OPP Brief: PATRIOT Act  
by Mark Csoros



This year, some debaters are running applications centered around the NSA’s surveillance programs. This is usually run as an affirmative application, though there is room for the application on both sides of the resolution (negative can certainly argue that it’s an unjust invasion of privacy). However, the current state of the Patriot Act and the NSA’s bulk collection of metadata is more complex than most affirmatives insinuate. Before we get into the application and responses, it’s important that we take a quick look at the current state of mass surveillance.

The Patriot Act (its full title is the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”, giving it the acronym USA PATRIOT), was passed following 9/11 with overwhelming bipartisan support[[1]](#footnote-1). It made a lot of sense, because it allowed us to fight terrorism the same way that we were already fighting organized crime. However, there was one major difference.

Back in 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which was designed to help the government collect intelligence on foreign actors who posed a threat to national security[[2]](#footnote-2). FISA created something called the Foreign Intelligence Surveillance Court (properly abbreviated FISC but is usually called the FISA Court). The Department of Homeland Security explains FISA and the FISA Court thusly:

*Subchapter I of FISA established procedures for the conduct of foreign intelligence surveillance and created the Foreign Intelligence Surveillance Court (FISC). The Department of Justice must apply to the FISC to obtain a warrant authorizing electronic surveillance of foreign agents. For targets that are U.S. persons (U.S. citizens, permanent resident aliens, and U.S. corporations), FISA requires heightened requirements in some instances.*

*Unlike domestic criminal surveillance warrants issued under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "*[*Wiretap Act*](http://it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop)*") , agents need to demonstrate probable cause to believe that the "target of the surveillance is a foreign power or agent of a foreign power," that "a significant purpose" of the surveillance is to obtain "foreign intelligence information," and that appropriate "minimization procedures" are in place.*[*50 U.S.C. § 1804*](http://www.law.cornell.edu/uscode/usc_sec_50_00001804----000-.html)*.*

*Agents do not need to demonstrate that commission of a crime is imminent.*

*For purposes of FISA, agents of foreign powers include agents of foreign political organizations and groups engaged in international terrorism, as well as agents of foreign nations.*[*50 U.S.C. § 1801*](http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001801----000-.html)

*Record Destruction: Where the government has accidentally intercepted communications that "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States," the government is required to destroy those records, "unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person."*[*50 U.S.C. § 1806*](http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001806----000-.html)*.[[3]](#footnote-3)*

This is important because Section 215 of the Patriot Act gave the FISA Court the responsibility to approve or deny warrants for wiretaps, taking business records, and collecting telephone and internet metadata (metadata means data about data - who you called, when you called them, but not the actual conversation)[[4]](#footnote-4). The FISA Court is what’s called an *ex parte* court, which means that the government is the only party present, and location of the tightly sealed courtroom is a secret. No one knows which judges sit on the FISA court, because their names are protected, and they are appointed, without a confirmation process, by the Chief Justice of the Supreme Court.[[5]](#footnote-5) The FISA Court also isn’t that picky about which warrants they approve. For example, a 2016 report to Congress by the DOJ found that in 2015, the FISA Court approved 1,456 requests to obtain electronic evidence, out of the 1,467 requests the government made[[6]](#footnote-6). That one request that wasn’t approved was withdrawn by the government, meaning that the FISA court denied exactly zero warrants. The FISA Court did, however, modify 5 requests to obtain physical business records, out of the 142 requests the government made that year, but the Court’s 2015 denial percentage was still a whopping zero percent.

The FISA Court’s secrecy, along with their extreme willingness to approve surveillance, raised some concerns. When Edward Snowden revealed the extent of the NSA’s collection practices (through the PRISM program and other mass collection programs), privacy advocates were understandably worried. In 2015, Congress passed the USA Freedom Act, which assuaged some privacy concerns by limiting the scope of bulk surveillance. The Washington Post reported:

*“The bill bans the bulk collection of data of Americans’ telephone records and Internet metadata. It limits the government’s data collection to the “greatest extent reasonably practical”—which means the government can’t collect all data pertaining to a particular service provider or broad geographic region, such as a city or area code.”*

*“Instead of bulk data collection, the bill authorizes the government to collect from phone companies up to “two hops” of call records related to a suspect, if the government can prove it has “reasonable” suspicion that the suspect is linked to a terrorist organization.”*

*“It extends the expiration of three Patriot Act provisions—Section 215, roving wiretaps and the lone wolf surveillance authority—to December 2019.”[[7]](#footnote-7)*

So, in a mere 9 months we may no longer have an NSA capable of collecting bulk data. This may seem frightening, especially since there is some evidence that terror attacks have been foiled because of bulk collection.[[8]](#footnote-8) However, recent evidence has suggested that the NSA has quietly ended its bulk collection of phone data, the Trump administration hasn’t used the program for the past six months, and may choose not to pursue renewal in December.[[9]](#footnote-9) In addition, the NSA recently deleted (or claimed to delete) millions of call and text records, dating back to 2015, that they had collected due to a coding error. Even the NSA can be sensitive to privacy, at least when public outcry requires it to be.

I know that was a lot of background, but it’s barely scratched the surface of the tangled web that is America’s mass surveillance system. There’s a lot more to know, and I hope you decide to delve deeper into this issue, because it’s important for you as a debater and as a citizen. But, before this brief gets too long, let’s look at some responses.

The best response on negative is that bulk surveillance isn’t an invasion of privacy at all, and so doesn’t represent an instance of conflict in the resolution. Remember privacy is made up of two things: subjective expectation (do I think that I have a right to my privacy in this situation), and objective societal views (where does society say that I have a reasonable expectation of privacy). Since the law and the courts say that it’s acceptable to conduct bulk data collection through FISA Court warrants, it doesn’t violate privacy for the NSA to do so.

A good way of supporting this argument is to bring up the Third-Party Doctrine. In a nutshell, this doctrine says that if you’ve willingly shared information with someone outside the direct line of communication (like your phone service provider), it’s no longer secrets, and the government can make use of that information. This doctrine has its roots in two Supreme Court Cases, Smith v. Maryland, and its predecessor, U.S. v. Miller. This article in The Atlantic[[10]](#footnote-10) gives a good and succinct summary of the doctrine, and I highly recommend it. Though there are legitimate arguments about the Third-Party Doctrine, it relies on a simple logic: if you share information, it’s not really secret. If you come up with a brand-new, super-secret, absolutely smashing argument, you can’t expect it to stay secret after you run it in a round. At that point, your argument is out in the public domain, and any expectation of privacy you have regarding that argument is probably unreasonable.

Another counter on negative is to turn the application back on the affirmative debater. Since the Patriot Act is established law, and doesn’t violate anyone’s reasonable expectation of privacy, what does it do? It reflects our commitment to protecting privacy as we search for truth. The NSA must get a warrant, albeit from a secret court that doesn’t refuse many requests. They delete information they obtained illegally. And they collect information that’s already been shared with a third party. If they can do all this truth seeking and foil terrorist plots without invading our privacy, why shouldn’t the judge vote negative?

1. U.S. Department of Justice “The USA PATRIOT Act: Preserving Life and Liberty” https://www.justice.gov/archive/ll/highlights.htm [↑](#footnote-ref-1)
2. U.S. Department of Justice “The Foreign Intelligence Surveillance Act of 1978 ([FISA](http://www.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36_20_I.html))” https://it.ojp.gov/privacyliberty/authorities/statutes/1286 [↑](#footnote-ref-2)
3. Department of Homeland Security Office for Civil Rights and Accountability “The Foreign Intelligence Surveillance Act of 1978 ([FISA](http://www.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36_20_I.html))” <https://it.ojp.gov/privacyliberty/authorities/statutes/1286> [↑](#footnote-ref-3)
4. Brennan Center for Justice “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance” Programs https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf [↑](#footnote-ref-4)
5. CNN, March 8th 2017 “What is the FISA court, and why is it so secretive?” https://www.cnn.com/2017/03/08/politics/fisa-court-explainer-trnd/index.html [↑](#footnote-ref-5)
6. U.S. Department of Justice, April 28 2016 *https://www.justice.gov/nsd/nsd-foia-library/2015fisa/download* [↑](#footnote-ref-6)
7. The Washington Post, June 2nd 2015 “USA Freedom Act: What’s in, what’s out” [*https://www.washingtonpost.com/graphics/politics/usa-freedom-act/*](https://www.washingtonpost.com/graphics/politics/usa-freedom-act/) [↑](#footnote-ref-7)
8. NY Times, June 18 2013 “*N.S.A. Chief Says Surveillance Has Stopped Dozens of Plots”*

   *https://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html* [↑](#footnote-ref-8)
9. NY Times, March 4th 2019 “Disputed N.S.A. Phone Program Is Shut Down, Aide Says” *https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html* [↑](#footnote-ref-9)
10. The Atlantic, December 2013 “What You Need to Know about the Third-Party Doctrine” *https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/* [↑](#footnote-ref-10)