steve Daines. According to a statement on Wyden's website, the changes proposed in the bill will "protect Americans' rights against unnecessary government surveillance." **The bill comes ahead of the March 15 expiration of Section 215 of the Patriot Act,** which the National Security Agency "used to create a secret mass surveillance program that swept up millions of Americans' phone calls." The phone record program was terminated last year.

**Impact:** Surveillance is the only way to draw connections between terror threats and potential attacks on the U.S.

AP News. "NSA: Bulk Collection Surveillance Keeps Us Safe." Www.Cbsnews.com, 11 Oct. 2013, www.cbsnews.com/news/nsa-bulk-collection-surveillance-keeps-us-safe/.

The NSA chief said Wednesday he knows of no better way his agency can help protect the U.S. from foreign threats than with spy programs that collect billions of phone and Internet records from around the world.

Pleading with the Senate Judiciary Committee to not abolish the National Security Agency's bulk-collection programs, Gen. Keith Alexander warned that global threats are growing - specifically in Iraq and Syria - that pose what he called "an unacceptable risk" to America. **"How do we connect the dots?" Alexander said, referring to often-hidden links between a foreign terror threat and a potential attack on the U.S. "There is no other way that we know of to connect the dots. ... Taking these programs off the table is absolutely not the thing to do."** The committee's chairman, Sen. Patrick Leahy, D-Vt.,

said it was troubling that the government was sweeping up millions, if not billions, of Americans' records. He has proposed legislation to prohibit the NSA from the bulk collection of U.S. phone records, and said Wednesday that he was concerned that Americans' Internet records also were vacuumed up before the program ended in 2011. That program now focuses only on people who live outside the United States - which could include Americans living abroad.

**Impact:** The government's surveillance programs have helped thwart more than 50 terror attacks.

Levy, Pema. "The Four Times NSA Surveillance Programs Stopped An Attack." International Business Times, 18 June 2013, www.ibtimes.com/four-times-nsa-surveillance-programs-stopped-attack-1312309.

Since the terrorist attacks of Sept. 11, 2001, **the government's surveillance programs have helped thwart a terrorist attack in more than 50 instances, according to Gen. Keith Alexander, director of the National Security Agency.** The intelligence community has decided to disclose four of these cases. Speaking at a House Intelligence Committee hearing on Tuesday, top intelligence community officials including Gen. Alexander defended the NSA's surveillance of phone records and Internet communications, which has come under fire as a breach of Americans' civil liberties since the program was revealed by former NSA contractor Edward Snowden. The five witnesses repeatedly told the committee that robust protections were in place to protect citizens' privacy.

**Analysis:** This argument can be weighed on magnitude. Any impact to privacy is severely mitigated if reform is happening in the status quo. A terror attack that would have otherwise been thwarted with surveillance would likely have more severe impacts than any small impact on privacy.

## CON – NSA surveillance is preferable to FBI surveillance

**Argument:** If the NSA surveillance program ends, domestic surveillance powers will probably transfer over to other government agencies like the FBI. It is more dangerous for the FBI to have this data because it is a domestic law enforcement agency, and thus is more likely to abuse such information to unfairly prosecute Americans.

**Uniqueness:** The FBI has abused NSA mass surveillance data in the past.

> Aaronson, Trevor. "A Declassified Court Ruling Shows How the FBI Abused NSA Mass Surveillance Data." The Intercept, 10 Oct. 2019, theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/.
>
> THE FOREIGN INTELLIGENCE Surveillance Court found that t**he FBI may have violated the rights of potentially millions of Americans — including its own agents and informants — by improperly searching through information obtained by the National Security Agency's mass surveillance program.** U.S. District Court Judge James E. Boasberg, who serves in the District of Columbia and the FISA court, made his sweeping and condemnatory assessment in October 2018 in a 138-page ruling, which was declassified by the U.S. government this week. **To longtime critics of the government's mass surveillance program, the FBI's abuses are confirmation that federal law enforcement agents are combing through the communications of Americans without warrants**, in violation of Fourth Amendment protections against unreasonable searches and seizures.

**Quantification:** In the status quo, the FBI only receives about 4 percent of the NSA's data collection.

Rangappa, Asha. "Don't Fall for the Hype: How the FBI's Use of Section 702 Surveillance Data Really Works." Just Security, 29 Nov. 2017, www.justsecurity.org/47428/dont-fall-hype-702-fbi-works/.

Some of these incidental communications may include parties who are U.S. persons (USPERs), which under FISA are defined as U.S. citizens or permanent legal residents. **Only a subset of the total communications collected under PRISM is passed on to the FBI. Specifically, the NSA passes on to the FBI information collected on selectors associated with "Full Investigations" opened by the FBI. Full Investigations are the most serious class of investigations within the Bureau, and require the most stringent predicate to open: There must be an "articulable factual basis" that a federal crime has occurred or is occurring or a threat to national security exists.** (Two other investigative classifications, Preliminary Investigations and Threat Assessments, have lower thresholds to open and shorter time limits to remain open.) In other words, the NSA provides the FBI with communications from selectors that are directly linked to the most serious crimes or threats to national security currently being investigated by the FBI. According to FBI Director Christopher Wray, **the FBI receives about 4.3 percent of the NSA's total collection** – and since not every incidental communication will necessarily involve an USPER, the number of communications involving Americans are likely less than that.

**Warrant:** Obama proposed letting the FBI hold the data instead of the NSA.

Toor, Amar. "Obama Assessing Four Alternatives to NSA Phone Data Collection: WSJ." The Verge, 26 Feb. 2014, www.theverge.com/2014/2/26/5448814/obama-assessing-four-alternatives-to-nsa-phone-data-collection-wsj.

One proposal would be to put phone metadata collection under the purview of US telecommunications companies. Under this option, the NSA would inform the

companies of when it needs to search their databases for terrorism-related investigations, and the phone companies would return only the results of those searches, rather than data on consumers unrelated to the investigations. **A second proposal would see a different federal agency hold the data — the Federal Bureau of Investigation (FBI), for instance** — and a third would place them under the control of a third entity that's neither a federal agency nor a telecom company. The final proposal would abolish the data collection program altogether, an option that Obama in January said would require more work "to determine exactly how this system might work."

**Warrant:** The FBI can search for information without pre-existing suspicion.

Granick, Jennifer. “Reining In Warrantless Wiretapping of Americans.” The Century Foundation, 16 Mar. 2017, tcf.org/content/report/reining-warrantless-wiretapping-americans/?agreed=1.

Once intelligence agents collect private messages under section 702, domestic law enforcement agencies are authorized to use the sensitive data in a range of worrisome ways. **The Federal Bureau of Investigation (FBI) may search the information to learn whether Americans are committing run-of-the-mill crimes without any pre-existing suspicion.** Normally, conversations people have with their attorneys are treated as privileged information: no one can compel a lawyer to testify against his or her client.

**Impact:** Surveillance tools could be used against Americans.

The American Civil Liberties Union. “More About FBI Spying.” American Civil Liberties Union, www.aclu.org/other/more-about-fbi-spying.

The FBI has a long history of abusing its national security surveillance powers. **The potential for abuse is once again great, particularly given that the lines between**

**criminal investigations and foreign intelligence operations have been blurred or erased since 9/11. As a result, intrusive surveillance tools originally developed to target Soviet spies are increasingly being used against Americans.** During the Cold War, the FBI ran a domestic intelligence/counterintelligence program called COINTELPRO that quickly evolved from a legitimate effort to protect the national security from hostile foreign threats into an effort to suppress domestic political dissent through an array of illegal activities.

**Impact:** The FBI disproportionately targets Arab, Middle Eastern, Muslim, and South Asian communities.

The American Civil Liberties Union. UNLEASHED AND UNACCOUNTABLE The FBI's Unchecked Abuse of Authority. 2013. https://www.aclu.org/other/unleashed-and-unaccountable-fbis-unchecked-abuse-authority.

**Arab, Middle-Eastern, Muslim, and South Asian (AMEMSA) communities in the U.S. have faced the brunt of the FBI's overzealous applications of its expanded authorities since 9/11.** In the immediate aftermath of the attacks, acting out of fear and ignorance, FBI agents and other federal officials arrested hundreds of Middle-Eastern immigrants, based mostly on minor visa violations, in a pre-emptive measure painfully reminiscent of the Palmer raids. 241 The Justice Department initiated a "hold until cleared" policy that assured the detainees would be held without bond until cleared by the FBI of any links to terrorism, meaning many languished in detention for months.

**Analysis:** This argument is strategic because it allows the con team to co-opt pro's arguments about privacy. It could be strategically read as a turn or offensive overview in round. It can also be weighed on probability. Because the FBI is a law enforcement agency, it's more likely to misuse data than the NSA.

## CON – Ending NSA surveillance props up Big Tech

**Argument:** The government will likely turn to Big Tech companies for information if they end their own surveillance programs. This is worse because Big Tech has less oversight and regulations than government agencies.

**Uniqueness:** The NSA is not as intrusive as other government agencies, companies, and political campaigns.

> Ambinder, Marc. "5 Reasons the NSA Scandal Ain't All That." Theweek.com, 20 Aug. 2013, theweek.com/articles/460928/5-reasons-nsa-scandal-aint-all-that.
>
> I will make the case for why I think the NSA scandal is as bad as it sounds in a future post. Now, I want to make the case, somewhat simplified, that the Snowden revelations, and everything we've learned until this point, do not paint a picture that resembles anything Edward Munch might come up with. I will not qualify any of the reasons below with phrases like, "but of course, they could do much, much better" or "without a doubt, the NSA hasn't been nearly as forthcoming as they ought to be" or "of course Americans have a right to know more." I do believe all of it, and I'll save that for the next post. **What NSA does with the metadata it collects on Americans is orders of magnitude less intrusive that what other government agencies do with what they collect, than what companies do with what we give them voluntarily and without our knowledge, or what political campaigns profess to know about you by buying data you did not intend for them to see.** It does matter that Americans have no way of knowing whether their number popped up during an analyst's call-chaining session.

**Uniqueness:** The NSA has more oversight and regulation than private companies.

McLaughlin, John. "NSA Intelligence-Gathering Programs Keep Us Safe." Washington Post, 2 Jan. 2014, www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html.

Regarding outrage over the NSA's collection of telephone calling records, or metadata, **I don't know why anyone would have greater confidence in this information being held by private companies.** And given the perceived threat to privacy, it's astonishing how little attention has been paid to the Senate commerce committee's recent report on companies that gather personal information on hundreds of millions of Americans and sell it to marketers, often highlighting people with financial vulnerability. Some companies group the data into categories including "rural and barely making it," "retiring on empty" and "credit crunched: city families." The aim is often to sell financially risky products to transient consumers with low incomes, the report found. **That's a real scandal — and a universe away from the NSA's ethical standards and congressional oversight.** The NSA, of course, is not perfect. But it is less a victim of its actions — the independent commission appointed by President Obama found no illegality or abuses — than of the broad distrust of government that has taken root in the United States in recent decades. Studies by Pew and others show distrust of government around 80 percent, an all-time high.

**Warrant:** Tech companies act as "surveillance intermediaries."

Margaret Jane Radin. "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance." Harvardlawreview.org, 10 Apr. 2018, harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

In just six months, law enforcement agencies turned to technology companies to gather evidence for thousands of investigations. Of the many conclusions that one might draw from these numbers, at least one thing is clear: technology companies have become major actors in the world of law enforcement and national security. **In his recent article, Professor Alan Rozenshtein dubs these technology companies "surveillance intermediaries" — entities that sit between law enforcement agencies and the public's personal information, and that have the power to decide just how easy or difficult it will be for law enforcement to access that information. Surveillance intermediaries hold extraordinary power when they decide how to respond to government requests for information — power that may or may not be to the public's benefit.** While intermediaries must comply with statutory and constitutional law governing law enforcement requests for information, Rozenshtein explains that they still hold a large degree of discretion when processing those requests: discretion in how critically they evaluate the legality of requests, in slowing down the process by insisting on proceduralism, and in minimizing their capacity to respond to legal requests by implementing encryption.

**Warrant:** Big Tech is increasingly beholden to Washington.

Samuels, David. "Is Big Tech Merging With Big Brother? Kinda Looks Like It." Wired, 23 Jan. 2019, www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/.

These troubling trends are accelerating in part because **Big Tech is increasingly beholden to Washington, which has little incentive to kill the golden goose that is filling its tax and political coffers.** One of the leading corporate spenders on lobbying services in Washington, DC, in 2017 was Google's parent company, Alphabet, which, according to the Center for Responsive Politics, spent more than $18 million. Lobbying Congress and government helps tech companies like Google win large government

contracts. Perhaps more importantly, it serves as a shield against attempts to regulate their wildly lucrative businesses.

**Impact:** Big Tech companies likely turn over enormous amounts of data, irrespective of its legality.

Margaret Jane Radin. "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance." Harvardlawreview.org, 10 Apr. 2018, harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

According to the AT&T engineer who initially revealed the company's cooperation with the government, AT&T built an entire room in its headquarters that appeared to be solely dedicated to "copying the whole Internet" for the NSA. AT&T did this despite the fact that the program was run without a clear legal basis from 2001 through 2008, at which point Congress passed a statute authorizing the program and granting full retroactive immunity for its participants. It is clear that AT&T went above and beyond to facilitate government surveillance without much concern over the legality of that surveillance. This story paints a bleak picture of AT&T undermining the legal structure built to protect its users' privacy rights. It shows that **surveillance intermediaries are capable of providing the U.S. government with an enormous amount of data, far exceeding what they are legally required to turn over. It is an ominous incident in the history of intermediaries that should raise concerns about the incredible amount of power that a company like AT&T holds.** Other commentators, including Rozenshtein, have concluded that the rise of surveillance intermediaries is likely to impose constraints on government surveillance,

**Impact:** Data from Big Tech in the hands of the government could result in "a softer version of China's Big Brother."

Samuels, David. “Is Big Tech Merging With Big Brother? Kinda Looks Like It.” Wired, 23 Jan. 2019, www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/.

The speed at which individual-rights-and-privacy-based social arrangements collapse is likely to depend on how fast Big Tech and the American national security apparatus consummate a relationship that has been growing ever closer for the past decade. While US surveillance agencies do not have regular real-time access to the gigantic amounts of data collected by the likes of Google, Facebook, and Amazon—as far as we know, anyway—there is both anecdotal and hard evidence to suggest that the **once-distant planets of consumer Big Tech and American surveillance agencies are fast merging into a single corporate-bureaucratic life-world, whose potential for tracking, sorting, gas-lighting, manipulating, and censoring citizens may result in a softer version of China’s Big Brother.** These troubling trends are accelerating in part because Big Tech is increasingly beholden to Washington, which has little incentive to kill the golden goose that is filling its tax and political coffers.

**Analysis:** This argument can be weighed on magnitude. Privacy violations will likely be even more severe if there is more cooperation between Big Tech and the government since these companies are largely unregulated.

## CON – NSA surveillance enables offensive cyber operations

**Argument:** NSA surveillance is necessary for the U.S. to conduct effective offensive cyber operations. These are necessary to deter cyber attacks.

**Warrant:** The NSA is responsible for offensive hacking operations.

> Lee, Timothy B. "The NSA Spying Debate, Explained." Vox, 1 June 2015, www.vox.com/2015/6/1/18093692/nsa-and-ed-snowden.
>
> Does the NSA engage in offensive hacking operations? Yes. **Many of the National Security Agency's spying activities rely on passive surveillance — intercepting information as it flows through public networks. But the agency also has a division called Tailored Access Operations (TAO) that is responsible for offensive hacking operations.** According to Spiegel, TAO is based in San Antonio, Texas, and "exploits the technical weaknesses of the IT industry, from Microsoft to Cisco and Huawei, to carry out its discreet and efficient attacks."

**Warrant:** Cyber operations rely on NSA surveillance.

> Goldsmith, Jack. "We Need an Invasive NSA." The New Republic, 10 Oct. 2013, newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks.
>
> What it does not appear to realize is the connection between the domestic NSA surveillance it detests and the governmental assistance with cybersecurity it cherishes. **To keep our computer and telecommunication networks secure, the government will eventually need to monitor and collect intelligence on those networks using techniques similar to ones the Timesand many others find reprehensible when done for counterterrorism ends.** The fate of domestic surveillance is today being fought

around the topic of whether it is needed to stop Al Qaeda from blowing things up. But the fight tomorrow, and the more important fight, will be about whether it is necessary to protect our ways of life embedded in computer networks.

**Warrant:** Trump shifted toward a more offensive cybersecurity strategy.

Fazzini, Kate. "Trump's New Strategy Means the U.S. Could Get More Aggressive with Russia and China over Hacking." CNBC, CNBC, 21 Sept. 2018, www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html.

The 40-page document mostly stays the course for past initiatives -- like working to strengthen the organizations that make up the country's "critical infrastructure" industries, including electrical operators and financial institutions. **But some of the changes emphasize a shift toward a more offensive cybersecurity posture, a longtime request from the National Security Agency and cybersecurity branches of the U.S. Armed Forces.** The document also builds on efforts by the Trump and Obama administrations to "name and shame" more cybercriminals, and the countries that back them, while acknowledging the available to federal cyber operators have been limited.

**Warrant:** The NSA is the de facto authority on cyber operations.

Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks, 3 Apr. 2019, warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.

The review process for a Cyber Command operation also requires an equities review by a multitude of government, intelligence, and military stakeholders. The idea is that all

relevant parties have an opportunity to address potential concerns with a proposed offensive cyberspace operation. While one of the principal original concerns with the dual hat arrangement was the potential for unfair prioritization of Cyber Command support requests to the NSA, the equities review process has instead created the opposite problem. **Because Cyber Command depends so heavily on NSA logistical and operational support, it has essentially lent the agency de facto veto authority on offensive cyberspace operations: Cyber Command risks losing NSA-facilitated training, NSA-provided office space, and access to NSA's signals intelligence data by bickering with NSA over who get a shot at a given targets.** The responsibility of balancing the prioritization of the distinct missions of two different organizations should not be delegated to a single individual. Doing so inevitably privileges one mission at the other's expense, and ultimately impedes overall progress for both

**Impact:** Credible U.S. threats would deter adversaries from launching attacks.

Gale, David, et al. "Cybermad: Should the United States Adopt a Mutually Assured Destruction Policy for Cyberspace?" Air University, Apr. 2009.

The nuclear MAD doctrine is credited with preventing the Cold War from turning hot, since neither side could expect to survive a full scale nuclear exchange. Although the loss of cyberspace might not rise to this level, the doctrine still applies. **If the US can credibly vow to destroy cyberspace, thus destroying world economies, the US can deter an adversary from launching an attack.** Critics may correctly argue that CyberMAD's deterrent effect is limited, since it will not deter non-state actors. However, nuclear MAD doctrine never deterred non-state actors. Critics will also argue that the lack of attribution will limit CyberMAD. Although true, it allows us to focus on developing the capability. We should not throw out the doctrine. We should develop the capability.

**Impact:** A cyber attack would put critical infrastructure at risk.

LaFrance, Adrienne. "When Is Cyberwar Just War?" The Atlantic, 16 May 2017, www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/.

The devastating effects of a massive cyberattack are no more confined to a computer network than any other action carried out online. People use the computers and the internet all the time to make things happen in the physical world. **A cyberattack isn't just a cyberattack. It's an attack. Hospitals, pharmacies, and major corporations like FedEx and the Spanish telecommunications giant Telefonica were among the 200,000 victims hobbled by a global ransomware attack on Friday, which locked people's computers and demanded Bitcoin payment in exchange for access. In the United Kingdom, some hospitals canceled procedures and other appointments as a result.** The software security firm Symantec found that people paid ransoms totaling about $54,000 in the attack, though officials strongly caution against paying such ransoms.

**Analysis:** This argument can be weighed on magnitude. A cyberattack that could destroy critical infrastructure would likely have more severe, tangible impacts than any threats to privacy. It can also be weighed on timeframe, as hospitals may be particularly vulnerable to cyberattacks with the pandemic ongoing.

## CON – The NSA is essential to stopping Chinese cyberattacks

**Argument:** The NSA plays a key role in preventing Chinese cyberwarfare.

**Warrant**: The NSA has historically been used to spy on China, even going back to the Obama administration.

Aid, Mathew. "Inside the NSA's ultra-secret China hacking group." South China Morning Post. 6/12/13. https://www.scmp.com/news/china/article/1259175/inside-nsas-ultra-secret-china-hacking-group

Last weekend, US President Barack Obama sat down for a series of meetings with China's newly appointed leader, Xi Jinping. We know that the two leaders spoke at length about the topic du jour – cyber-espionage – a subject that has long frustrated officials in Washington and is now front and centre with the revelations of sweeping US data mining. The media has focused at length on China's aggressive attempts to electronically steal US military and commercial secrets, but Xi pushed back at the "shirt-sleeves" summit, noting that China, too, was the recipient of cyber-espionage. But what Obama probably neglected to mention is that he has his own hacker army, and it has burrowed its way deep, deep into China's networks.

When the agenda for the meeting at the Sunnylands estate outside Palm Springs, California, was agreed to several months ago, both parties agreed that it would be a nice opportunity for President Xi, who assumed his post in March, to discuss a wide range of security and economic issues of concern to both countries. According to diplomatic sources, the issue of cyber-security was not one of the key topics to be discussed at the summit. Sino-American economic relations, climate change, and the growing threat posed by North Korea were supposed to dominate the discussions.

**Warrant**: The government has been known to use the surveillance state to keep track of Chinese Americans.

Hvistendahl, Mara. "The FBI's China obsession." The Intercept. 2/2/20. https://theintercept.com/2020/02/02/fbi-chinese-scientists-surveillance/

As Chinese American scientists returned to visit long-lost friends and relatives, the bureau closely tracked them.
In 1972, Jen led a delegation of Chinese American scientists and their families to China. Katherine Yih, who joined her father on the trip, recalled a highly orchestrated tour that included visiting agricultural communes and watching children's dance performances. "We were being shown the successes of the revolution," she said. The visitors were seen as important enough that they were also taken to meet Premier Zhou Enlai, a development that almost certainly heightened the suspicions of U.S. counterintelligence operatives.

**Evidence**: Today, the government surveils Chinese Americans suspected of spying.

Waldman, Peter. "Mistrust and the hunt for spies among Chinese Americans." Bloomberg. 12/10/19. https://www.bloomberg.com/news/features/2019-12-10/the-u-s-government-s-mistrust-of-chinese-americans

Su's ordeal reflects how the U.S. government's distrust of China, which flared during the Obama administration and erupted openly during President Donald Trump's trade war, has mutated into distrust of Chinese Americans. Signs of this heightened scrutiny emerged in July when FBI Director Christopher Wray told the Senate Judiciary Committee that the bureau is investigating more than 1,000 cases of attempted theft of U.S. intellectual property, with "almost all" leading back to China. Last year the U.S. National Institutes of Health, working with the FBI, started probes into some 180

researchers at more than 70 hospitals and universities, seeking undisclosed ties to China. Some of the suspected scientists were instructed by their associates in China to conceal their connections to the country while in the U.S., says Ross McKinney, chief scientific officer for the Association of American Medical Colleges. “The presumption of trust is blown by the fact that there’s a systematic approach to lying,” he says.

**Evidence**: NSA surveillance has revealed Chinese targeting of military and defense contractors.

Volz, Dustin. “U.S. spy agency warns that Chinese hackers target military, defense industry.” Wall Street Journal. 10/20/20. https://www.wsj.com/articles/u-s-spy-agency-warns-beijing-s-hackers-aiming-at-u-s-defense-industry-military-11603206459

The National Security Agency on Tuesday warned that Chinese government hackers were taking aim at U.S. computer networks involved in national defense, characterizing the threat posed by Beijing as a critical priority in need of urgent attention.

The vulnerabilities described in the NSA’s new alert were already known to cybersecurity professionals, but the nation’s premier electronic spy agency for the first time described them as targets of Chinese state-sponsored hacking campaigns. The NSA urged cyber defenders across the Defense Department and within the defense industrial base to take action to guard against Chinese intrusion.

“These networks often undergo a full array of tactics and techniques used by Chinese state-sponsored cyber actors to exploit computer networks of interest that hold sensitive intellectual property, economic, political, and military information,” the alert warned.

**Impact:** A cyber attack would put critical infrastructure at risk.

LaFrance, Adrienne. "When Is Cyberwar Just War?" The Atlantic, 16 May 2017, www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/.

The devastating effects of a massive cyberattack are no more confined to a computer network than any other action carried out online. People use the computers and the internet all the time to make things happen in the physical world. **A cyberattack isn't just a cyberattack. It's an attack. Hospitals, pharmacies, and major corporations like FedEx and the Spanish telecommunications giant Telefonica were among the 200,000 victims hobbled by a global ransomware attack on Friday, which locked people's computers and demanded Bitcoin payment in exchange for access. In the United Kingdom, some hospitals canceled procedures and other appointments as a result.** The software security firm Symantec found that people paid ransoms totaling about $54,000 in the attack, though officials strongly caution against paying such ransoms.

**Analysis**: Spying on permanent residents is an effective way for the NSA to keep tabs on potential threats. At a time where the United States is constantly at risk of being attacked online, the presence of the NSA is an essential deterrent.

## CON – The NSA stops radical anti-government groups

**Argument:** The NSA is now targeting far-right anti-government groups who seek to start a new civil war.

**Warrant**: The US intelligence community is now targeting the Boogaloo movement.

> Klippenstein, Ken. "US intelligence turns to the Boogaloo movement." The Nation. 7/16/20. https://www.thenation.com/article/politics/intelligence-agencies-boogaloo/
>
> The US Intelligence Community, the consortium of spy agencies you most often hear about in the context of things like Russian espionage or Chinese cyberattacks, has a new target: the Boogaloo movement.
> Widely known for their provocative memes and penchant for Hawaiian shirts paired with military fatigues, Boogaloos are a loosely affiliated coalition of far-right anti-government groups who aim to prepare for—or even instigate—a second American civil war. Their love of guns and zealous opposition to government allegedly resulted last month in the murder of two security guards and a police officer. This prompted Attorney General William Barr to announce the formation of a task force to investigate the group.

**Warrant**: The NSA has been involved with a report implicating far-right extremists.

> Klippenstein, Ken. "US intelligence turns to the Boogaloo movement." The Nation. 7/16/20. https://www.thenation.com/article/politics/intelligence-agencies-boogaloo/

The Boogaloo movement has been implicated in a string of horrific murders in the past several months, so it's not surprising that federal agencies would be monitoring them. The report does not disclose which agencies produced the intelligence, but the Intelligence Community isn't a typical organization—it includes within it top-tier intelligence bodies like the CIA, the NSA, and the FBI.

These agencies are often tasked with spying on nation-state adversaries as well as countering their respective intelligence services. Many employees possess top secret security clearances and access to such sensitive information that they are routinely given polygraph tests to ensure that they haven't disclosed secrets without authorization. That the Intelligence Community is monitoring the Boogaloo movement speaks to the seriousness of the threat.

**Impact**: Info from the NSA in tandem with changing policies is leading to reform and more effective handling of extremism.

Klippenstein, Ken. "US intelligence turns to the Boogaloo movement." The Nation. 7/16/20. https://www.thenation.com/article/politics/intelligence-agencies-boogaloo/

As a consequence of the violence, the Defense Department has been quietly debating how to better monitor military personnel for signs of extremism, according to a senior department official who was not authorized to speak publicly. Many among the department's leadership believe that simply monitoring personnel's social media accounts would be effective, but privacy rules often prevent them from doing so, the official explained.

**Analysis**: The NSA is known for targeting terrorist organizations, but rarely do Americans consider domestic terrorists among those ranks. In reality, the threat of far-right extremism is

greater than that of international terrorism for the average American, and it's important for organizations like the NSA to stay ahead of those groups.

## CON – The NSA saves lives

**Argument:** Intrusions into privacy are justified so long as security is preserved, and the NSA has proven that it can stop attacks and save lives.

**Warrant**: NSA has struck an appropriate balance to where it preserves privacy while saving lives.

> Epstein, Jennifer. "Obama: Lives have been saved by surveillance." Politico. 6/19/13. https://www.politico.com/story/2013/06/barack-obama-surveillance-programs-nsa-leak-093035
>
> President Barack Obama took office with a "healthy skepticism" of national security surveillance programs, but has scrutinized them to a point where he is confident his administration has "struck the appropriate balance," he said Tuesday.
> "This applies very narrowly to leads that we have obtained on issues related to terrorism or proliferation of weapons of mass destruction," he said in Berlin at a joint press conference with German Chancellor Angela Merkel. "This is not a situation where we are rifling through, you know, the ordinary emails of German citizens or American citizens or French citizens or anyone else."

**Evidence**: At least 50 terrorist threats have been stopped around the globe by the NSA

> Epstein, Jennifer. "Obama: Lives have been saved by surveillance." Politico. 6/19/13. https://www.politico.com/story/2013/06/barack-obama-surveillance-programs-nsa-leak-093035
>
> Ultimately, he said, "lives have been saved" because of the cautious execution of the surveillance systems. "We know of at least 50 threats that have been averted" not just

in the United States, but in countries around the world, including Germany. That number, which the administration has been using in recent days to defend its actions, includes plots thwarted by PRISM and by the National Security Agency's scrutiny of phone metadata.

**Impact**: Dozens of attacks have been foiled by the NSA, saving countless lives.

Whitesides, John. "NSA director says surveillance helped stop 'dozens' of attacks." Reuters. 6/12/20. https://www.reuters.com/article/us-usa-security/nsa-director-says-surveillance-helped-stop-dozens-of-attacks-idUSBRE95910O20130612

In his first appearance before Congress since an NSA contractor lifted the veil on the agency's broad monitoring of phone and internet data, General Keith Alexander defended the program as an essential tool in the fight against terrorism.
"It's dozens of terrorist events that these have helped prevent," the NSA director told a U.S. Senate committee. "Both here and abroad, in disrupting or contributing to the disruption of terrorist attacks."
Relying on documents from NSA contractor Edward Snowden, Britain's Guardian newspaper and the Washington Post revealed last week the vast U.S. government effort to monitor phone and internet data at big companies such as Google Inc and Facebook Inc.
Alexander said the disclosures, which have sparked a criminal investigation and an internal Obama administration review of the potential national security damage, had jeopardized safety in the United States and elsewhere.

**Analysis**: The NSA's ability to stop threats before they come to fruition is unrivaled in terms of its ability to save lives. While other counterterror measures can be effective, the NSA is one of the only institutions that can preemptively address the problem.

## CON – The NSA is cost-efficient

**Argument:** The NSA is one of the most cost-effective surveillance organizations.

**Warrant**: It only costs six and a half cents per hour to use NSA surveillance tech.

Cohen, Drew. "It costs the government just 6.5 cents an hour to spy on you." Politico. 2/10/14. https://www.politico.com/magazine/story/2014/02/nsa-surveillance-cheap-103335

In this, he's pushing on an open door. By now, most Americans agree that the NSA surveillance program, brought to light by leaked documents from former NSA contractor Edward Snowden, went "too far." But what Greenwald and many other analysts often miss is that an overzealous security apparatus is not the driving reason behind government overreach. A lot of it has to do with dollars and cents: **The price of surveillance technology has dropped so precipitously over the past two decades that once the agency overcame any moral objections, few practical considerations stood in its way of implementing a system that could monitor 315 million Americans every day. Indeed, one estimate tagged the NSA's annual surveillance costs at $574 per taxpayer, a paltry 6.5 cents an hour.**

**Warrant**: Investment in the NSA is now paying off by saving lives.

Epstein, Jennifer. "Obama: Lives have been saved by surveillance." Politico. 6/19/13. https://www.politico.com/story/2013/06/barack-obama-surveillance-programs-nsa-leak-093035

> President Barack Obama took office with a "healthy skepticism" of national security surveillance programs, but has scrutinized them to a point where he is confident his administration has "struck the appropriate balance," he said Tuesday.
> "This applies very narrowly to leads that we have obtained on issues related to terrorism or proliferation of weapons of mass destruction," he said in Berlin at a joint press conference with German Chancellor Angela Merkel. "This is not a situation where we are rifling through, you know, the ordinary emails of German citizens or American citizens or French citizens or anyone else."

**Evidence**: At least 50 terrorist threats have been stopped around the globe by the NSA

> Epstein, Jennifer. "Obama: Lives have been saved by surveillance." Politico. 6/19/13. https://www.politico.com/story/2013/06/barack-obama-surveillance-programs-nsa-leak-093035

> Ultimately, he said, "lives have been saved" because of the cautious execution of the surveillance systems. "We know of at least 50 threats that have been averted" not just in the United States, but in countries around the world, including Germany. That number, which the administration has been using in recent days to defend its actions, includes plots thwarted by PRISM and by the National Security Agency's scrutiny of phone metadata.

**Analysis**: Ultimately, many debaters will try to argue that the NSA is too expensive. But looking at NSA spending comparatively, it's actually extremely cheap for them to spy on residents and citizens. Thus, because lives are invaluable, it's easy to argue that the low cost is easily justified by the lives saved.

# CON – The NSA surveillance program is justified under the constitution

**Argument:** NSA surveillance is constitutional and unconstitutional parts have ended.

**Warrant:** the narrow NSA fits into different exceptions to the fourth amendment

Blake Covington Norvell, 2009, "The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation," Yale Journal of Law, https://yjolt.org/constitution-and-nsa-warrantless-wiretapping-program-fourth-amendment-violation

The expansive model of the NSA wiretapping program, which allows a member of the Executive Branch to monitor certain international phone calls without a warrant under the justification of protecting the security of the nation, violates the Fourth Amendment of the Constitution. The Fourth Amendment contains a warrant requirement and a reasonableness requirement. The expansive model of the NSA program violates both the warrant requirement and reasonableness test of the Fourth Amendment. Furthermore, the expansive model of the NSA program does not fit within any existing Fourth Amendment exception. Therefore, the expansive model NSA warrantless wiretapping program is unconstitutional. By contrast, the narrow model of the NSA program does not violate the Fourth Amendment of the Constitution. **The narrow model of the NSA program does not fall within the ambit of the Fourth Amendment and, even if it did, the program would qualify for an exception under the special needs exception and would also qualify under a narrow foreign surveillance exception to the Fourth Amendment. Additionally, the narrow model of the NSA program complies with the reasonableness requirement of the Fourth Amendment.**

**Warrant:** NSA is protected by the third part exception to the fourth amendment

Timothy M. Phelps, 12-27-2013, "Federal judge says NSA phone data collection is constitutional," Los Angeles Times, https://www.latimes.com/nation/la-na-nsa-telephones-20131228-story.html

"The government learned from its mistake and adapted to confront a new enemy, a terror network capable of orchestrating attacks across the world," he wrote. At issue is the NSA's collection of "metadata" — information such as which numbers are called from other numbers and how long the calls last — from virtually all telephone calls made within or from the U.S. While that data collection is vast, Pauley said, **a previous Supreme Court ruling has made clear that the 4th Amendment does not protect information that a person turns over to someone else, including a telephone company**. "**When a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information,"** Pauley wrote. Less than two weeks ago, the NSA's critics celebrated a victory in federal court as **a district judge in Washington, D.C., ruled that the wholesale collection of metadata did violate the Constitution's ban on unreasonable searches.** Both rulings are certain to be appealed — the Washington decision to the D.C. Circuit Court of Appeals and Pauley's to the New York-based 2nd Circuit. Ultimately, whichever side loses in the appeals courts probably will ask the Supreme Court to rule on the issue.

**Argument:** the NSA no longer does unconstitutional things

**Warrant:** NSA shut down unconstitutional bulk collection program

Charlie Savage, 3-4-2019, "Disputed N.S.A. Phone Program Is Shut Down, Aide Says (Published 2019)," New York Times, https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html

> The National Security Agency has shut down a controversial program that collects domestic phone and text records, a senior Republican congressional aide said.
> WASHINGTON **— The National Security Agency has quietly shut down a system that analyzes logs of Americans' domestic calls and texts, according to a senior Republican congressional aide, halting a program that has touched off disputes about privacy and the rule of law since the Sept. 11 attacks.** The agency has not used the system in months, and the Trump administration might not ask Congress to renew its legal authority, which is set to expire at the end of the year, according to the aide, Luke Murry, the House minority leader's national security adviser.

**Analysis**: Surveillance can be justified under the constitution, as it is in this instance. The highly publicized instances of NSA invasion of privacy were part of a cancelled program, so there are no obvious aspects of NSA surveillance that is unconstitutional as of now.

## CON – The NSA surveillance program is well regulated

**Argument:** The NSA is designed to protect citizens, and it does so through surveillance, but there are a number of checks on that power to ensure surveillance is justified.

**Warrant:** The FBI, and any governmental investigative agency, has an obligation protect citizens from the government too.

> Mukasey, Michael B. "THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS" Justice.gov. 29 September 2008. https://www.justice.gov/archive/opa/docs/guidelines.pdf
>
> "The general objective of these Guidelines is **the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States.** At the same time**, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people.** The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. **They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.** "

**Warrant:** FISA laws allow surveillance, just targeted and with proper justification and process to protect citizens.

Scott, Jeramie.“Foreign Intelligence Surveillance Act.” Electronic Privacy Information Center. 2020. https://epic.org/privacy/surveillance/fisa/

**“Under the Fourth Amendment, a search warrant must be based on probable cause to believe that a crime has been or is being committed.** This is not the general rule under FISA: **surveillance under FISA is permitted based on a finding of probable cause that the surveillance target is a foreign power or an agent of a foreign power, irrespective of whether the target is suspected of engaging in criminal activity.** However, if the target is a "U.S. person," **there must be probable cause to believe that the U.S. person's activities may involve espionage or other similar conduct in violation of the criminal statutes of the United States. Nor may a U.S. person be determined to be an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the Constitution of the United States."**

**Warrant:** There are determined limits to the information from surveilling citizens in courts to ensure legal retrieval of information**.**

McAdams, James G. “Foreign Intelligence Surveillance Act (FISA): An Overview” Federal Law Enforcement Traning Centers. 2020. https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

“**Disclosure by a federal officer or employee of information acquired pursuant to one of the provisions of FISA must be for a lawful purpose and is only permitted where the disclosure is accompanied by an admonishment that use of FISA information or FISA-derived information in a criminal proceeding may only occur with advance authorization of the Attorney General.** When such use is intended, the government, before the trial or other proceeding at which disclosure is to be made, must give notice

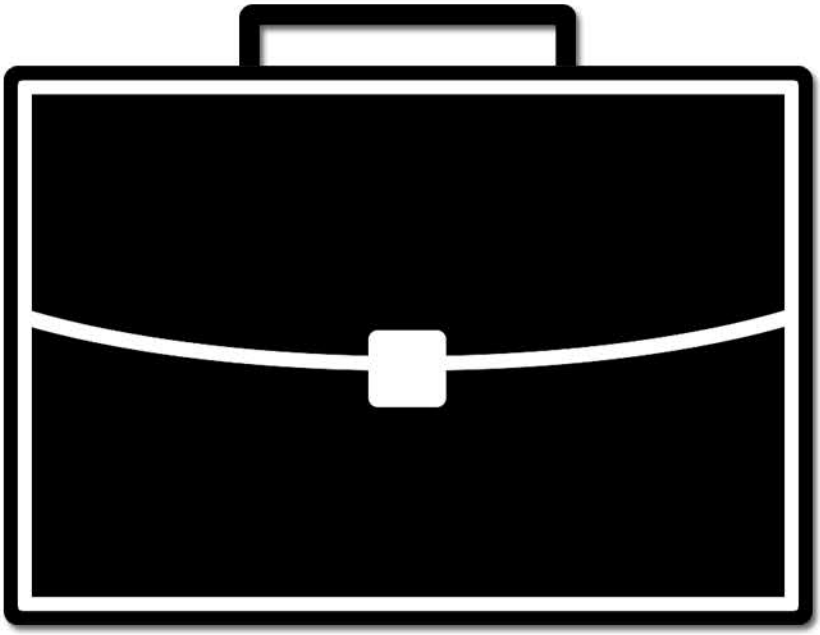
of its intent to the aggrieved person and to the Court. **An aggrieved person may thereafter move to suppress the FISA-related evidence based on either the argument that the FISA information was unlawfully acquired, or that the government the government in some way acted outside of the FISC order. If the court grants that motion, the government must either appeal or refrain from using any evidence that is subject to the court's order.** Denial of the motion by the court will allow the government to use the FISA evidence. "

**Analysis:** For the NSA to use surveillance tactics against American citizens, it first must pass through a system of checks and balances that prevent abuse of power. While there is always a fear of violation of privacy, Americans can feel safe knowing that the NSA is not randomly spying on them.

# Champion Briefs

## January 2021

## Public Forum Brief



# Con Responses to Pro Arguments

## A/2: The NSA surveillance program amounts to authoritarianism

**Response:** There are legal and democratic methods for surveillance without mass surveillance tactics which violate citizens' rights.

**Warrant:** The FBI, and any governmental investigative agency, has an obligation protect citizens from the government too.

Mukasey, Michael B. "THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS" Justice.gov. 29 September 2008. https://www.justice.gov/archive/opa/docs/guidelines.pdf

"The general objective of these Guidelines is **the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States.** At the same time**, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people.** The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. **They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.** "

**Warrant:** FISA laws allow surveillance, just targeted and with proper justification and process to protect citizens.

Scott, Jeramie.“Foreign Intelligence Surveillance Act.” Electronic Privacy Information Center.
2020. https://epic.org/privacy/surveillance/fisa/

**“Under the Fourth Amendment, a search warrant must be based on probable cause to believe that a crime has been or is being committed.** This is not the general rule under FISA: **surveillance under FISA is permitted based on a finding of probable cause that the surveillance target is a foreign power or an agent of a foreign power, irrespective of whether the target is suspected of engaging in criminal activity.** However, if the target is a "U.S. person," **there must be probable cause to believe that the U.S. person's activities may involve espionage or other similar conduct in violation of the criminal statutes of the United States. Nor may a U.S. person be determined to be an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the Constitution of the United States."**

**Warrant:** There are determined limits to the information from surveilling citizens in courts to ensure legal retrieval of information**.**

McAdams, James G. “Foreign Intelligence Surveillance Act (FISA): An Overview” Federal Law Enforcement Traning Centers. 2020. https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

“**Disclosure by a federal officer or employee of information acquired pursuant to one of the provisions of FISA must be for a lawful purpose and is only permitted where the**

**disclosure is accompanied by an admonishment that use of FISA information or FISA-derived information in a criminal proceeding may only occur with advance authorization of the Attorney General.** When such use is intended, the government, before the trial or other proceeding at which disclosure is to be made, must give notice of its intent to the aggrieved person and to the Court. **An aggrieved person may thereafter move to suppress the FISA-related evidence based on either the argument that the FISA information was unlawfully acquired, or that the government the government in some way acted outside of the FISC order. If the court grants that motion, the government must either appeal or refrain from using any evidence that is subject to the court's order.** Denial of the motion by the court will allow the government to use the FISA evidence. "

**Analysis:** The United States, has a system in place where the government does not have to engage in mass surveillance as an abuse of power. There is a set of checks and legal paths to protect citizens and give them legal recourse to address abuses. There is no need for a government, especially the United States to go outside of its boundaries when there are ample means at their disposal.

**Response:** Authoritarian mass surveillance has not been effective in protecting against dangers foreign or domestic.

Kirchner, Lauren. "What's the Evidence Mass Surveillance Works? Not Much." Propublica.org. 18 Nov 2015. https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much

"**An internal review of the Bush administration's warrantless program –** called Stellarwind – **found it resulted in few useful leads from 2001–2004, and none after that.** New York Times reporter Charlie Savage obtained the findings through a Freedom

of Information Act lawsuit and published them in his new book, Power Wars: Inside Obama's Post–9/11 Presidency:

**[The FBI general counsel] defined as useful those [leads] that made a substantive contribution to identifying a terrorist, or identifying a potential confidential informant. Just 1.2 percent of them fit that category**. **In 2006, she conducted a comprehensive study of all the leads generated** from the content basket of Stellarwind between March 2004 and January 2006 **and discovered that zero of those had been useful.**

**Warrant:** The mass collection of data isn't even hardly viewed or used.

Michelle Cayford & Wolter Pieters."The effectiveness of surveillance technology: What intelligence officials are saying: The Information Society. 2018. https://www.tandfonline.com/doi/full/10.1080/01972243.2017.1414721

"With the issue of proportionality comes **the question of how much data intelligence agencies collect, particularly in regards to the collection of communications data off the Internet.** On the one hand, modern digital communications have generated massive flows of information. Hayden argues that the only way for agencies to handle these volumes of data is to perform bulk collection. (Hayden, May 2014) On the other hand, **even in collecting this data in bulk, the NSA itself states that it touches a mere 1.6% of Internet traffic. Of that 1.6%, only 0.025% is selected for review and seen by an analyst. In effect, NSA analysts see only 0.00004% of the world's Internet traffic** (NSA, 2013). In a similar vein, Omand strongly denies the accusation that the GCHQ is processing data about everybody (Omand, Dec. 2015)."

**Analysis:** The mass collection of data is not manageable to even search for information and has not led to much actionable information. If surveillance is only collecting the information and not even going through it, there is no point in actually collecting or storing it in the first place. If the information that has been received and looked at hasn't let to helpful information to be

used, then it remains to be questioned if it is worth the time, effort and funding when other strategies exist.

## A/2: The NSA surveillance program can be hacked

**Response:** The Government protections are not enough.

**Warrant:** Hacking from other governments into US data bases is on the rise.

Sobers, Rob. "Hacking Exploits, Examples and Prevention Tips". Varonis. 8 Sept 2020. https://www.varonis.com/blog/government-hacking-exploits/

**"Government hacking exploits, unfortunately, pose a very real threat for organizations of all kinds,** and those of us working in cybersecurity need to be aware of it. **A decade ago, the majority of government-sponsored attacks were launched against other governments, and most aimed at demonstrating a state's capabilities rather than causing real disruption.** There are now signs that this is changing**: governments around the world have ramped up cyber operations** and are increasingly targeting commercial organizations. **In just the last few months, we have seen many government hacking attempts. July 2020. Canada, the UK, and the U.S. announced that hackers associated with Russian intelligence had attempted to steal information related to COVID-19 vaccine development. July 2020. Media reports say a 2018 Presidential finding authorized the CIA to cyber operations against Iran, North Korea, Russia, and China.** The operations included disruption and public leaking of information**. June 2020. Suspected North Korean hackers compromised at least two defense firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defense contractors."**

**Warrant:** US Citizens have little faith that the government can protect their information from being stolen.

Pew Research. "The State of Privacy in Post-Snowden America."

Pewresearch.org. 21 Sept 2016. https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

**"Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them – particularly when it comes to the use of online tools. And they exhibited a deep lack of faith in organizations of all kinds, public or private, in protecting the personal information they collect.** Only tiny minorities say they are "very confident" that the records maintained by these organizations will remain private and secure."

**Warrant:** The government has a duty to protect its citizens.

Eggers, William. "Government's cyber challenge: Protecting sensitive data for the public good." Deloitte Insights. 25 July 2016 https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html

**Whatever the motive, it's clear that governments are the highest-value targets for hackers today. Thus, it's critical that agencies invest in strong cyber defenses—stronger, if anything, than those found in the private sector.** At the state and local levels in particular, however, most agencies simply are devoting too little manpower and funding to the problem.

**New thinking in this arena involves three fundamental capabilities built around being secure, vigilant, and resilient.** These three principles reflect the fact that defense mechanisms must evolve. **Government agencies can't rely on perimeter security alone—they should also build strong capabilities for detection, response, reconnaissance, and recovery.** The SANS Institute, which performs security training and research, codifies this as a guiding principle: **"Prevention is ideal, but detection is a**

**must."** And given Estonia's experience after removing the Soviet statue, you can see why effective recovery plans are important.

**Furthermore, officials must relinquish a zero-tolerance mindset—they should accept risk while trying to minimize it as much as possible, especially for top-priority information**. **As Ed Powers writes** in the WSJ Risk & Compliance Journal**: "The reality is that cyber risk is not something that can be avoided; instead, it must be managed. By understanding what data is most important, management can then determine what investments in security controls might be needed to protect those critical assets."**

**Warrant:** Ending surveillance of Citizens is necessary to protect US citizens.

Gandour, Jackson and Human Rights Watch Staff. "US: End Bulk Data Collection Program." Human Rights Watch. 5 Mar 2020. https://www.hrw.org/news/2020/03/05/us-end-bulk-data-collection-program.

**The United States Congress should swiftly pass the Safeguarding American's Private Records Act of 2020 (SAPRA) to end bulk data collection and improve transparency and oversight of surveillance in the US,** Human Rights Watch said today**. The bill would end the bulk collection of US phone metadata by intelligence agencies** authorized under Section 215 of the USA Patriot Act. **Though Section 215 was reformed by the USA Freedom Act of 2015, it still permits the government to collect a staggering amount of data, in secret and without a warrant, on how people use their phones, chilling freedom of expression and association. "Congress should put an end to mass phone metadata collection," said Kian Vesteinsson,** senior law and tech policy officer at Human Rights Watch. **"Though the Safeguarding American's Private Records Act of 2020 could do more to safeguard rights, the bill as written will greatly improve privacy protections for millions of people."**

**Analysis:** The United States government has an obligation to protect its own citizens and the first major step is to improve and enforce the privacy protections they deserve. As hackers, even other governments, are continuing to breach the US governments' own data servers, compromising millions, they must stop collecting this data to ensure it is not stolen and misused.

## A/2: The NSA surveillance program should be ended by the Freedom Act

**Response:** It is not necessary for the government to surveil its own citizens, or lawful permanent residents, without going through the legal channels available.

**Warrant:** The Freedom act maintains targeted surveillance with the necessary warrants and ends the illegal mass surveillance.

Michael J. Orlando. "Joint Statement with Department of Justice Deputy Assistant Attorney General J. Bradford Wiegmann and Susan Morgan, National Security Agency, Before the Senate Judiciary Committee Washington, D.C." FBI.gov. 6 Nov 2019. https://www.fbi.gov/news/testimony/reauthorizing-the-usa-freedom-act-of-2015-110619

"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 significant FISA reforms designed to enhance privacy and civil liberties. It replaced the National Security Agency's (NSA's) bulk telephony metadata collection program with a new legal authority whereby the bulk metadata would remain with the telecommunications service providers. The CDR authority provides a "narrowly-tailored mechanism 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 investigation 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 committee is aware, the NSA recently discontinued the CDR program for technical and operational 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."**

**Warrant:** Even with these limits in place, the FBI has been found to have violated the rights of citizens in failure to comply with the laws.

Goltein, Elizabeth. "How the FBI Violated the Privacy Rights of Tens of Thousands of Americans." Brennan Center for Justice. 22 Oct 2019. https://www.brennancenter.org/our-work/Analysis:opinion/how-fbi-violated-privacy-rights-tens-thousands-americans

**"**In March 2018, the government submitted its annual certifications and procedures to the FISA Court for its approval. **In a decision dated October 18, 2018, and released last week, the FISA Court held that the FBI's minimization procedures violated both the statute and the Fourth Amendment. The court's opinion addresses three main practices by the FBI: downstream collection of certain communications; the FBI's failure to record USP queries; and the FBI's improper use of USP queries."**

**Warrant**: Government surveillance of civilians isn't an effective tool anyway and it isn't worth the violation of rights.

Laperruque, Jake. "The History and Future of Mass Metadata Surveillance". Project on Government Oversight. 11 June 2019. https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/

> "The policy justification for the nationwide bulk collection program crumbled, too**. The Obama Administration initially responded to the Snowden disclosures by claiming the programs had discovered or disrupted over 50 terrorist plots. But as Congress pressed the NSA to prove it, the number dropped from dozens to potentially four to just one, and that one case was revealed not to be a terrorist plot but a material support case involving just $8,000. The Privacy and Civil Liberties Oversight Board**, as it announced in its report**, also found that there was "no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack." And the President's Review Group on Surveillance**, a specially created task force of experts including former high-ranking intelligence officials, **concluded bulk collection "was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional [i.e., targeted] section 215 orders." Eventually, even the intelligence community acknowledged that ending the program would not harm national security."**

**Analysis:** The government has legal channels to surveil citizens with proof of illegal activity without the need to do so illegally. The Fact that government agencies continually break their own laws, and violate the rights of citizens without their knowledge is of grave concern. Enhancing limits and ending Governmental surveillance of citizens and lawful permanent residents is a vital step in fulfilling their responsibility and upholding the law and spirit of the law. Doing so is not taking away any tools to solve crimes, prevent terror, or in any way inhibit their duty.

**Response:** Government Surveillance suppresses and hurts individuals and society rather than keeping it safe.

**Warrant:** Mass surveillance only suppressed society, doesn't help solve terrorism.

Munn, Nathan. “HOW MASS SURVEILLANCE HARMS SOCIETIES AND INDIVIDUALS - AND WHAT YOU CAN DO ABOUT IT”. Canadian Journalists for Free Expression. 8 Nov 2019. **https://www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it#:~:text=Evidence%20shows%20that%20mass%20surveillance,to%20not%20prevent%20terrorist%20attacks.**

**“**While many people immediately recognize the problems that arise from this kind of mass surveillance, others have no issues with the practice**. A common argument that skeptics use to brush off concerns about mass surveillance is that “only people who have something to hide” need to worry about it.**
**This is a dangerous position to take for anyone who cares about democratic values, such as free expression, freedom of political affiliation and the right to privacy. Evidence shows that mass surveillance erodes intellectual freedom and damages the social fabric of affected societies; it also opens the door to flawed and illegal profiling of individuals.** Mass surveillance has also been shown to not prevent terrorist attacks. **Evidence shows that even the possibility of being under surveillance changes the way people think and act, causing them to avoid writing or talking about sensitive or controversial subjects—discussions that are necessary for the functioning of a free society. Beyond this ‘self-censorship’, the mass monitoring of citizens’ communications and movements achieves only one thing: the development of mutual mistrust between the individual and the state.”**

**Warrant:** You do not have to be doing anything wrong to be hurt by surveillance.

Richards, Neil M. “The Dangers of Surveillance.” Harvard Law Review. 20 May 2013**. https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/**

"If you haven't done anything wrong, you have nothing to fear."

**This is a typical argument used by governments and other groups to justify their spying activities.** Upon cursory inspection**, it seems to make sense as most people are law-abiding citizens, most ostensibly will not be targeted for surveillance and it will not impact their lives, while making their lives more comfortable and safer through the elimination of criminals.** Thus, the government's use of closed-circuit television cameras in public spaces, warrantless wiretapping, and library record checks have the potential to save lives from criminals and terrorists with only minimal invasion of its citizens' privacy. Next, **this argument fails to take into consideration a number of important issues when collecting personally identifiable data or recordings. First, that such practices create an archive of information that is vulnerable to abuse by trusted insiders.** One example emerged in September of 2007 when **Benjamin Robinson, a special agent of the Department of Commerce, was indicted for using a government database** called the Treasury Enforcement Communications System (TECS) **for tracking the travel patterns of an ex-girlfriend and her family. Records show that he used the system illegally at least 163 times before he was caught (Mark 2007). With the expansion of surveillance, such abuses could become more numerous and more egregious as the amount of personal data collected increases.**

**Analysis:** The current system and protections promised by the Freedom Act are not being met by the federal government, especially when it comes to potential issues for innocent individuals caught up in surveillance. Their private thoughts, searches, and contact with others, may lead to potential legal issues without their knowing that it is occurring and is clearly a concern, even if you are not doing anything illegal.

## A/2: The NSA surveillance program harms mental health

**Response:** The government surveillance is terrorism on its own citizens.

**Warrant:** Terrorism is not just violent attacks by foreign assailants: .

Dale L. Watson. "Before the Senate Select Committee on Intelligence." FBI. 6 Feb 2002. https://www.fbi.gov/news/testimony/the-terrorist-threat-confronting-the-united-states

**"Domestic terrorism is the unlawful use, or threatened use, of violence by a group or individual based and operating entirely within the United States (or its territories) without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."**

**Warrant:** Government surveillance is totalitarian and violates the liberties of its citizens for social objectives.

Chambers, Chris. "NSA and GCHQ: the flawed psychology of government mass surveillance." The Guardian. 26 Aug 2013. https://www.theguardian.com/science/head-quarters/2013/aug/26/nsa-gchq-psychology-government-mass-surveillance

"**There are two ways to resolve this conflict between the motivations of elected representatives and security services. One is to embrace totalitarianism**, breaking all bonds of social identity between politicians and the electorate. **In this (unpalatable) scenario, democracy converts to a police state in which all parts of government are**

**seen by the populace as an outgroup. An alternative is to put an end to mass surveillance, forcing the security services to fall in line with the parts of government that value liberty.** What seems clear is that the government can't moonlight as both an ingroup and an outgroup – **it can't claim to serve the liberty of its citizens while in the same breath violating that liberty.** If they achieve nothing else, the Snowden revelations throw this contradiction into sharp relief."

**Warrant:** The government must be kept in check even in the face of future terrorism.

Jacobs, Deborah. "Safe & Free-Civil Liberties in the Age of Terrorism." ACLU New Jersey. 1999.
https://www.aclu-nj.org/theissues/opengovernment/safefreecivillibertiesinth

**"In past times of crisis, our government has harassed, investigated and arrested people solely because of their race, religion, national origin, speech or political beliefs. We must not allow this to happen again, even as we work together to protect ourselves from future terrorist attacks."**

**Response:** Government Surveillance is intended to control and intimidate citizens.

**Warrant:** Mass Surveillance is the tool of coercion and control.

Shaw. Jonathan. "Assaults on Privacy in America." The Watchers.
JANUARY-FEBRUARY 2017. https://harvardmagazine.com/2017/01/the-watchers

"**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 pervasive surveillance," reiterates security expert Bruce Schneier, a fellow at the Berkman** and in the cybersecurity program of the Kennedy School's Belfer Center for Government 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 effectiveness 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."**

**Warrant:** Government surveillance controls self determination by commodifying our identities.

Ellis, D., Harper, D. & Tucker, I. The psychology of surveillance:
Experiencing the 'Surveillance Society'. The Psychologist. 29 (September), 682-685. ISSN: 0952- 8229: https://thepsychologist.bps.org.uk/volume-29/september/experiencingsurveillance-society

"**This exchange presents new challenges to notions of privacy and identity. Our thoughts, feelings and desires – as represented in our search histories – are now recorded in the databases of huge technology companies. People risk becoming commodified, through their personal information. In social psychological terms**, we could say that with the incessant rise in the prominence of information technologies in

everyday life, **people are increasingly defined by information as well as biology. It is also notable that much of this dataveillance takes place in 'private' spaces (e.g. the home). The spread of surveillance across public and private space presents the potential for people's sense of self and identity to be shaped by surveillance.**

**Warrant:** Government surveillance leads to fear and collective conformity.

Nathan Munn. "HOW MASS SURVEILLANCE HARMS SOCIETIES AND INDIVIDUALS - AND WHAT YOU CAN DO ABOUT IT." Canadian Journalists for Free Expression. 8 Nov 2016. https://www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it#:~:text=Evidence%20shows%20that%20mass%20surveillance,to%20not%20prevent%20terrorist%20attacks.

**"According to Glenn Greenwald, governments, corporations and other institutions of authority "crave surveillance…precisely because the possibility of being monitored radically changes individual and collective behavior," leading to "fear and collective conformity."**

**Analysis:** Government surveillance of citizens and lawful permanent residents is nothing more than government terrorism on its own citizens. It creates self censorship, suppresses free expression and open civic discourse, and conformity for mass control of citizens. While done in the name of preventing terrorism and crime, the unintended consequences are evident and clearly a violation of civic rights. This terrorism is contributing to the increase of mental health crisis in the United States which, while a pandemic virus cannot be controlled, government surveillance can be.

## A/2: The NSA surveillance program runs contrary to the right to be forgotten

**Response:** Phone calls, data, and browsing histories are not public information.

**Warrant:** The 4th Amendment protects against invasion or search and seizure of personal information.

> Ingram, David. "Can the government look at your web habits without a warrant? Senators hope to clarify that." NBC News. 15 May 2020. https://www.nbcnews.com/tech/security/can-government-look-your-web-habits-without-Warrant:senators-hope-n1207936
>
> **"The Fourth Amendment guarantees Americans the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and lays out the requirements for the government to get a warrant.** People may wonder if the amendment has lost some effect after more than 220 years. **Some 63 percent of Americans do not think it is possible to go about their daily lives without government entities collecting data about them, according to the Pew Research Center, and 84 percent say they feel very little or no control over data collected by the government. "Americans deserve the strong protections for their online activities provided by the proposed amendment," Ferras Vinh, a policy manager at Mozilla, said in a statement. "It would have made clear that the government needs a warrant for browsing and search history, which may provide an intimate portrait of our health, our finances, and our daily lives."**

**Warrant:** The government regulates tech but not themselves.

Global Legal Group. "USA: Data Protection Laws and Regulations". ICLG. 7 June 2020.https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq.

**"Unlawful surveillance continues to be a major concern in the United States and the Federal government** and most states have enacted legislation that criminalizes recording communications without obtaining consent from either one or all of the parties, depending on the statute. **A Number of states have enacted discrete laws pertaining to surveillance, including cellular location tracking, drone photography, and even smart tv "snooping' features. State laws also may impose restrictions and obligations on businesses relating to the collection, use and disclosure, security, or retention of special categories of information, such as biometric data, medical records, SSNs, driver's license information, email addresses, library records, television viewing habits, financial records, tax records, insurance information, criminal justice information, phone records, and education records, just to name some of the most common."**

**Warrant:** Right to Privacy includes individual autonomy over their information.

Sharp, Tim. "Right to Privacy: Constitutional Rights and Privacy Laws." Live Science. 12 June 2013. https://www.livescience.com/37398-righttoprivacy.html#:~:text=No%20state%20shall%20make%20or,equal%20protection%20of%20the%20laws.

**"A person has the right to determine what sort of information about them is collected and how that information is used**. In the marketplace, the FTC enforces this right through laws intended to prevent deceptive practices and unfair competition**. The Privacy Act of 1974 prevents unauthorized disclosure of personal information held by**

**the federal government. A person has the right to review their own personal information, ask for corrections and be informed of any disclosures."**

**Warrant:** Right to Life, Liberty and Pursuit of happiness is integral with right to privacy and to control one's own information.

Warren; Brandeis. "The Right to Privacy". Harvard Law Review. Vol. IV. 15 Dec 1890. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

**"the right to life has come to mean the right to enjoy life,—the right to be let alone . . . .** This development of the law was inevitable**. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature."**

**Analysis:** Individuals have the right to privacy and control of the information that they put out, whether it is personal thoughts, phone calls, searches on the internet. They have the right to determine if they want it to be stored, deleted, etc and it is an ingrained part of our country's core values of "life, liberty, and pursuit of happiness." The Government surveillance and storage of personal data, browser histories, phone calls etc infringes on these core values, violates their own laws on tech corporations, and can lead to life altering damages on individual's lives.

## A/2 - NSA Surveillance hurts U.S. credibility

**Response** foreign countries care more that the U.S. spied on them than that the U.S. spied on itself and there are alternate causes to a decline in credibility.

**Warrant:** surveillance of foreign nationals continues in the aff world

AP, 10-26-2013, "NSA spying threatens to hurt US foreign policy," AP NEWS, https://apnews.com/article/27ad701f742447568b539a426ade4c38

WASHINGTON (AP) — Secretary of State John Kerry lands in Rome and Paris to talk about Mideast issues but is confronted by outrage over U.S. spying abroad. President **Barack Obama has defended surveillance activities to leaders of Russia, Mexico, Brazil, France and Germany. Classified disclosures by former National Security Agency contractor Edward Snowden about NSA tactics — that allegedly include tapping as many as 35 world leaders' cellphones — threaten to harm U.S. foreign policy in several areas.** ADVERTISEMENT In Washington on Saturday, demonstrators held up signs reading "Thank you, Edward Snowden!" as they marched near the U.S. Capitol to demand that Congress investigate the NSA's mass surveillance programs. "The magnitude of the eavesdropping is what shocked us," former French Foreign Minister Bernard Kouchner said in a radio interview. "Let's be honest, we eavesdrop too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous." The British ambassador to Lebanon, Tom Fletcher, tweeted this week: "I work on assumption that 6+ countries tap my phone. Increasingly rare that diplomats say anything sensitive on calls."

**Warrant:** NSA organization, not surveillance on citizens, hurts credibility and encourages poor behavior

Henry Farrell, 2-10-2016, "The NSA is massively reorganizing itself. That's going to hurt its credibility," https://www.washingtonpost.com/news/monkey-cage/wp/2016/02/10/the-nsa-is-massively-reorganizing-itself-that's-going-to-hurt-its-credibility/

Bureaucratic politics mean that people's careers and resources depend on advocating the priorities of their own part of the organization, defending it against others with clashing aims and, if possible, increasing their share of resources by taking it away from others. Hence, **when the NSA had visibly separate organizational structures, with separate budget lines for offense** (attacking other people's systems) **and defense** (defending one's own systems), **it helped reassure outside observers a little that the defense perspective has its internal advocates within the organization, even if those advocates often lost. In a combined structure, that is no longer the case. Outsiders will find it harder to adjudicate whether the organization is prepared to prioritize defense over offense** (at least some of the time). **And that has consequences. It may make America's adversaries more likely to invest in cyber techniques, to defend themselves against the perceived increased risk of U.S. incursions, perhaps creating a spiral of decreased security in which states start to arm themselves against each other**. It may make it less likely that businesses will trust the NSA with information about vulnerabilities — since they do not know if this information will be used to fix the vulnerabilities or to exploit them. **It may further erode the dominance of U.S. security standards (and U.S. firms) in world markets. It will surely make the cryptographic community more skeptical of cooperating with the NSA. Because the NSA is the kind of organization it is, it has great difficulty in communicating its true intentions and getting others to believe them, even when it wants to. Split organizational structures** (which are costly because they go along with budget lines, factional fighting and so on**) are one of the very few ways that it can credibly communicate its priorities to outsiders**, and reassure them, if it wants to reassure them, that it is interested in protecting networks as well as subverting them. By getting rid of the split, the NSA,

whether it likes it or not, is making it harder for others to trust its claims. **If one were a cynical game theorist one could go further, and argue that because outsiders are even less likely to trust the NSA than they were, the NSA has less to gain from trust-based cooperation, and hence is more likely to behave in an untrustworthy fashion.**

**Warrant:** other countries didn't care about NSA revelations

Michael J. Green, 11-4-2013, "The NSA Leaks Are Bad, but Syria Hurt U.S. Credibility More," Foreign Policy, https://foreignpolicy.com/2013/11/04/the-nsa-leaks-are-bad-but-syria-hurt-u-s-credibility-more/

And yet**, what has struck me in numerous recent discussions with senior politicians and officials from East Asian allies is how little the NSA revelations come up in conversation.** Our **East Asian allies know that Henry Stimson ("gentlemen do not read other gentlemen's mail") is no longer Secretary of State. With a rising China and a nuclear armed North Korea, they have become quintessential realists and know how the game is played. What worries them much, much more than Snowden is Syria.** It comes up in private conversation all the time. I have tried to explain that our "never mind" on Syria should not lead governments in Seoul or Tokyo to question the resolve of Americans to defend our allies against growing threats in East Asia. I have pointed to recent surveys showing that more Americans than ever say we should fight to protect Korea if it comes under attack from the North. And I have noted that despite the Asia pivot's drift in recent months, the U.S. military continues giving top priority to the region.

**Analysis:** there are so many alternate causes to this argument it is difficult for the pro to generate much unique offense. The con should exploit this as much as possible, however do not spend too much time on this argument as pro teams may be inclined to use it as a time suck.

## A/2 - NSA surveillance is unconstitutional

**Response** NSA surveillance is constitutional and unconstitutional parts have ended.

**Warrant:** the narrow NSA fits into different exceptions to the fourth amendment

Blake Covington Norvell, 2009, "The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation," Yale Journal of Law, https://yjolt.org/constitution-and-nsa-warrantless-wiretapping-program-fourth-amendment-violation

The expansive model of the NSA wiretapping program, which allows a member of the Executive Branch to monitor certain international phone calls without a warrant under the justification of protecting the security of the nation, violates the Fourth Amendment of the Constitution. The Fourth Amendment contains a warrant requirement and a reasonableness requirement. The expansive model of the NSA program violates both the warrant requirement and reasonableness test of the Fourth Amendment. Furthermore, the expansive model of the NSA program does not fit within any existing Fourth Amendment exception. Therefore, the expansive model NSA warrantless wiretapping program is unconstitutional. By contrast, the narrow model of the NSA program does not violate the Fourth Amendment of the Constitution. **The narrow model of the NSA program does not fall within the ambit of the Fourth Amendment and, even if it did, the program would qualify for an exception under the special needs exception and would also qualify under a narrow foreign surveillance exception to the Fourth Amendment. Additionally, the narrow model of the NSA program complies with the reasonableness requirement of the Fourth Amendment.**

**Warrant:** NSA is protected by the third part exception to the fourth amendment

Timothy M. Phelps, 12-27-2013, "Federal judge says NSA phone data collection is constitutional," Los Angeles Times, https://www.latimes.com/nation/la-na-nsa-telephones-20131228-story.html

"The government learned from its mistake and adapted to confront a new enemy, a terror network capable of orchestrating attacks across the world," he wrote. At issue is the NSA's collection of "metadata" — information such as which numbers are called from other numbers and how long the calls last — from virtually all telephone calls made within or from the U.S. While that data collection is vast, Pauley said, **a previous Supreme Court ruling has made clear that the 4th Amendment does not protect information that a person turns over to someone else, including a telephone company**. "**When a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information,"** Pauley wrote. Less than two weeks ago, the NSA's critics celebrated a victory in federal court as **a district judge in Washington, D.C., ruled that the wholesale collection of metadata did violate the Constitution's ban on unreasonable searches.** Both rulings are certain to be appealed — the Washington decision to the D.C. Circuit Court of Appeals and Pauley's to the New York-based 2nd Circuit. Ultimately, whichever side loses in the appeals courts probably will ask the Supreme Court to rule on the issue.

**Argument:** the NSA no longer does unconstitutional things

**Warrant:** NSA shut down unconstitutional bulk collection program

Charlie Savage, 3-4-2019, "Disputed N.S.A. Phone Program Is Shut Down, Aide Says (Published 2019)," New York Times, https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html

The National Security Agency has shut down a controversial program that collects domestic phone and text records, a senior Republican congressional aide said.
WASHINGTON **— The National Security Agency has quietly shut down a system that analyzes logs of Americans' domestic calls and texts, according to a senior Republican congressional aide, halting a program that has touched off disputes about privacy and the rule of law since the Sept. 11 attacks.** The agency has not used the system in months, and the Trump administration might not ask Congress to renew its legal authority, which is set to expire at the end of the year, according to the aide, Luke Murry, the House minority leader's national security adviser.

**Warrant:** NSA bulk collection declared illegal

Josh Gerstein, 9-2-2020, "Court rules NSA phone snooping illegal after 7-year delay," POLITICO, https://www.politico.com/news/2020/09/02/court-rules-nsa-phone-snooping-illegal-407727

**The National Security Agency program that swept up details on billions of Americans' phone calls was illegal and possibly unconstitutional, a federal appeals court ruled Wednesday.** However, **the unanimous three-judge panel of the 9th Circuit Court of Appeals said the role the so-called telephone metadata program played in a criminal terror-fundraising case against four Somali immigrants was so minor that it did not undermine their convictions.** The long-awaited decision is a victory for prosecutors, but some language in the court's opinion could be viewed as a rebuke of sorts to officials who defended the snooping by pointing to the case involving Basaaly Moalin and three other men found guilty by a San Diego jury in 2013 on charges of fundraising for Al-Shabaab. **Judge Marsha Berzon's opinion**, which contains a half-dozen references to the role of former NSA contractor and whistleblower Edward Snowden in disclosing the NSA metadata program**, concludes that the "bulk collection" of such data violated the Foreign Intelligence Surveillance Act.**

## A/2 - Ending NSA Surveillance ends surveillance on minorities

**Response** as the NSA program was shut down, the majority of race based surveillance is conducted by local communities, ICE, and the FBI.

**Warrant:** the dragnet program was shut down in 2018

> Devlin Barrett, 9-4-2020, "Surveillance program that gathered Americans' phone data was illegal, court finds," https://www.washingtonpost.com/national-security/phone-records-surveillance-edward-snowden/2020/09/02/97f26498-ed67-11ea-99a1-71343d03bc29_story.html
>
> The court also rejected the Justice Department's argument that the call records were properly obtained because they were relevant to a terrorism investigation. That argument, they wrote, "depends on an after-the-fact determination of relevance: once the government had collected a massive amount of call records, it was able to find one that was relevant to a counterterrorism investigation." The problem, the judges wrote, is that the Foreign Intelligence Surveillance Act "required the government to make a showing of relevance to a particular authorized investigation before collecting the records." AD Therefore, **the judges found, "the telephony metadata collection program exceeded the scope of Congress's authorization" and therefore violated the law. The ruling marks the second time a federal appeals court has found the bulk phone records program illegal. In 2015, a federal appeals court in New York issued a scathing opinion finding the program had wrongly gathered a "staggering" volume of information about Americans to conduct "sweeping surveillance." That same year, Congress ended the program, replacing it with a system in which phone companies kept such records and provided information about specific numbers when presented with a court order. That replacement program, however, was deemed so difficult and unhelpful that it was effectively shelved in late 2018.**

**Warrant:** local surveillance against minority communities would still continue

Tawana Petty, 7-10-2020, "Defending Black Lives Means Banning Facial Recognition," Wired, https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/

Despite this, the Detroit Police Department's "Real Time Crime Center" has been using facial recognition since 2017. When combined with Project Green Light, a program in which the city partners with private businesses to install CCTV cameras and give police 24/7 access to footage, facial recognition enables a dystopian surveillance state. What's happening in my city should be a wakeup call for the nation. Those of us who live in Detroit have known for years the human impact of being surveilled. A four-year study that I co-led called Our Data Bodies found that residents could not shake the feeling of being watched, even before the real-time crime surveillance program ramped up. The realities of this brutal surveillance regime heightened concerns and brought Detroit national attention when the country learned of the story of Robert Williams, a Black man who was arrested by Detroit police in front of his wife and children and held for more than 30 hours. Facial recognition falsely accused him of a crime after matching his photo with an image from surveillance footage. The experience was humiliating for Williams, but it could have been much worse. Had he resisted the unjust arrest, which would have been reasonable given the circumstances, he might not have lived to tell his story. We see the videos of the people police hurt and kill—but the surveillance that led to that brutality is often hidden from us. Surveillance is the foundation of modern policing. It has ties to a long racist legacy, from the branding of enslaved people to the Lantern Laws of the 18th century. Police and politicians defend these programs by claiming they are intended to keep people safe. But for Black people, surveillance ain't safety.

**Warrant:** FBI and counter-terrorism task forces preform the majority of racist behavior

Murray, Nancy. "Profiling in the Age of Total Information Awareness." Race & Class 52, no. 2 (October 2010): 3–24. https://doi.org/10.1177/0306396810377002.

**Customary lines of authority and accountability are further blurred by 'Joint Terrorism Task Forces' (JTTFs) which are now based in more than one hundred cities nationwide and draw participants from six hundred state and local agencies and thirty federal operations**. In JTTFs, local and state police are deputised by the FBI and given clearance to conduct 'field investigations of actual or potential terrorism threats'.22 **Often they work side by side with agents from** the 8 Race & Class 52(2) **Defense Department and the Bureau of Immigration and Customs Enforcement (ICE). When local and state police work with JTTFs, they are no longer under the supervision of and accountable to their state and community jurisdictions but instead become federal domestic intelligence agents beyond meaningful state and local contro**l. **As police departments spend more and more resources on 'intelligence' work, and are no longer entirely 'local', their emphasis shifts away from building relationships through the kind of 'community policing' that has long been held up as the best way to overcome anti-police attitudes in communities of colour**. No longer are police focused on investigating crimes that have already occurred, using the traditional criminal justice standard of 'reasonable suspicion' in targeting suspects. **The federal Suspicious Activity Reporting (SAR) initiative plans to enlist some 800,000 local and state police in the filing of 'suspicious activity reports' (SARs) on even the most common everyday behaviours** and the depositing of information in a near real-time 'Information Sharing Environment' (ISE) where it can be accessed by agencies around the country.23 The SARs will be assessed at the nation's seventy-two fusion centres, which will funnel data to the FBI's National Security Branch Center for TIA analysis. What are 'suspicious behaviours'**? Since 9/11, police have followed up on 'tips' they have received from a public prone to rely on racial and religious profiling**. In Massachusetts, for instance, police pursued reports about 'a Middle Eastern looking man who came to buy a used car and ended up

not buying the car and two Middle Eastern looking men who were seen driving a Ryder truck on the expressway'.24 **The SAR initiative may well serve as yet another 'platform for prejudice' that invites racial profiling**.25

**Analysis:** the one thing not to do is downplay the impacts. Instead focus on why the pro could not solve for the impacts. Then if you have evidence that the plan would cause no other plans to pass (political capital warrant, complacency, etc.) put it here to give an impact to this defense.

## A/2 - NSA Surveillance is inefficient

**Response:** NSA surveillance is efficient

**Warrant:** Program is efficient as machines process data, not human analysts

Anna Dorothea Ker, 1-22-2020, "United States Of Surveillance," Privacy Issue, https://theprivacyissue.com/government-surveillance/united-states-of-surveillance-us-history-spying

**Government departments are working closely with private-sector tech companies,** notably the secretive software firm Palantir, founded in 2004 by Peter Thiel and Alex Karp. Palantir had once sold its products to military organizations to track crime and "enemy activity". In 2018, despite protests from its employees, Palantir renewed its contracts with ICE, providing ICE with “investigative case management software” for building extensive databases used to monitor the undocumented immigrants who are being targeted by President Trump’s immigration crackdown, including the separation of children from their families at the border. **Palantir’s databases are designed to quickly and accurately identify patterns and links in large swathes of data, which allows law enforcement officials to efficiently go from knowing one or two data points about a person to creating a highly-specific profile of them – including photos, biometrics, vehicle information, phone records, criminal records, and police reports.** Since Palantir began working with ICE, there has been a sharp increase in arrests for civil immigration violations – 1,525 between October 2017 to 2018, compared to 172 in the previous year.

**Argument:** NSA surveillance is needed even if it’s not efficient

**Warrant:** bulk collection is needed for national security

Peter Margulies, Surveillance By Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights, 68 Fla. L. Rev. 1045. (2016). Available at: http://scholarship.law.ufl.edu/flr/vol68/iss4/3

In contrast**, bulk collection involves the collection of a mass of data, which analysts subsequently query using selectors or other methods.51 In bulk collection, much of the data collected is by definition substantively irrelevant**. Suppose that the government wishes to sort through the content of communications in a foreign state to uncover individuals' efforts to join ISIS, Al Qaeda, or the Taliban. Despite ISIS's popularity in some quarters, in any state only a tiny minority of communications will concern ISIS recruiting—most will deal with countless other more mundane issues, from personal, family, and business matters to entertainment, recreation, and so on.52 However, **collecting these substantively irrelevant communications is nonetheless relevant methodologically to a state's efforts to protect its nationals or those of other countries from ISIS**.53 **Bulk collection ensures that the government has a database that is comprehensive when it searches for specific content about ISIS recruiting**. While scanning is evanescent because information is not stored, collection gives the government access to communications over **time. That enables the government to search more effectively for evolving patterns in ISIS's communications**. For example, if ISIS uses different forms of encryption or code to hide its communications, collecting information in bulk will allow the government to trace the evolution of ISIS's tradecraft. In contrast, relying on scanning or targeted collection fails to reckon with ISIS's ability to transform its tactics.

**Argument:** the NSA no longer does bulk collection

**Warrant:** bulk collection ended in 2015

Corinne Reichert, Laura Hautala, 9-2-2020, "Appeals court finds NSA's bulk phone data collection was unlawful," CNET, https://www.cnet.com/news/appeals-court-finds-nsas-bulk-phone-data-collection-was-unlawful/

**A federal appeals court ruled Wednesday that the US National Security Agency's bulk collection of citizens' phone records was against the law. The program, now ended, collected records from phone carriers about who called whom**. The massive collection went beyond the scope of what Congress allowed under a foundational surveillance law, the panel of judges ruled, adding that the program may have violated the US Constitution. The collection program was first revealed to the public in 2013 by journalists who received a document leak from Edward Snowden, a former NSA contractor. Snowden also revealed several other programs in which the NSA and agencies in cooperating countries tapped into the backbone of the internet in the name of foreign surveillance. The NSA news outraged privacy advocates and US citizens whose data was caught up in the dragnet. It also prompted US tech companies to distance themselves from government spy agencies in an effort to reassure customers that their data was secure. "I never imagined that I would live to see our courts condemn the NSA's activities as unlawful and in the same ruling credit me for exposing them," Snowden tweeted on Wednesday. "And yet that day has arrived." **Congress ended the bulk collection program in 2015 with the approval of the USA Freedom Act, requiring the NSA to stop the collection later that year.** Nonetheless, ACLU senior staff attorney Patrick Toomey called Wednesday's ruling a victory for privacy rights. "The decision also recognizes that when the government seeks to prosecute a person, it must give notice of the secret surveillance it used to gather its evidence," Toomey said. "This protection is a vital one given the proliferation of novel spying tools the government uses today."

**Analysis:** obviously do not say that bulk collection is good and that there is no more bulk collection. However, chose where as a con team you want to fight here and demand that the pro warrant what specific part of NSA surveillance is inefficient. The argument that bulk

collection already ended can cut a lot of pro offensive out of the round and could be read as an overview or even as an observation in constructive. It would be a nice surprise to see a second speaking con read an observation that clarifies the topic in constructive.

## A/2 - NSA Surveillance hurts the economy

**Response-** NSA surveillance is avoidable by businesses and needed

**Warrant:** NSA Surveillance is an unpopular attempt to protect people

Villanova University, 1-15-2020, "Business Intelligence Role in NSA Surveillance Programs," https://www.villanovau.com/resources/bi/business-intelligence-nsa-surveillance/

Human beings today exist in ethereal states. Your name, address, occupation, purchases and favorite television shows are floating through the atmosphere, logged somewhere on the internet, and they have never been easier to track than right now. It's a scary thought, because that level of accessibility makes everyone more vulnerable. But **to the National Security Agency (NSA) and the United States government, that data presents an opportunity to prevent crimes and protect citizens. This advanced surveillance is driven by business intelligence: using data and patterns to make insightful and meaningful decisions. The NSA gathers multitudes of data about the American population, and its goal is to use those findings to keep the country safe from internal and external threats.** Some Americans, however, aren't totally in support of advanced surveillance, according to research by the Pew Research Center. There's no consensus among the public, and a measurable sector remains concerned about the lengths that the government may go, and the rights that may be violated to keep the country safe from harm.

**Warrant:** businesses can push against the government, gaining more privacy for everyone

Harvard Law Review, 4-10-2018, "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance,"

https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/

Consider, for example, Microsoft's 2016 lawsuit against the U.S. government. **Microsoft alleged that the government routinely attached secrecy orders to search warrants and other requests for information, often for an indefinite amount of time, even when the facts of a case did not support the need for secrecy**. As a result, Microsoft was compelled to turn over user information to the government but was not able to notify its users when it did so. **Microsoft claimed that the routine use of indefinite secrecy orders violated its customers' Fourth Amendment rights and Microsoft's own First Amendment rights**. 103. First Amended Complaint for Declaratory Judgment, supra note 101, at 2**. In October 2017, the Department of Justice issued new secrecy order guidelines for U.S. Attorneys' Offices. According to Brad Smith, Microsoft's President and Chief Legal Officer, the new policy "helps ensure that secrecy orders are used only when necessary and for defined periods of time." Microsoft then dropped its lawsuit**, but Smith assured its users that it would continue fighting for their privacy rights: We applaud the Department of Justice for taking these steps, but that doesn't mean we're done with our work to improve the use of secrecy orders. We have been advocating for our customers before the DOJ for a long time, and we'll continue to do that. We will continue to turn to the courts if needed. And we are committed to working with Congress.

**Response:** the affirmative doesn't solve for foreign collection of data

**Warrant:** businesses became unpopular due to foreign data collection not domestic

Tim Edgar, 9-5-2017, "Why Should Americans Care About Foreign Privacy?," Forbes, https://www.forbes.com/sites/ciocentral/2017/09/05/why-should-americans-care-about-foreign-privacy/?sh=7187d51f9b5a

In the rest of the world, Snowden is even more popular. **The internet gave American companies a reason to care about what foreigners in other countries thought about U.S. government spying. Snowden's decision to leak details about the NSA's surveillance programs had major implications for American business**. **Foreign competitors argued that U.S. companies could not be trusted to store personal data because they were in bed with the NSA**. **The constant talk by U.S. officials of protecting "U.S. persons" was not helping. I**nitial estimates of lost business from the "Snowden effect" ranged from $35 billion to $180 billion. The nervous giants of Silicon Valley demanded surveillance reforms that go beyond protecting the privacy of Americans. Obama responded with a directive requiring intelligence agencies have rules to protect the privacy of everyone whose data is collected in mass surveillance programs. **In 2015 the European Court of Justice struck down a vital agreement allowing business to transfer personal data to the United States, citing fears of U.S. government surveillance. By 2016, officials from the United States and the European Union had negotiated a new deal on personal data,** the US-EU Privacy Shield. The deal was based in part on assurances from U.S. intelligence officials they were serious about privacy. As evidence, they pointed to the new rules protecting the personal data of foreigners required by Obama's presidential directive. While EU officials went along, the deal is being challenged in European courts because U.S. law still permits very broad surveillance.

**Analysis:** the easiest way out of this argument is by pointing out that the revenue lost was by foreign business deals due to fears they would be surveilled. The pro does not end that. Strengthening this argument would be cards about the economic ramifications of terrorism to give you clear weighing and a lives first framework. The argument that the aff only applies to domestic surveillance may be read as an overview depending on the aff's structure.

## A/2: The NSA spies on activists and protestors

**Response:** NSA spying on activist groups and protestors is a means of preventing credible threats from launching attacks.

**Warrant:** The NSA is the de facto authority on cyber operations.

> Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks, 3 Apr. 2019, warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.
>
> The review process for a Cyber Command operation also requires an equities review by a multitude of government, intelligence, and military stakeholders. The idea is that all relevant parties have an opportunity to address potential concerns with a proposed offensive cyberspace operation. While one of the principal original concerns with the dual hat arrangement was the potential for unfair prioritization of Cyber Command support requests to the NSA, the equities review process has instead created the opposite problem. **Because Cyber Command depends so heavily on NSA logistical and operational support, it has essentially lent the agency de facto veto authority on offensive cyberspace operations: Cyber Command risks losing NSA-facilitated training, NSA-provided office space, and access to NSA's signals intelligence data by bickering with NSA over who get a shot at a given targets.** The responsibility of balancing the prioritization of the distinct missions of two different organizations should not be delegated to a single individual. Doing so inevitably privileges one mission at the other's expense, and ultimately impedes overall progress for both

**Impact:** Credible U.S. threats would deter adversaries from launching attacks.

Gale, David, et al. "Cybermad: Should the United States Adopt a Mutually Assured Destruction Policy for Cyberspace?" Air University, Apr. 2009.

The nuclear MAD doctrine is credited with preventing the Cold War from turning hot, since neither side could expect to survive a full scale nuclear exchange. Although the loss of cyberspace might not rise to this level, the doctrine still applies. **If the US can credibly vow to destroy cyberspace, thus destroying world economies, the US can deter an adversary from launching an attack.** Critics may correctly argue that CyberMAD's deterrent effect is limited, since it will not deter non-state actors. However, nuclear MAD doctrine never deterred non-state actors. Critics will also argue that the lack of attribution will limit CyberMAD. Although true, it allows us to focus on developing the capability. We should not throw out the doctrine. We should develop the capability.

**Impact:** A cyber attack would put critical infrastructure at risk.

LaFrance, Adrienne. "When Is Cyberwar Just War?" The Atlantic, 16 May 2017, www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/.

The devastating effects of a massive cyberattack are no more confined to a computer network than any other action carried out online. People use the computers and the internet all the time to make things happen in the physical world. **A cyberattack isn't just a cyberattack. It's an attack. Hospitals, pharmacies, and major corporations like FedEx and the Spanish telecommunications giant Telefonica were among the 200,000 victims hobbled by a global ransomware attack on Friday, which locked people's computers and demanded Bitcoin payment in exchange for access. In the United Kingdom, some hospitals canceled procedures and other appointments as a result.** The software security firm Symantec found that people paid ransoms totaling about $54,000 in the attack, though officials strongly caution against paying such ransoms.

**Analysis**: While activist groups may disagree, the choice to spy on political organizations ensures that the government can preemptively respond to credible threats. In order to handle these threats, the government first must be able to collect information which is only possible through the NSA.

## A/2: NSA spying is unpopular among Americans

**Response:** Government surveillance of Americans will happen regardless of whether the NSA is around. Spying may be unpopular, but the NSA is the least of our problems.

**Quantification:** In the status quo, the FBI only receives about 4 percent of the NSA's data collection.

Rangappa, Asha. "Don't Fall for the Hype: How the FBI's Use of Section 702 Surveillance Data Really Works." Just Security, 29 Nov. 2017, www.justsecurity.org/47428/dont-fall-hype-702-fbi-works/.

Some of these incidental communications may include parties who are U.S. persons (USPERs), which under FISA are defined as U.S. citizens or permanent legal residents. **Only a subset of the total communications collected under PRISM is passed on to the FBI. Specifically, the NSA passes on to the FBI information collected on selectors associated with "Full Investigations" opened by the FBI. Full Investigations are the most serious class of investigations within the Bureau, and require the most stringent predicate to open: There must be an "articulable factual basis" that a federal crime has occurred or is occurring or a threat to national security exists.** (Two other investigative classifications, Preliminary Investigations and Threat Assessments, have lower thresholds to open and shorter time limits to remain open.) In other words, the NSA provides the FBI with communications from selectors that are directly linked to the most serious crimes or threats to national security currently being investigated by the FBI. According to FBI Director Christopher Wray, **the FBI receives about 4.3 percent of the NSA's total collection** – and since not every incidental communication will necessarily involve an USPER, the number of communications involving Americans are likely less than that.

**Warrant:** Obama proposed letting the FBI hold the data instead of the NSA.

Toor, Amar. “Obama Assessing Four Alternatives to NSA Phone Data Collection: WSJ.” The Verge, 26 Feb. 2014, www.theverge.com/2014/2/26/5448814/obama-assessing-four-alternatives-to-nsa-phone-data-collection-wsj.

One proposal would be to put phone metadata collection under the purview of US telecommunications companies. Under this option, the NSA would inform the companies of when it needs to search their databases for terrorism-related investigations, and the phone companies would return only the results of those searches, rather than data on consumers unrelated to the investigations. **A second proposal would see a different federal agency hold the data — the Federal Bureau of Investigation (FBI), for instance** — and a third would place them under the control of a third entity that's neither a federal agency nor a telecom company. The final proposal would abolish the data collection program altogether, an option that Obama in January said would require more work "to determine exactly how this system might work."

**Warrant:** The FBI can search for information without pre-existing suspicion.

Granick, Jennifer. “Reining In Warrantless Wiretapping of Americans.” The Century Foundation, 16 Mar. 2017, tcf.org/content/report/reining-warrantless-wiretapping-americans/?agreed=1.

Once intelligence agents collect private messages under section 702, domestic law enforcement agencies are authorized to use the sensitive data in a range of worrisome ways. **The Federal Bureau of Investigation (FBI) may search the information to learn whether Americans are committing run-of-the-mill crimes without any pre-existing suspicion.** Normally, conversations people have with their attorneys are treated as privileged information: no one can compel a lawyer to testify against his or her client.

**Impact:** Surveillance tools could be used against Americans.

> The American Civil Liberties Union. "More About FBI Spying." American Civil Liberties Union, www.aclu.org/other/more-about-fbi-spying.
>
> The FBI has a long history of abusing its national security surveillance powers. **The potential for abuse is once again great, particularly given that the lines between criminal investigations and foreign intelligence operations have been blurred or erased since 9/11. As a result, intrusive surveillance tools originally developed to target Soviet spies are increasingly being used against Americans.** During the Cold War, the FBI ran a domestic intelligence/counterintelligence program called COINTELPRO that quickly evolved from a legitimate effort to protect the national security from hostile foreign threats into an effort to suppress domestic political dissent through an array of illegal activities.

**Analysis**: The NSA is likely responsible for violations of privacy, and it has justifiably drawn the ire of Americans for that very reason. However, the NSA is not the root cause of the problem – the U.S surveils its citizens regardless, meaning that the public should likely prefer the NSA to more invasive alternatives.

## A/2: The NSA is subject to leaks

**Response:** Reforms to the NSA should resolve issues with leaks. If anything, leaks have pressured the NSA to change its ways.

**Uniqueness:** The NSA suspended their controversial phone surveillance program.

Lardieri, Alexa. "NSA Suspends Controversial Phone Surveillance Program." US News, 5 Mar. 2019, www.usnews.com/news/politics/articles/2019-03-05/nsa-suspends-controversial-phone-surveillance-program.

**THE NATIONAL SECURITY Agency has shut down the controversial program that tracks Americans' domestic calls and texts.** Luke Murry, national security adviser to House Minority Leader Kevin McCarthy, said during a Lawfare podcast that the NSA has not used the system in six months. The program is set to expire at the end of the year, and the Trump administration is unlikely to request an extension from Congress.

**Warrant:** Snowden forced the NSA to reform.

Edgar, Timothy. "Why the NSA Should Thank Edward Snowden." Fortune, 3 Oct. 2017, fortune.com/2017/10/03/edward-snowden-nsa-fisa-section-702/.

From 2006 to 2013, I worked inside the surveillance state as a privacy official, first in the Office of the Director of National Intelligence and later at the White House under President Barack Obama. While I helped put the NSA's programs on firmer legal ground and made some improvements in oversight, broader changes to protect privacy were elusive. **Obama's aides showed little interest in reforming mass surveillance until after I left, when the Snowden leaks forced their hands. It was Snowden who forced the NSA to be more transparent, accountable, and protective of privacy. The NSA took**

**painful steps to open up.** It released thousands of pages of previously top-secret documents in a transparency drive intended to put the Snowden leaks in context. The head of the intelligence community now publishes an annual transparency report. Congress ended bulk collection of Americans' telephone records after an outside review found it to be of marginal value.

**Warrant:** Senators proposed a bill to drastically reform the NSA.

Coble, Sarah. "US Rolls Out New Bill to Reform NSA Surveillance." Infosecurity Magazine, 27 Jan. 2020, www.infosecurity-magazine.com/news/us-rolls-out-new-bill-to-reform/.

**US senators have proposed a bill that would drastically reform the surveillance practices of the National Security Agency (NSA) and increase oversight of government surveillance.** Titled The Safeguarding Americans' Private Records Act, the bill was introduced on Thursday by Senators Ron Wyden, Zoe Lofgren, Pramila Jayapal, Warren Davidson, and Steve Daines. According to a statement on Wyden's website, the changes proposed in the bill will "protect Americans' rights against unnecessary government surveillance." **The bill comes ahead of the March 15 expiration of Section 215 of the Patriot Act,** which the National Security Agency "used to create a secret mass surveillance program that swept up millions of Americans' phone calls." The phone record program was terminated last year.

**Analysis**: The NSA has had several high-profile leaks in the past, but these leaks have forced the organization to clamp down on their data security. As a result, while the NSA may be known for leaking data, impending reforms are likely to make that data more secure than ever.

## A/2: The NSA antagonizes China and Chinese Americans

**Response:** The NSA's surveillance of China and Chinese Americans could prevent a major cyberattack.

**Evidence**: NSA surveillance has revealed Chinese targeting of military and defense contractors.

Volz, Dustin. "U.S. spy agency warns that Chinese hackers target military, defense industry." Wall Street Journal. 10/20/20. https://www.wsj.com/articles/u-s-spy-agency-warns-beijing-s-hackers-aiming-at-u-s-defense-industry-military-11603206459

The National Security Agency on Tuesday warned that Chinese government hackers were taking aim at U.S. computer networks involved in national defense, characterizing the threat posed by Beijing as a critical priority in need of urgent attention. The vulnerabilities described in the NSA's new alert were already known to cybersecurity professionals, but the nation's premier electronic spy agency for the first time described them as targets of Chinese state-sponsored hacking campaigns. The NSA urged cyber defenders across the Defense Department and within the defense industrial base to take action to guard against Chinese intrusion.

"These networks often undergo a full array of tactics and techniques used by Chinese state-sponsored cyber actors to exploit computer networks of interest that hold sensitive intellectual property, economic, political, and military information," the alert warned.

**Warrant:** Credible U.S. threats would deter adversaries from launching attacks.

Gale, David, et al. "Cybermad: Should the United States Adopt a Mutually Assured Destruction Policy for Cyberspace?" Air University, Apr. 2009.

The nuclear MAD doctrine is credited with preventing the Cold War from turning hot, since neither side could expect to survive a full scale nuclear exchange. Although the loss of cyberspace might not rise to this level, the doctrine still applies. **If the US can credibly vow to destroy cyberspace, thus destroying world economies, the US can deter an adversary from launching an attack.** Critics may correctly argue that CyberMAD's deterrent effect is limited, since it will not deter non-state actors. However, nuclear MAD doctrine never deterred non-state actors. Critics will also argue that the lack of attribution will limit CyberMAD. Although true, it allows us to focus on developing the capability. We should not throw out the doctrine. We should develop the capability.

**Impact:** A cyber attack would put critical infrastructure at risk.

LaFrance, Adrienne. "When Is Cyberwar Just War?" The Atlantic, 16 May 2017, www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/.

The devastating effects of a massive cyberattack are no more confined to a computer network than any other action carried out online. People use the computers and the internet all the time to make things happen in the physical world. **A cyberattack isn't just a cyberattack. It's an attack. Hospitals, pharmacies, and major corporations like FedEx and the Spanish telecommunications giant Telefonica were among the 200,000 victims hobbled by a global ransomware attack on Friday, which locked people's computers and demanded Bitcoin payment in exchange for access. In the United Kingdom, some hospitals canceled procedures and other appointments as a result.** The software security firm Symantec found that people paid ransoms totaling about $54,000 in the attack, though officials strongly caution against paying such ransoms.

**Analysis**: Spying on China and Chinese Americans will not always yield fruitful results, but in some cases surveillance has been effective. Chinese Americans are obviously no more dangerous than any other Americans, but given the risk of a major cyberattack, it makes sense to check in on potential threats.

## A/2: NSA surveillance is an invasion of privacy

**Response:** Alternatives to NSA surveillance are more invasive. Were the private sector to become involved, even more restriction of privacy would occur.

**Uniqueness:** The NSA has more oversight and regulation than private companies.

McLaughlin, John. "NSA Intelligence-Gathering Programs Keep Us Safe." Washington Post, 2 Jan. 2014, www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html.

> Regarding outrage over the NSA's collection of telephone calling records, or metadata, **I don't know why anyone would have greater confidence in this information being held by private companies.** And given the perceived threat to privacy, it's astonishing how little attention has been paid to the Senate commerce committee's recent report on companies that gather personal information on hundreds of millions of Americans and sell it to marketers, often highlighting people with financial vulnerability. Some companies group the data into categories including "rural and barely making it," "retiring on empty" and "credit crunched: city families." The aim is often to sell financially risky products to transient consumers with low incomes, the report found. **That's a real scandal — and a universe away from the NSA's ethical standards and congressional oversight.** The NSA, of course, is not perfect. But it is less a victim of its actions — the independent commission appointed by President Obama found no illegality or abuses — than of the broad distrust of government that has taken root in the United States in recent decades. Studies by Pew and others show distrust of government around 80 percent, an all-time high.

**Warrant:** Tech companies act as "surveillance intermediaries."

Margaret Jane Radin. "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance." Harvardlawreview.org, 10 Apr. 2018, harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

In just six months, law enforcement agencies turned to technology companies to gather evidence for thousands of investigations. Of the many conclusions that one might draw from these numbers, at least one thing is clear: technology companies have become major actors in the world of law enforcement and national security. **In his recent article, Professor Alan Rozenshtein dubs these technology companies "surveillance intermediaries" — entities that sit between law enforcement agencies and the public's personal information, and that have the power to decide just how easy or difficult it will be for law enforcement to access that information. Surveillance intermediaries hold extraordinary power when they decide how to respond to government requests for information — power that may or may not be to the public's benefit.** While intermediaries must comply with statutory and constitutional law governing law enforcement requests for information, Rozenshtein explains that they still hold a large degree of discretion when processing those requests: discretion in how critically they evaluate the legality of requests, in slowing down the process by insisting on proceduralism, and in minimizing their capacity to respond to legal requests by implementing encryption.

**Analysis**: Big tech has been cozying up to Washington in an attempt to secure major government contracts. Were the NSA to be shut down, optimists may claim that to be a victory, but in reality that would just push the burden of surveillance to the private sector where there is even less regulation than at the NSA.