# January Topic Analysis

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

## Definitions:

**Should**: Merriam-Webster clarifies that should is used to express obligation, propriety, or expediency. Essentially, the use of the term "should" in the resolution poses the question of whether or not it is morally correct for the National Security Agency to end its surveillance practices or whether it is proper to do so.

**National Security Agency (NSA)**: The National Security Agency, or NSA, is an agency within the US Department of Defense that is responsible for cryptographic (codebreaking) and communications intelligence and security activities, according to Britannica. As part of the intelligence community, the NSA gathers intel in the name of America's safety.

**End**: While I'm sure the term 'end' doesn't require a formal definition, it's important to note that ending surveillance is not the same as reducing surveillance. Thus, pro teams must argue for the complete elimination of the NSA's surveillance activities, where con teams could argue for a reduction.

## Background:

The NSA was established in 1952 by a presidential directive from Harry S. Truman with the goal of providing for a unified and integrated organization for communications intelligence activities of the US conducted against foreign governments[1]. In 1978, the Foreign Intelligence Surveillance Act (FISA) was passed, allowing law enforcement and intelligence agencies to track communications and make searches of people and foreign powers engaging in spying or planning acts of terrorism[2]. This Act restricted NSA operations by forbidding such searches against US citizens, permanent residents, corporations, or associations. Section 702 of FISA, added in the late 2000s, allows surveillance without a court order or warrant for non-US people certified as targets, granting the NSA the ability to monitor domestic communications without a warrant as long as one party is believed to be located outside of the US.

The NSA's activities were given national attention in 2013 after a former computer security contractor, Edward Snowden, leaked classified information about two surveillance programs in the NSA - PRISM and cellular tracking. PRISM is a tool used to collect private electronic data belonging to users of major internet websites and services such as Facebook, Google, Microsoft Outlook, and more[3]. It essentially allows the NSA to request data on specific people from major technology companies, and both the companies involved and the government insist this can only happen with approval from the Foreign Intelligence Surveillance Court and can only be used for specific targets. The NSA also collects information regarding telecommunications, including the metadata of most calls made in the US - that is, the phone numbers and length of calls but not the content[4]. On top of this, the NSA can see "nearly everything a user does on the internet," according to a 2013 ProPublica report. Though the NSA is only authorized to intercept internet communications with at least one party outside of the US, there is no fully reliable automatic way to separate domestic from international communications, so the program captures some domestic activity as well.

This topic becomes a little tricky when examining the breakdown of the programs. There are legal limitations on what kinds of data the NSA can collect on US citizens and permanent residents, though these legalities can be murky or confusing. The agency continues to collect a great deal of data on US citizens, particularly through their collection of the metadata of phone

---

[1] Encyclopedia Britannica. "National Security Agency | History, Role, & Surveillance Programs." Encyclopedia Britannica. Last accessed 13 Dec 2020. https://www.britannica.com/topic/National-Security-Agency

[2] Lachman, Andrew. "The NSA Revelations and FISA: What It Is — and Isn't." Trumancenter.org. 8 Oct. 2020. http://trumancenter.org/doctrine-blog/the-nsa-revelations-and-fisa-what-it-is-and-isnt/

[3] Sottek, T.C. "Everything you need to know about PRISM." The Verge. 17 Jul. 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

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

calls and their operations through PRISM. Teams will need to define what “ending surveillance” really means in each round of debate, what actions the NSA will need to take in order to end this surveillance, and whether the benefits of taking such actions outweigh the costs.

# Aff Arguments:

## Invasion of Privacy

The first argument that likely comes to mind on the pro side is an invasion of privacy. As discussed, the NSA has argued that their primary goal is to collect intelligence on those located outside of the US who are suspected of harmful or terrorist activity against the US. However, the ACLU argues that when government officials advocated for the FISA Amendments Act, they made it clear that the "one-end-domestic" communications, or communications in which one party is located in the US, are the kinds of communications they most want to gain information on[5]. Under the FISA Amendments Act, the NSA has the ability to collect international communications, retain them, and potentially even share them with other US government agencies or foreign governments.

Other organizations and judges have noted that the FISA court needed for approval of domestic surveillance measures rarely denies access to the NSA and that many procedures have been modified and adapted in recent years, creating further confusion over legalities.[6] The problem in this area is that even when restrictions on the NSA's activities exist, they often find ways to circumvent them. An internal audit revealed that the NSA has broken privacy rules or overstepped its legal authority thousands of times every year since Congress expanded its powers in 2008.[7] This was a major part of Edward Snowden's leak - the documents he shared revealed the extent of the NSA's ignorance of the legal limitations placed on them. This negligence from the NSA is why a majority of Americans oppose the government collecting bulk data on its citizens, and two-thirds believe there are not adequate limits on what types of data can be collected.[8]

---

[5] ACLU. "Documents Confirm How the NSA's Surveillance Procedures Threaten." American Civil Liberties Union. Last accessed 14 Dec. 2020. https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy

[6] Nakashima, Ellen. "FBI and NSA violated surveillance law or privacy rules, a federal judge found." Washington Post. 4 Sept. 2020. https://www.washingtonpost.com/national-security/fbi-and-nsa-violated-surveillance-law-or-privacy-rules-a-federal-judge-found/2020/09/04/b215cf88-eec3-11ea-b4bc-3a2098fc73d4_story.html

[7] Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds." Washington Post. 15 Aug. 2013. https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

[8] Gao, George. "What Americans think about NSA surveillance, national security and privacy." Pew Research Center. 29 May 2015. https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

## Surveillance Hurts US Econ

This argument can be split into two major areas: the cost of surveillance programs for the government and the impact of these programs on businesses. First, surveillance operations are far from cheap. A newly declassified study reveals that an NSA system that analyzed logs of domestic phone calls and text messages from 2015 to 2019 cost $100 million to conduct.[9] What's worse, the program generated only one significant investigation and two unique leads that the FBI did not already possess. Again, this program was specific to domestic texts and phone calls, so this is a great example to use under the resolution.

The other crucial economic aspect to consider is the potential for NSA operations to harm US businesses. As more and more information is revealed about the NSA's surveillance operations, other countries - particularly China - have reported distrust in US businesses. Major US technology companies, including Microsoft and IBM, have reported declines in business operations in China since the NSA's surveillance program was exposed.[10] Cisco has reported a 19% loss of revenue in China due to claims that the NSA was installing backdoors and implants on its routers[11]. Reports have estimated that distrust in US operations because of the NSA will cost US businesses anywhere from $22 billion to $180 billion.

## No Reason to Continue

The idea that there's simply no reason to continue with these operations may seem like a lazy argument, but it's a true argument, and it could constitute a good case argument or a good block. The main idea is that the NSA's surveillance programs don't actually produce any national security benefits. Plenty of reviews have found that NSA surveillance generates little to no useful leads. A 2013 analysis from the President's Review Group on Intelligence and Communications technologies determined that the NSA's bulk collection of phone records "was not essential to preventing attacks" and that government claims about the success of surveillance programs since 9/11 are overblown and misleading.[12] Combined with the cards on cost, it's clear that there is no reason to continue funding NSA operations.

---

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

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

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

[12] Kirchner, Lauren. "What's the Evidence Mass Surveillance Works? Not Much." ProPublica. 18 Nov. 2015. https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much?token=--sanitized--

The other important aspect of this argument is the fact that the NSA itself doesn't see a reason to continue surveillance operations. Last year, the NSA recommended that the a surveillance program that collects information about domestic phone calls and text messages be dropped by the White House.[13] When making this recommendation, they claimed that the logistical and legal burdens of keeping it outweigh its intelligence benefits.[14] Here, the NSA does the weighing for you. They've conducted a cost-benefit analysis and have come to the conclusion that with this specific program, it's simply not worth keeping. Additionally, it doesn't seem like the programs will become any more useful in the future. Scholars who have studied the NSA's Section 215 CDR program have concluded that the program has been ineffective since its inception in 2015 and is unlikely to be effective in the future.[15]

## Disproportionately Affects Minorities

As with many topics we debate, there is an argument to be made about the impact of NSA surveillance on minority populations across the United States. Intelligence gathering operations are conducted primarily online, and mass surveillance is much easier to conduct on minority populations.[16] Those in "targeted communities" are often victims of surveillance simply because of their race, ethnicity, or religion because of "predictive policing," a practice that uses advanced data to predict crime or terrorism.[17] Even with the insistence that the NSA only surveils terrorist agents, foreign spies, or those aiding high crimes, high-profile Muslim Americans have been the targets of NSA surveillance efforts.[18] Activists and analysts argue that mass shootings are a much greater threat to the US than Muslim extremists, as those happen domestically and at a much more frequent rate. Members of lower-income minority

[13] Eddington, Patrick. "The Snowden Effect, Six Years On." Just Security. 6 Jun. 2019. https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

[14] Volz, Dustin and Strobel, Warren P. "NSA Recommends Dropping Phone-Surveillance Program." Wall Street Journal. 24 Apr., 2019. https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247

[15] Bradford Franklin, Sharon. "Congress Needs to Throw This Surveillance Program Away." Slate. 27 Jan. 2020. https://slate.com/technology/2020/01/usa-freedom-act-renewal-section-215-cdr.html

[16] Dennis, Andrea. "Mass Surveillance and Black Legal History," American Constitution Society. https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/

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

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

populations are also frequently over-policed due to crime statistics and methods such as predictive policing, and are also unable to find ways to avoid this level of surveillance.[19]

[19] Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds." Washington Post. 15 Aug. 2013. https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

# Neg Arguments:

## NSA Surveillance Prevents Terrorist Attacks

The major reason for the NSA to continue their operations is to prevent attacks against the US - primarily terrorist attacks. Most Americans agree that the NSA's program tracking phone records is an acceptable way for the government to investigate terrorist plots against the country.[20] The struggle with this is that it's difficult to provide concrete statistics on how useful the programs have been - there isn't really a clear-cut way of understanding how many potential attacks have been deterred based on what could have escalated into an attack or what plans could have emerged before they were stopped. The NSA provides one number, though, reporting to Congress that more than 50 terrorist attacks were prevented by their two main surveillance operations.[21]

A key part of thwarting terrorist attacks is the ability to prevent domestic terrorism. Using intelligence collection capabilities on white supremacist groups could help put a stop to these types of attacks before they occur.[22] This is something that countries across the globe have been working diligently on, and the US seems to be lagging behind. Putting a stop to these attacks would be significant, as the FBI has made about 100 domestic terrorism-related arrests from October 2018 to August 2019, with the majority of these being tied to white supremacy. Many assert that if the NSA's surveillance programs had been as expansive in 2001 as they are today, they could have prevented the 9/11 attacks.[23]

## Surveillance Deters Cyber Attacks

On top of terrorist attacks, the NSA's intelligence is intended to prevent cyber attacks from foreign nations. In order to keep computer and telecommunication networks secure, the

[20] Pew Survey. "Majority Views NSA Phone Tracking as Acceptable Anti-Terror Tactic." The Pew Research Center. 10 Jun. 2013. https://www.pewresearch.org/politics/2013/06/10/majority-views-nsa-phonetracking-as-acceptable-anti-terror-tactic/

[21] Parkinson, John. "NSA: 'Over 50' Terror Plots Foiled by Data Dragnets," ABC News. 18 Jun 2013. https://abcnews.go.com/Politics/nsadirector-50-potential-terrorist-attacks-thwartedcontroversial/story?id=19428148

[22] Levinson, Robert. "The Fight in the Right: It is Time to Tackle White Supremacity Terrorism Globally." War on the Rocks. 22 Aug. 2019. https://warontherocks.com/2019/08/the-fight-in-the-right-it-is-time-to-tackle-white-supremacist-terrorism-globally/

[23] Morrell, Michael. "Correcting the Record on NSA Recommendations." The Washington Post. 27 Dec. 2013. 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

government must monitor and gather intelligence on certain networks.[24] The NSA is the primary collector of this data in the status quo, and doing away with NSA surveillance measures would mean losing training opportunities, office space, and access to prior data.[25] Now is a crucial time for the US to ensure they have great cyber attack intelligence and surveillance, as more than 30 countries are currently bolstering their cyber attack capabilities to bypass traditional defense measures.[26] Cyber attackers and hackers are also increasingly targeting more severe areas - the FBI has reported that hackers have been targeting nuclear facilities to attempt to cause events like Chernobyl, which resulted in 50 deaths and has left the region uninhabitable.[27]

## Preventing the Spread of COVID-19

This topic has the potential to be immensely relevant if teams want to discuss the impact of NSA surveillance on preventing the spread of COVID-19. Plenty of countries around the world have employed track-and-trace services to help limit the number of people being infected, including the UK, South Korea, Israel, and Russia, among many others.[28] The foundation for surveillance activities in the time of COVID exists, and the NSA has a great opportunity to help contribute to this cause and rebuild some credibility. In fact, the US and Europe are already moving towards using cellphone surveillance to track residents infected with COVID,[29] and the NSA has the capabilities to help with this. Surveillance strategies have proven to be overwhelmingly successful in South Korea, where fatalities are a third of the global average.[30] Obviously, preventing COVID has the potential for huge scope and magnitude weighing, but it would also work very well to outweigh on timeframe. If the con team can make the case that now is not the time to end surveillance programs, there could be a really interesting case for keeping surveillance for a little longer.

---

[24] Goldsmith, Jack. "We Need an Invasive NSA." The New Republic. 10 Oct. 2013. www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks

[25] Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks. 3 Apr. 2019. www.warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/

[26] Ranger, Steve. "US Intelligence: 30 countries building cyber attack capabilities." ZD Net. 5 Jan. 2017. https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/

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

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

[29] Deese, Kaelan. "US, Europe Turning to Cell Phone Tracking Data to Slow Coronavirus Spread." TheHill, 3 Apr. 2020. thehill.com/policy/technology/technology/490991-us-europe-cellphone-data-halt-coronavirus

[30] 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/

## Reform is Preferable

This argument is a good way to agree with some of the pro claims that the NSA programs may not be the most useful, or even that the NSA wants to end certain surveillance activities. With this, you can claim that NSA surveillance strategies simply need rethinking rather than scrapping. The Snowden leaks forced the NSA to take a look inward and become more transparent and accountable in their actions.[31] There are already status quo measures to reform the ways that the NSA collects intelligence - just this year, senators proposed a bill to drastically change the surveillance practices of the NSA and increase governmental oversight of these functions.[32] Surveillance can offer a lot of benefits to a country, including being the only way to connect links between foreign terror threats and potential attacks on the US.[33] Arguing for reform allows you to advocate for these benefits while also accepting flaws with the current system.

## NSA is Better than FBI

The basic premise of this argument is the idea that if the NSA ends its surveillance of US citizens and permanent residents, those surveillance responsibilities will likely fall on other government agencies - primarily the FBI - as previously proposed.[34] Since the FBI is technically a law enforcement agency, there is potential for abuse of intelligence gathered through their systems. The FBI even has a track record - just last year, the Foreign Intelligence Surveillance Court found that the FBI potentially violated the rights of millions of Americans by improperly searching intelligence gathered by the NSA.[35] This is bad enough on its own, but becomes even more shocking when contextualized. In the status quo, only around 4% of the NSA's total data is available to the FBI.[36] On top of the abuse seen with FBI practices, it's also worth noting that the FBI is able to search for information on US citizens and permanent residents without pre-existing suspicion,[37] setting them apart from the NSA.

---

[31] Edgar, Timothy. "Why the NSA Should Thank Edward Snowden." Fortune. 3 Oct. 2017. www.fortune.com/2017/10/03/edward-snowden-nsa-fisa-section-702/

[32] 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/

[33] AP News. "NSA: Bulk Collection Surveillance Keeps Us Safe." CBS News, 11 Oct. 2013. www.cbsnews.com/news/nsa-bulk-collection-surveillance-keeps-us-safe/

[34] 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

[35] Aaronson, Trevor. "A Declassified Court Ruling Shows How the FBI Abused NSA Mass Surveillance Data." The Intercept. 10 Oct. 2019. www.theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/

[36] 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/

[37] Granick, Jennifer. "Reining In Warrantless Wiretapping of Americans." The Century Foundation. 16 Mar. 2017. www.tcf.org/content/report/reining-warrantless-wiretapping-americans/?agreed=1