Overview of Section 215 of the USA PATRIOT Act/USA FREEDOM Act

July 9, 2019

This report is the first in a series that will be released throughout 2019.

Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) in response to revelations of grave abuses by the executive branch, including the unlawful domestic surveillance of cultural and political leaders and U.S. intelligence-agency interference in domestic politics. FISA broadly prohibited this kind of domestic surveillance. However, it granted the government the authority to spy on Americans who are suspected of knowingly engaging in clandestine activities under a lower evidentiary standard than is required in criminal contexts.

Two decades later, in response to public outcry about the government’s failure to prevent the September 11th terrorist attacks, Congress weakened the limited protections established by FISA by enacting the USA PATRIOT Act. Contrary to the government’s political messaging around the PATRIOT Act, the failure to prevent the attacks was a function of poor intelligence sharing, not insufficient government authority to gather information, as the 9/11 Commission Report would later conclude. Congress subsequently amended both laws, generally by providing the government with new ways to secretly collect information without showing probable cause, as it is required to do when obtaining a warrant. Despite the secrecy that shrouds these collection tools — and the greater ease of collection enabled by post-September 11th legislation — public records show that the executive branch has been in nearly constant violation of FISA since September 11th, and during this time, it has warrantlessly collected information on virtually every American.

Section 215 of the PATRIOT Act amended a provision of FISA\(^1\) in order to grant the government broad authority to collect vast swaths of records held by businesses — including in the absence of any allegation of wrongdoing. These records reveal personal details about people’s lives, like whom they call, when, and for how long. The records can also include, among other digital and physical things, people’s purchase records, which reveal what people buy, when, and where. To obtain that information, the government makes an application to the Foreign Intelligence Surveillance Court (FISC) for an order to produce those records,\(^2\) which the FISC must issue if Section 215’s low standards are met. This order will compel a business to produce volumes of records for the government — sometimes numbering in the millions — while also barring the company from disclosing that they received the order or any other information about it.

The general public, including the authors of the PATRIOT Act, never anticipated the government’s unbounded application of Section 215. For example, when Congress first debated the PATRIOT Act in 2001, critics

\(^{1}\) 50 USC § 1861.

\(^{2}\) These records are often described in legal documents as “tangible things.”

For any questions or comments, please contact Sean Vitka at sean@demandprogress.org or Jason Pye at jpye@freedomworks.org.
protested, rather quaintly in hindsight, that it would provide the government with warrantless access to library records.\(^3\) Twelve years later, the public would learn that the government used Section 215 to force the major telephone companies in the United States to programmatically provide the National Security Agency (NSA) with all telephone metadata — records about phone calls — for all customers. This became publicly known as the “bulk telephone metadata program.”\(^4\)\(^5\)

The most recent legislation directly amending Section 215 was the USA FREEDOM Act of 2015. The new law prohibited the untargeted collection of all records of all customers (i.e., “bulk” collection), instituted certain transparency requirements, extended Section 215’s sunset to December 15, 2019, made records available to the government that it had previously been unable to obtain under Section 215, and permitted the collection of records up to two degrees away from a target. This two-degree surveillance, sometimes called ‘two hops,’ dramatically expands how many innocent people Section 215 affects: if a target receives a marketing call, records of the hundreds or thousands of other people contacted by that marketer would then be collected by the NSA.

A brief chronology illuminates the compromise at the heart of the USA FREEDOM Act:

- Until February 5, 2014, the government collected all records in bulk and was permitted to search them for all records within three degrees of a target, which would return all of a target’s contacts, all of the target’s contacts’ contacts, and then once more, revealing another set of contacts.
- On February 5, 2014, pursuant to a directive from President Obama, the government continued to collect all records in bulk, but had to submit targets’ selectors (e.g., a phone number) for approval to the FISC first, and analysts’ search results were limited to records within two degrees of a target.
- On May 7, 2015, the U.S. Court of Appeals for the Second Circuit held that the government’s expansive interpretation of Section 215 was “unprecedented and unwarranted.” To date, this is the highest court known to rule on the merits of Section 215 surveillance.
- On June 2, 2015, President Obama signed the FREEDOM Act into law, which codified in statute that the government may programmatically collect records within two degrees of a target on an ongoing basis under Section 215, and for the first time allowed the government to compel technical assistance from providers.

\(^3\) [https://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-library-records](https://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-library-records).


\(^5\) Notably, the FISC did not render a legal opinion on whether Section 215 authorized bulk collection until after the program was disclosed in 2013 — the Court simply approved the application and ordered recipients to produce the records. In that first analysis, FISC Judge Eagan concluded: “Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.” The opinion is available at [https://www.aclu.org/files/assets/br13-09-primary-order.pdf](https://www.aclu.org/files/assets/br13-09-primary-order.pdf).

For any questions or comments, please contact Sean Vitka at sean@demandprogress.org or Jason Pye at jpye@freedomworks.org.
USA FREEDOM thus modified and codified the ongoing, programmatic collection of records within two degrees of a target. Under this authority, the government established the “Call Detail Records” program.

**Call Detail Records vs. ‘Traditional’ Business Records**

Section 215’s newly created Call Detail Records (CDR) provision requires companies to process and tailor the records they provide the government. These requests provide the government with all of a target’s telephone records, including what phone numbers they called and when, *as well as* all records relating to those newly identified phone numbers. The company must provide those records on a daily basis for up to 180 days. Each order can affect many people: while the government issued only 14 CDR program orders in 2018, it collected over 434 million records relating to over 19 million phone numbers.

Section 215’s traditional business records orders are distinct from CDR program orders, but we know less about them. We do know the government can use traditional business records orders for a wider variety of purposes; that intelligence agencies do not report the total number of records collected pursuant to them; and that far more types of records are subject to them, including medical records, firearms sales records, and purchase records. However, the government may disfavor the use of traditional business records in some circumstances. For example, Section 215 does not explicitly provide them with the power to compel ongoing, daily production.

The Foreign Intelligence Surveillance Court issued 56 traditional business records orders in 2018, which collected information pertaining to at least 214,860 unique identifiers, including but not limited to telephone numbers and email addresses. It is possible that the government collected significantly more information, but we do not know because it is only required to report those unique identifiers “used to communicate information.”

**Problems with Section 215**

Section 215 collection has been plagued by abuse and misuse. This includes the overproduction of information, which is when a company gives the government more information than it is permitted to obtain under a FISC order, and overcollection, which is the government’s acquisition of that information. The government has admitted to both collecting more information than permitted by law and exceeding its authorized use of that information.

A recent overproduction issue may have imperilled the CDR program’s very existence, although Congress and the public cannot be certain in the absence of more information from the government. In June 2018 the NSA
announced it had collected a substantial amount of information that it was not permitted by law to receive. The NSA said it was not feasible to identify the unlawfully acquired information, and that it would instead delete all records it had collected since the CDR program’s inception. Oddly, while procedures around the NSA’s intake process are specifically designed to identify this kind of overproduction, it took over two years for the government to realize its error — at the expense of the privacy of millions of innocent people. After resuming collection, the government again discovered an overproduction. According to The New York Times, the government shut down the CDR program in late 2018. The government, however, has not provided official confirmation that it was shut down. Additionally, we would not know whether this collection was restarted, and if so, under what authority.

Severe privacy violations have been attendant to this type of collection for almost two decades — since even before Congress passed the PATRIOT Act. On October 4, 2001, President George W. Bush directed the NSA to use electronic surveillance within the United States without a court order, beginning what would become known as the “President’s Surveillance Program” (PSP). As a consequence of this order, “the NSA intercepted the content of international telephone and Internet communications of both U.S. and non-U.S. persons. In addition, the NSA collected telephone and Internet metadata.”

The program was founded on secret, and later repudiated, legal memoranda written by the Department of Justice’s (DOJ) Office of Legal Counsel, namely by attorney John Yoo, who concluded that FISA “cannot restrict the President’s ability to engage in warrantless searches that protect the national security.” (Yes, that John Yoo.) The companies that unlawfully provided the government with sensitive customer information pursuant to the PSP would later be given legal immunity by Congress for claims arising from that production.

While in operation, the PSP collected in bulk the same kinds of records the FISC would later order telephone companies to provide under Section 215. The PSP also permitted analysis of information two degrees away from a target (sometimes referred to as ‘contact chaining’), which USA FREEDOM would later codify. The entire endeavor was a violation of the Foreign Intelligence Surveillance Act.

Since the PSP concluded in 2007, the government has continuously failed to operate within the bounds of FISA. Publicly known violations of the statute include the unlawful overcollection of information and failure to adhere to rules set by the Foreign Intelligence Surveillance Court, most often described as ‘minimization procedures.’

For any questions or comments, please contact Sean Vitka at sean@demandprogress.org or Jason Pye at jpye@freedomworks.org.
The FISC establishes such rules to protect privacy when issuing an order pursuant to a Section 215 application. In our 2017 report, “Institutional Lack of Candor,”\(^9\) we detailed extensive violations identified by the FISC itself, primarily involving the government’s use of Section 702 of the FISA Amendments Act of 2008. A separate report will provide a more thorough overview of the government’s history of misusing Section 215 as well as the government’s repeated failure to be transparent with and abide by the rules set by its oversight bodies (namely the FISC and Congress).

Questions Congress Must Have Answers to Before Reauthorizing Section 215

USA FREEDOM has significant and conspicuous gaps in its transparency requirements involving Section 215, even though it has increased the transparency of FISA surveillance generally. These gaps include the absence of required reporting on the total number of records collected under Section 215 and explicit exemptions to various reporting requirements for the FBI. Congress must not legislate in the dark, and as such the following questions should be fully and publicly answered as Congress considers reauthorizing Section 215:

Regarding the CDR program:

1. Did the government shut down the Call Detail Records program, and if so, why? Was it due to the overproduction/overcollection issues reported by the NSA in June 2018 or a subsequent incident?

2. The NSA said it deleted all CDR program records because of “technical irregularities in some data received from telecommunications service providers” that “resulted in the production to NSA of some CDRs that NSA was not authorized to receive.” NSA further determined that it would be “infeasible to identify and isolate properly produced data.” Was the collection of this improperly produced data specifically prohibited by Congress? Or did it implicate people who were not within two degrees of a court-approved target? Why is it infeasible for the NSA to identify and/or isolate the improperly produced data?

3. Will the NSA publicly identify which provider or providers have overproduced information since enactment of the FREEDOM Act?

4. Was the delivery of this data illegal under FISA or any other law?

5. Has the NSA referred the company or companies that overproduced this information, in violation of their customers’ privacy, to the Department of Justice or Federal Trade Commission? If not, why not?

6. Is collection similar to that which occurred under the CDR program occurring under any other authority, such as the DEA program obtaining call records to specific countries?

7. What specific terrorist attacks have been thwarted that would not have been absent the CDR program? What other national security threats have been mitigated?


For any questions or comments, please contact Sean Vitka at sean@demandprogress.org or Jason Pye at jpye@freedomworks.org.
Regarding traditional business records orders:

8. What kinds of records did the government seek in the twenty traditional business records applications made in 2018 that, according to the Department of Justice, “did not specifically identify an individual, account, or personal device as the specific selection term”? How many records were produced in response?

9. Does the FBI or NSA consider an IP address or a physical address for a high-traffic, public location (such as a hotel) an “address” for the purposes of satisfying the specific selection term requirement of a traditional business records application? (Traditional orders have lower standards for records collection, and the government may argue that so-called “bulky” selection terms that produce large volumes of information on innocent people satisfy that lower standard.)

10. What types of records have been collected using traditional business records orders?

11. What specific selection terms have the FBI and NSA used that do not identify a person, account, address, or personal device?

12. How many unique identifiers, beyond those “used to communicate information,” were collected pursuant to traditional business records orders in 2018?

13. How many records were collected pursuant to the 56 traditional business records orders in 2018?

14. How many records and unique identifiers were received by the FBI and NSA through non-electronic means, for instance in hard-copy or portable media formats? How many times has the FBI or NSA received information in such formats? (The government does not disclose how much information is collected in these formats.)

15. Has the FBI or NSA used, or concluded it may use, traditional business records orders to collect information on an ongoing basis, without a new or renewed order from the FISC? (The CDR program explicitly provides for ongoing collection, but the provision authorizing traditional business records orders is silent on the question.)

16. Can the government compel and are providers compensated for technical assistance related to the production of traditional business records, including production of CDRs pursuant to traditional business records orders, as they are in the CDR program?

17. What specific terrorist attacks have been thwarted that would not have been absent traditional business records orders? What other national security threats have been mitigated?

Regarding Section 215 and FISA generally:

For any questions or comments, please contact Sean Vitka at sean@demandprogress.org or Jason Pye at jpye@freedomworks.org.
18. Can or have characteristics such as race, religion, national origin, gender, sexual orientation, or political views be used to make targeting and surveillance decisions under Section 215 or other FISA authorities?

19. Has there been any effort to assess the disproportionate impacts Section 215 and Section 702 surveillance have on immigrant communities and communities of color? If not, why not? If so, what conclusions did the government reach?

20. Has the government used First Amendment-protected activities as a basis, in whole or in part, to conduct surveillance under Section 215 or other FISA authorities?

21. How many people in the United States has the government incidentally collected information on pursuant to Section 702?

22. How many times has Section 215 information or information derived from Section 215 surveillance been used in criminal investigations or prosecutions? What are the Department of Justice’s procedures regarding provision of notice to defendants in such cases? And has such information been disseminated to law enforcement or prosecutorial entities without specific disclosure to those entities that it was obtained pursuant to a Section 215 order? (The government maintains it is not constitutionally or statutorily obligated to provide notice to defendants of Section 215 surveillance.)

23. Is the government collecting, under FISA or otherwise, metadata regarding apps such as Signal, WhatsApp, Facebook Messenger, iMessage or similar apps?

24. Are there any non-public Office of Legal Counsel opinions interpreting Section 215 or Section 702? If so, what specific conclusions do they reach?

25. Does the Department of Justice maintain that the Foreign Intelligence Surveillance Act “cannot restrict the President’s ability to engage in warrantless searches that protect the national security”?