

# **Section 215: A Brief History of Violations**

September 2019

One of the most controversial surveillance authorities in United States history, Section 215 of the USA PATRIOT Act, is scheduled to sunset on December 15, 2019. As Congress considers whether to reauthorize this provision and, if so, with what reforms, it is important to understand the context of how the government has used this authority. Since September 11, 2001, the government has been in nearly continuous violation of the statutory and judicial rules governing domestic surveillance.

Specifically, the government has:

1. Used Section 215 to unlawfully acquire large amounts of sensitive information about innocent people in the United States;
2. Repeatedly failed to comply with court orders that limit the handling, sharing, and analysis of information acquired pursuant to Section 215; and
3. Lied to, misled, and failed to be transparent with Congress about its use of Section 215.

In this report, we review the government's application of Section 215 and related legal authorities to conduct surveillance in the United States since September 11. We divide the past 18 years into three periods, reflecting the different legal foundations asserted for the government's collection of phone records. After covering these periods, we briefly survey the executive branch's refusal to fully inform Congress of its Section 215-related surveillance practices since September 11.<sup>1</sup>

---

<sup>1</sup> Due to secrecy around these programs, the limited ability of overseers to identify every compliance issue, and the sheer volume of known problems, this report is not a comprehensive accounting of every violation.

## Table of Contents

<b>I. SUMMARY OF SECTION 215</b>	<b>3</b>
A. History of Surveillance	3
B. History of Section 215	3
<b>II. TIMELINE OF RECORDS SURVEILLANCE IN VIOLATION OF FISA</b>	<b>6</b>
<b>III. PERIOD ONE: STELLARWIND (2001 - 2006)</b>	<b>8</b>
A. Starting the Dragnet	8
B. Whistleblowers and Shifting Legal Foundations	10
<b>IV. PERIOD TWO: THE BULK TELEPHONE METADATA PROGRAM (2006 - 2015)</b>	<b>12</b>
A. Minimization Procedures	13
B. First Amendment Review	15
C. Overproduction and Overcollection	16
<b>V. PERIOD THREE: THE CALL DETAIL RECORDS PROGRAM (2015 - 2019)</b>	<b>18</b>
A. More Overproduction and Overcollection Issues	19
B. Amicus Curiae Review	19
<b>VI. INADEQUATE DISCLOSURES TO CONGRESS (2001 - PRESENT)</b>	<b>21</b>
A. Avoiding Congress	21
B. Capturing the House Permanent Select Committee on Intelligence	22
C. Misleading Congress	23
<b>VII. CONCLUSION</b>	<b>25</b>

## **I. SUMMARY OF SECTION 215**

### **A. History of Surveillance**

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, FISA also granted the government the authority to spy on Americans 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 11 terrorist attacks, Congress weakened the limited protections established by FISA by enacting the USA PATRIOT Act (PATRIOT Act). Contrary to the government's political messaging around the PATRIOT Act, the 9/11 Commission Report later concluded that the failure to prevent the attacks was a result of poor intelligence sharing, not insufficient government authority to gather information.

Congress subsequently amended both laws to provide the government with new ways to secretly collect information. Guarded by the secrecy that shrouds these collection tools, the executive branch has been in nearly constant violation of FISA and the rules governing surveillance since September 11, 2001, and during this time, it has warrantlessly collected information on virtually every American.

### **B. History of Section 215**

One PATRIOT Act amendment, Section 215 of that law, expanded a provision of FISA to provide the government with 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. Section 215 orders also apply to people's purchase records, which reveal what people buy, when, and where. Location, medical, and firearms sales records are among the other digital and physical things subject to Section 215. These intended uses are similar to other legal processes to acquire information, such as subpoenas.

Congress established a sunset provision for the changes made by Section 215 so that Congress could periodically review whether the law achieved its intended effects.<sup>2</sup> During those sunset and reauthorization

---

<sup>2</sup> Colloquially, "Section 215" is used to refer to both the original PATRIOT Act section that created the modern 50 U.S.C. § 1861 and 50 U.S.C. § 1861 itself.

debates, Section 215 was further altered, which both expanded and contracted the surveillance permitted. Throughout this report, we will refer to different versions of Section 215 based on which law most recently amended the authority.

To obtain information pursuant to Section 215, the government makes an application to the Foreign Intelligence Surveillance Court (FISC) for an order to produce records (or other tangible things)<sup>3</sup> that the FISC *must* issue so long as Section 215's low standards are met. The FISC only hears from the government, and the people affected by the order never have an opportunity to contest the government's application. 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 the fact 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 protested, rather quaintly in hindsight, that it would provide the government with warrantless access to library records.<sup>4</sup> 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.”<sup>5,6</sup>

The most recent legislation directly amending Section 215 was the USA FREEDOM Act of 2015 (FREEDOM Act). 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

---

<sup>3</sup> These records are often described in legal documents and in statute as “tangible things.” The law explicitly provides for the collection of “books, records, papers, documents, and other items,” as well as “library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records.” 50 U.S.C. § 1861(a).

<sup>4</sup> See <https://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-library-records>.

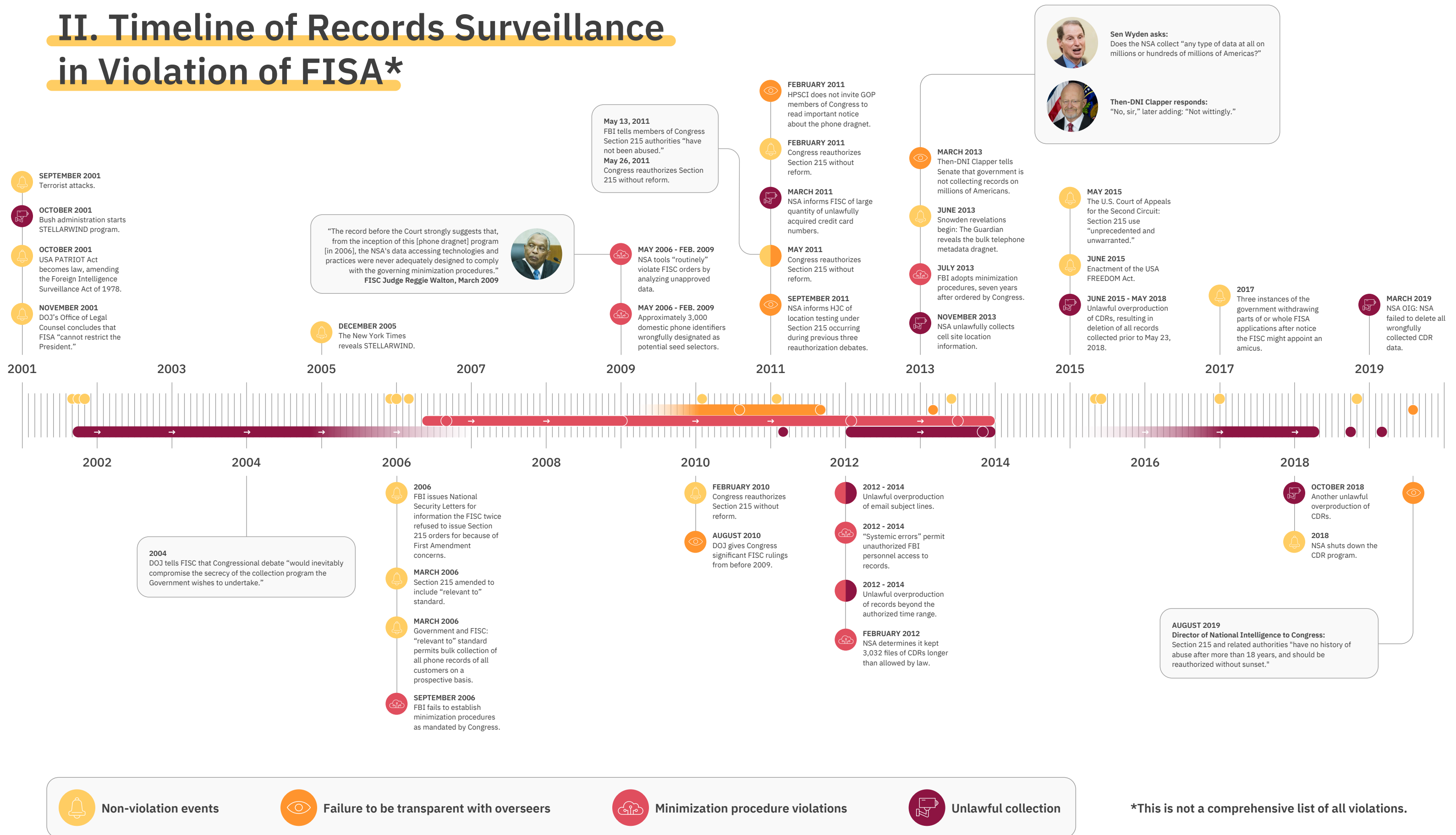
<sup>5</sup> See <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

<sup>6</sup> 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 applications 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.” Claire Eagan, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], Docket Number: BR 13-109, date redacted, at 22, available at <https://www.aclu.org/files/assets/br13-09-primary-order.pdf>.



receives a marketing call, records relating to the hundreds or thousands of other people contacted by that marketer might then be delivered to the NSA.

## II. Timeline of Records Surveillance in Violation of FISA\*



**\*This is not a comprehensive list of all violations.**

### **III. PERIOD ONE: STELLARWIND (2001 - 2006)**

#### **A. Starting the Dragnet**

On October 4, 2001, in the immediate aftermath of the September 11 terrorist attacks, then-President George W. Bush directed the NSA to use electronic surveillance within the United States without a court order. The directive established a program known as STELLARWIND, which for over five years continued in violation of the Foreign Intelligence Surveillance Act of 1978, a law Congress explicitly enacted to define “the exclusive means by which electronic surveillance” may be conducted in the United States.<sup>7,8</sup>

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.”<sup>9,10</sup> In other words, the NSA collected communications of people in the United States, and information about the communications of people in the United States, without obtaining approval by a federal court.

The program was founded on secret, and later repudiated, legal memoranda written by the Department of Justice’s (DOJ) Office of Legal Counsel (OLC) that concluded FISA “cannot restrict the President’s ability to engage in warrantless searches that protect the national security.”<sup>11</sup>

Secrecy around the program was extreme: The first STELLARWIND authorization and subsequent renewals, founded upon OLC attorney John Yoo’s conclusion that FISA did not bind the president, were kept in a safe.<sup>12</sup> Only three Department of Justice officials were aware of it, not including Yoo’s direct supervisor, and his legal conclusions did not undergo “the usual editing and review process.”<sup>13,14</sup> Even the NSA, charged with conducting

---

<sup>7</sup> 50 U.S.C. § 1812.

<sup>8</sup> The government has used other terms, namely the “President’s Surveillance Program” (PSP) and the “Terrorist Surveillance Program,” to refer to parts of STELLARWIND. They are incorporated in this report by necessity because they are sometimes used by judicial and executive documents that assess the program.

<sup>9</sup> “Report on the President’s Surveillance Program,” by the Offices of the Inspectors General of the Department of Defense, the Department of Justice, the Central Intelligence Agency, the National Security Agency, and the Office of the Director of National Intelligence (July 10, 2009), at 1, available at <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>. The Inspectors General report also revealed that then-NSA Director Michael Hayden began expanding surveillance practices starting on September 14, 2001. Significant portions of those activities are redacted from the report, and so we are unable to assess their lawfulness. However, the report describes certain actions by Hayden on September 14 as “an aggressive use of authority because of [redacted].” Hayden described his actions as a “tactical decision.” *Id.* at 5.

<sup>10</sup> Metadata refers to the records of communications, like who communicated with whom, when, and for how long.

<sup>11</sup> *Id.* at 14.

<sup>12</sup> See <https://www.newyorker.com/magazine/2013/12/16/state-of-deception>.

<sup>13</sup> Report on the President’s Surveillance Program at 14.



the surveillance and analyzing its results, was prohibited from accessing the underlying OLC opinion.<sup>15</sup> The authorization was not written by the president or the president’s attorneys, but by David Addington, an attorney for then-Vice President Dick Cheney. When executive branch officials, and later the press, inquired into the legal underpinnings of STELLARWIND, others say Addington responded: “The blood of hundreds of thousands of Americans will be on your hands if you try to stop this. It’s time for you to decide what side you’re really on.”<sup>16</sup>

With this secret and flawed legal interpretation, the executive branch reclaimed much of the domestic surveillance power prohibited by FISA, even while Congress contemporaneously expanded the government’s surveillance powers by passing the PATRIOT Act. An unredacted draft of an NSA Inspector General’s report explains: “Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.”<sup>17</sup> Here, “otherwise” admits this domestic surveillance was prohibited by FISA.

By dismissing FISA’s legal mandates and the FISC’s statutorily mandated role, the government ensured that STELLARWIND would be governed by a more permissive set of rules for intelligence collection that are founded on the executive branch’s assertions concerning the president’s inherent Article II powers (broadly referred to as Executive Order 12333). The NSA draft report also identified the secrecy around the authorization and renewals as “a primary cause of two early violations of the Authorization,” though it does not offer more details about those violations. The executive branch renewed STELLARWIND every 30 to 60 days for five years in constant violation of FISA.

Nevertheless, Congress would later pass laws that the government interpreted as permission to conduct similar and even more expansive surveillance, and the government shifted its legal theories accordingly: “[B]etween July 2004 and January 2007, NSA ceased PSP collection activities [referring to STELLARWIND] under Presidential authorization and resumed them under four separate court orders issued in accordance with the Foreign Intelligence Surveillance Act of 1978 as amended.”<sup>18</sup> Until that legal foundation changed,

---

<sup>14</sup> Yoo would go on to be recognized for his role in laying the legal foundations for torture, also from his post at the Office of Legal Counsel — work that the DOJ’s Office of Professional Responsibility would later conclude constituted “intentional professional misconduct.” “Investigation into the Office of Legal Counsel’s Memoranda Concerning Issues Relating to the Central Intelligence Agency’s Use of ‘Enhanced Interrogation Techniques’ on Suspected Terrorists,” by the Office of Professional Responsibility of the Department of Justice (July 29, 2009), at 11, available at [https://www.aclu.org/sites/default/files/field\\_document/opr\\_full\\_release.pdf](https://www.aclu.org/sites/default/files/field_document/opr_full_release.pdf).

<sup>15</sup> “ST-09-0002 Working Draft,” by the Office of the Inspector General of the National Security Agency and Central Security Service (March 24, 2009), at 21, available at <https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf>.

<sup>16</sup> See <https://www.businessinsider.com/nsa-surveillance-authorization-came-from-cheney-attorney-2014-5>.

<sup>17</sup> ST-09-0002 Working Draft at 7.

<sup>18</sup> Report on the President’s Surveillance Program at 1, available at <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>.

STELLARWIND collected in bulk<sup>19</sup> the same kinds of records that the FISC would later order telephone companies to provide under Section 215.

## **B. Whistleblowers and Shifting Legal Foundations**

Escalating concerns about STELLARWIND's legality caused a shift in the program's legal foundations between 2004 and 2007, spurred in large part by a significant number of DOJ officials threatening resignation.<sup>20</sup> While senior staff debated the legality of the program, others took action. In 2005, one concerned DOJ attorney, Thomas Tamm, contacted The New York Times to reveal STELLARWIND.<sup>21</sup>

The administration's public response to media coverage of STELLARWIND, delivered by President Bush and then-Deputy Director of National Intelligence General Michael Hayden, focused on narrow slices of the program, misleadingly obscured the scope of the surveillance, and claimed that there had been no opposition to the program from the officials involved.<sup>22</sup>

The government's misleading response prompted Thomas Drake, a senior NSA official, to go to the press — the first in a series of NSA whistleblowers who had for years been expressing their grave concerns over the program. The whistleblowers and those connected to them faced FBI raids and years-long prosecutions — including celebrated senior NSA employees and Diane Roark, a longtime Republican staffer for the House Permanent Select Committee on Intelligence.<sup>23</sup>

While the investigations largely failed to unearth any criminal activity, they came at a tremendous cost. Legal fees practically bankrupted Drake — he pled guilty to a misdemeanor, which was the only “success” of the investigations and served to mitigate fierce public condemnation of the prosecution.<sup>24</sup> Given that result, the judge who sentenced him called the “four years of hell” Drake and his family experienced “unconscionable.”<sup>25</sup>

---

<sup>19</sup> “Bulk” collection refers to acquisition of information without a specific target or other limiting factors, for instance the records of all calls made by all customers of a telephone service provider.

<sup>20</sup> See [https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a\\_story.html](https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html).

<sup>21</sup> After multiple discussions, in which the government asserted revealing the program would lead to bloodshed, Times executive editor Bill Keller decided to kill the story. About one year later, James Risen, one of the authors of the story, forced The New York Times to revive the story by threatening to publish a book about the same matter, including the Times's decision to back down. Then-President Bush personally told The New York Times that they would be complicit in the next terrorist attack. See “United States of Secrets, Part One,” Frontline (May 13, 2014), at 1:08:28, available at <https://www.pbs.org/wgbh/frontline/film/united-states-of-secrets/>.

<sup>22</sup> See *id.* at 1:20:10.

<sup>23</sup> See *id.* at 1:23:42.

<sup>24</sup> See <https://www.npr.org/2014/07/22/333741495/before-snowden-the-whistleblowers-who-tried-to-lift-the-veil>.

<sup>25</sup> <https://www.baltimoresun.com/maryland/bs-md-thomas-drake-sentencing-20110715-story.html>

The FBI raided the homes of William Binney, Drake, Ed Loomis, Roark, and J. Kirk Wiebe with guns drawn.<sup>26</sup> They all lost their jobs.

The companies that unlawfully provided the government with sensitive customer information pursuant to STELLARWIND would later be given legal immunity by Congress for claims arising from that production.<sup>27</sup> To this day, companies are given significant legal immunity and financial compensation for their cooperation in spying on their customers.

STELLARWIND would continue in part until 2007, and it continually violated FISA until its end. But the government did not cease these practices — it moved them. Perhaps the most egregious FISA violation among the collection occurring under STELLARWIND — the warrantless collection of the content of communications originating or terminating in the United States — ended and restarted under another legal authority in 2007. The collection most similar to that currently occurring under Section 215 shifted to that authority in 2006.

---

<sup>26</sup> See <https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers>.

<sup>27</sup> See 50 U.S.C. § 1885a.

#### **IV. PERIOD TWO: THE BULK TELEPHONE METADATA PROGRAM (2006 - 2015)**

The government barely used Section 215 before 2004.<sup>28</sup> But secret interpretations of the PATRIOT Act, including subsequent amendments to it, would soon use Section 215 as a sweeping surveillance authority. Indeed, Section 215 would become the home of some of the illegal surveillance that had been occurring under STELLARWIND.

Before the PATRIOT Act, the provision amended by and now known as Section 215 provided the FBI with the ability to obtain records from “common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities.”<sup>29</sup> To obtain a Section 215 order either then or now, the government must make an application to the Foreign Intelligence Surveillance Court for an order, which the court must issue if Section 215’s low standards are met. Records subject to the pre-PATRIOT Act Section 215 would reveal, for instance, who was renting a car or a particular storage locker.

In 2001, Section 215 of the PATRIOT Act changed the language that limited the types of records that could be acquired, permitting the government to obtain “any tangible things,” such as “books, records, papers, documents, and other items,” while also lowering the evidentiary threshold for obtaining an order.<sup>30</sup> This expansion sparked widespread public concern that Section 215 would be used to collect library records without a warrant.<sup>31</sup>

The FISC first approved the bulk telephone metadata program under Section 215 in 2006.<sup>32</sup> Both the FISC and the government concluded that Section 215 permitted bulk collection under an aggressive interpretation of the Third Party doctrine, which generally holds that a person does not have a reasonable expectation of privacy in records held by third parties and therefore that the government does not need a warrant to seize that

---

<sup>28</sup> A 2016 DOJ IG Report describes just one pre-PATRIOT Act order, issued between 1998 and the passage of the PATRIOT Act in 2001. See “A Review of the FBI’s Use of Section 215 Orders for Business Records in 2012 through 2014” (“2016 DOJ IG Report”), by the Office of the Inspector General of the Department of Justice (September 2016), at 4, available at <https://oig.justice.gov/reports/2016/o1604.pdf>. A 2007 DOJ IG Report describes the first “pure” post-PATRIOT Act Section 215 order being approved in May 2004. See “A Review of the Federal Bureau of Investigation’s Use of Section 215 Orders for Business Records” (“2007 DOJ IG Report”), Office of the Inspector General of the Department of Justice (March 2007), at 17, available at <https://oig.justice.gov/special/s0703a/final.pdf>.

<sup>29</sup> These records are often described in legal documents as “tangible things.”

<sup>30</sup> 2016 DOJ IG Report at 4-5.

<sup>31</sup> See <https://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-library-records>.

<sup>32</sup> See “Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act,” (August 9, 2013), at 1, available at <https://fas.org/irp/nsa/bulk-215.pdf>.

information.<sup>33</sup> Accordingly, the government held, these records were not protected by the Fourth Amendment, no matter the volume or number of people affected.

The government's unbounded interpretation of Section 215 would later be subject to intense public criticism. That interpretation would also fail in front of the highest court to rule on the merits of the issue.<sup>34</sup> However, even without consideration for the Fourth Amendment, the government's mass surveillance during this period failed to comply with Section 215 and the rules ordered by the FISC.

### A. Minimization Procedures

One of the FISC's most critical roles is to establish the conditions under which Section 215 collection may be conducted, which it does by overseeing the government's "minimization procedures." When the government fails to abide by minimization procedures, it fails to abide by the rules judges set when they approve orders. In other words, violations of minimization procedures break the FISC's rules, which are mandated by Congress.

These minimization procedures are intended to protect against the unnecessary collection, retention, and dissemination of information about U.S. persons, as FISA is focused on the collection of "foreign intelligence information" between "foreign powers" and the "agents of foreign powers," in particular those who are suspected of espionage or terrorism. In general, minimization procedures limit who can access the data, how it can be disseminated, and how long it may be kept.

The government first failed to comply with minimization rules involving Section 215 by failing to establish them at all. In March 2006, as part of a PATRIOT Act reauthorization, Congress mandated that "Not later than 180 days after the date of the enactment" of the reauthorization, "the Attorney General shall adopt specific minimization procedures governing the retention and dissemination" of information collected under Section 215.<sup>35</sup> The FBI only finalized minimization procedures designed to reduce the retention of non-public information on March 7, 2013, with formal adoption on July 1, 2013, *seven years after* Congress first required the FBI to adopt them.<sup>36</sup>

---

<sup>33</sup> See *id.* at 19-21. This precedent was significantly curtailed by the Supreme Court's 2018 decision in *Carpenter v. United States*, where the Court held that the Third Party doctrine "does not by itself overcome the user's claim to Fourth Amendment protection." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

<sup>34</sup> See *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), available at <https://www.aclu.org/legal-document/aclu-v-clapper-appeals-court-ruling>.

<sup>35</sup> Section 106(g) of the USA PATRIOT Improvement and Reauthorization Act of 2005, available at <https://www.congress.gov/109/plaws/publ177/PLAW-109publ177.pdf>.

<sup>36</sup> The DOJ's Inspector General first reported that the FBI had failed to fulfill this obligation in "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006" ("2008 DOJ IG Report"), by the Office of the Inspector General of the Department of Justice (March 2008) at 75-83, available at <https://oig.justice.gov/special/s0803a/final.pdf>. It reported on the seven-year delay in fulfilling this mandate in the 2016 DOJ IG Report at 10-16, available at <https://oig.justice.gov/reports/2016/o1604.pdf>. The Inspector

While this violation spans years, it is not the only example of the government violating minimization procedures during this period. In 2009, the government informed the FISC about a slew of violations involving the bulk telephone metadata program, including using unauthorized analytical techniques and permitting access to the data outside of trained NSA analysts.

FISC Judge Reggie Walton reviewed the compliance problems from 2006 to 2009 and explained that “the root of the non-compliance is not a terminological misunderstanding, but the NSA's decision to treat the accessing of all call detail records produced by [redacted] no differently than other collections under separate NSA authorities, to which the Court-approved minimization procedures do not apply.”<sup>37</sup> Walton went on, “The record before the Court strongly suggests that, from the inception of this [phone dragnet] program [in 2006], the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures.”<sup>38</sup>

Effectively, the NSA had treated data collected under a more stringent domestic surveillance law the same way it treated data collected overseas pursuant to Executive Order 12333, which is significantly more permissive than FISA and is the same authority STELLARWIND operated under. In sum, it had been violating the law for three years, including after being explicitly ordered to correct its practices by the FISC.<sup>39</sup>

In 2012, the NSA discovered it had kept thousands of files containing call detail records longer than allowed by law, and that it had commingled that data with wrongfully retained information collected under STELLARWIND. The agency found that “approximately 3,032 files containing call detail records” had been retained “in violation of the 5-year retention period,” on a server that also “contain[ed] information related to the STELLARWIND program and files which do not appear to be related to either of these programs.”<sup>40</sup>

As noted by an oversight body within the executive branch, the Privacy and Civil Liberties Oversight Board (PCLOB), the NSA never identified how serious the violation was. “Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the

---

General found that the FBI adopted only Interim Procedures that did not add any new requirements by the mandated deadline, and that the Interim Procedures also failed to, among other things, define what “necessary to understand foreign intelligence information or assess its importance” meant, terms that govern both data dissemination and retention rules. 2016 DOJ IG Report at 11.

<sup>37</sup> Reggie Walton, In Re Production of Tangible Things from [redacted], Docket Number: BR 08-13, March 2, 2009, at 6, available at <https://www.aclu.org/files/natsec/nsa/March%202009%20FISC%20Order%20BR%2008-13.pdf>.

<sup>38</sup> *Id.* at 14-15.

<sup>39</sup> *See id.*

<sup>40</sup> “NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – Executive Summary,” letter from SID Oversight & Compliance to SIGINT Director (May 3, 2012) at 11-12, available at <https://www.aclu.org/foia-document/sid-oversight-and-compliance>.



NSA could not provide an estimate regarding the *volume* of calling records that were retained beyond the five-year limit” (emphasis added).<sup>41</sup> The NSA destroyed the records, making it impossible to determine the extent of their violation.

Since 2012, the DOJ’s Inspector General has identified violations of rules designed to avoid overcollection of information, which occurs when the government receives more information than permitted by the FISC or the law. One FBI database permitted agents to access data before the data was reviewed to ensure it was responsive to the FISC order.<sup>42</sup> An incident like this is particularly troubling because this review is a key step to avoiding overproduction of records to the government, another persistent problem with Section 215 compliance.

## **B. First Amendment Review**

The First Amendment protects political speech, which is implicated when the government collects information about a person based upon, for instance, their political views. Courts have generally focused on the Fourth Amendment, even when a First Amendment issue has been raised by a plaintiff.<sup>43</sup> Nevertheless, First Amendment considerations were a significant compliance problem for the bulk telephone metadata program that operated between 2006 and 2015.

Section 215 prohibits the government from obtaining a Section 215 order “solely upon the basis of activities protected by the first amendment.”<sup>44</sup> Such activities include organizing, protesting, and other expressions that are vital to our democracy. Notably, however, this also means that a Section 215 order predicated primarily or significantly on First Amendment-protected activity is not prohibited. Even with this low bar, the government has not consistently provided adequate protections for First Amendment-protected activity relative to Section 215.

One problem affected approximately 3,000 domestic telephone identifiers between May 24, 2006, and February 2, 2009. According to a declaration to the FISC by the government, if an identifier does not undergo NSA

---

<sup>41</sup> “Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court” (“PCLOB 215 Report”), by the Privacy and Civil Liberties Oversight Board (January 23, 2014), at 55, available at [https://www.pclob.gov/library/215-Report\\_on\\_the\\_Telephone\\_Records\\_Program.pdf](https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf).

<sup>42</sup> 2016 DOJ IG Report at vii, 63, available at <https://oig.justice.gov/reports/2016/o1604.pdf>.

<sup>43</sup> In *United States v. Basaaly Moalin*, for example, Judge Jeffrey Miller conducted a thorough analysis of defendant’s Fourth Amendment rights relative to the bulk telephone metadata program, but dismissed his First Amendment claim cursorily. See *United States v. Basaaly Moalin*, “Order Denying New Trial,” Case Number: 10cr4246 JM (S.D. Cal., November 14, 2013), at 14, available at <https://www.emptywheel.net/wp-content/uploads/2013/11/131114-Deny-New-Trial.pdf>. Similarly, in *Klayman v. Obama*, Judge Richard Leon issued an injunction against the bulk telephone metadata program but offered only a Fourth Amendment analysis, deeming it the most likely to succeed. See *Klayman v. Obama*, Docket Number: 13-0851 RJL (D.D.C., December 16, 2013), available at [https://ecf.dcd.uscourts.gov/cgi-bin/show\\_public\\_doc?2013cv0851-48](https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48).

<sup>44</sup> 50 U.S.C. § 1861(a)(1).

Office of General Counsel [OGC] approval, it means “the domestic telephone identifier [can be] chained without having first gone through an NSA OGC First Amendment review.”<sup>45</sup> Chaining, or “contact chaining,” refers to using the collected communications records to map people’s associations. This review is designed to ensure that the surveillance is not predicated “solely upon the basis of activities protected by the first amendment.” “NSA’s OGC had not reviewed and approved their use as ‘seeds’ as required by the Court’s Orders.”<sup>46</sup>

In 2008, the DOJ’s Inspector General revealed the government bypassed the FISC when a First Amendment issue arose. After the FISC, “citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation,” the FBI used National Security Letters to obtain the same information.<sup>47</sup> National Security Letters (NSLs) do not undergo court review, but, the government argues, allow the FBI to compel the production of records similar to those subject to Section 215.

In spite of the required First Amendment review and violations of that requirement, the FISC is not known to have issued a ruling on the degree to which First Amendment-protected activities can factor into an order until February 19, 2013.<sup>48</sup>

### C. Overproduction and Overcollection

---

<sup>45</sup> In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of the National Security Agency, (August 17, 2009), at 82, available at [https://www.aclu.org/files/assets/pub\\_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf](https://www.aclu.org/files/assets/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf).

<sup>46</sup> *Id.* at 81.

<sup>47</sup> 2008 DOJ IG Report at 5, available at <https://oig.justice.gov/special/s0803a/final.pdf>.

<sup>48</sup> John Bates, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], Docket 13-25, February 19, 2013. Available at <https://www.fisc.uscourts.gov/sites/default/files/BR%2013-25%20Opinion-1.pdf>.

In that opinion, the FISC notes that a proposed target’s speech “seems to fall well short of the sort of incitement to imminent violence or ‘true threat’ that would take it outside the production of the first amendment.” A redacted portion continues: “Indeed, the government’s own assessment of [redacted] points to the conclusion that it is protected speech.” The court concluded, however, that FISA “does not restrict the Court to considering only the activities of the subject of the investigation” in determining whether an application for a Section 215 order by the FBI is predicated solely on First Amendment-protected activity. The judge then appears to have incorporated the activities of others into the analysis: “According to the application, the government is investigating [redacted] not only on the basis of his own personal words and conduct ... but also on the basis of the admitted or suspected [redacted],” and ultimately concludes that the actions of those apparent associates overcome the prohibition. *Id.* at 5. Notably, the target’s association with those individuals might itself be protected by the First Amendment.

In the same period that the FISC issued this opinion, “several” applications were withdrawn short of final submission to the FISC — applications predicated on statements “advocating jihad” that may have raised First Amendment concerns. 2016 DOJ IG Report at 26, available at <https://oig.justice.gov/reports/2016/o1604.pdf>.



Overproduction is when a company gives the government more information than it is permitted to obtain under a FISC order; overcollection is the government's intake of that information. Over the years, the government has admitted to both collecting more information than permitted by law and exceeding its authorized use of that information. These problems have persisted since the bulk collection program and since passage of the FREEDOM Act. Among these violations are:

- The unlawful collection of “a large quantity of customer credit card numbers” described in letters to the FISC in 2011;<sup>49</sup>
- Instances of unlawful productions of cell site location information, which NSA disclosed to an oversight board in 2013;<sup>50</sup>
- The unlawful production of email subject lines relating to orders issued in 2013 and 2014, which constitute communication content and trigger Fourth Amendment protections;<sup>51</sup> and
- The unlawful production of records beyond the authorized time range, which relates to an unknown number of orders issued between 2012 and 2014.<sup>52</sup>

Regarding the unlawful production of records beyond the authorized time range, and potentially the unlawful production of email subject lines, the DOJ Inspector General wrote: “Given the large number of business records orders issued between 2012 and 2014, we did not attempt to independently identify or describe all of the compliance incidents that occurred during our review period.”<sup>53</sup> In other words, they didn't look into the can of worms the government's violations had opened. What may prove to be the most consequential overproduction incident, however, was yet to come.

---

<sup>49</sup> PCLOB 215 Report at 55, available at [https://www.pclob.gov/library/215-Report\\_on\\_the\\_Telephone\\_Records\\_Program.pdf](https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf). See also Martin Feldman, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], Docket 11-57, April 13, 2011, available at <https://www.aclu.org/files/natsec/nsa/FISC%20Supplemental%20Order%20BR%2011-57.pdf>.

<sup>50</sup> See “Final Report of the Audit on the FISA Amendments Act §702 Detasking Requirements,” by the National Security Agency/Central Security Service (November 24, 2010), at 62-63, available at <https://www.documentcloud.org/documents/2755677-NSA-IG-reports-reprocessed-pages-March-2016.html>. Full report with additional redactions available at <https://www.documentcloud.org/documents/2712306-Savage-NYT-FOIA-IG-Reports-702-2.html>.

<sup>51</sup> See 2016 DOJ IG Report at 17, available at <https://oig.justice.gov/reports/2016/o1604.pdf>.

<sup>52</sup> See *id.* at 17-18.

<sup>53</sup> See *id.* at 17.

## **V. PERIOD THREE: THE CALL DETAIL RECORDS PROGRAM (2015 - 2019)**

Edward Snowden's revelations in 2013 triggered intense political and legal battles. Congress debated how to respond for two years, but did not act until sunset dates and court cases generated even more urgency.

In May 2015, the U.S. Court of Appeals for the Second Circuit fundamentally changed the debate around the government's use of Section 215. It held the government's use of Section 215 was "unprecedented and unwarranted."<sup>54</sup> To date, this is the highest court known to rule on the merits of Section 215 surveillance, and it ruled that the government's use of Section 215 since 2006 was unlawful. On the other side of this ruling, it seemed the courts might force the telephone metadata dragnet to end — at least in the absence of congressional action.

Almost immediately after, however, Congress passed the FREEDOM Act, which established a Call Detail Records (CDR) program as a discrete provision of Section 215. This program was designed to maintain the theoretical value of the bulk telephone metadata dragnet, providing for similar analytical results but limiting the government's overall intake of call detail records.<sup>55</sup> "Traditional" Section 215 orders continue to exist alongside this CDR program, and were limited to a lesser extent by the FREEDOM Act. A brief chronology illuminates the compromise at the heart of the new program:

- 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 issued amid public outcry over the telephone dragnet, the government continued to collect all records in bulk, but had to submit targets' selectors (e.g., phone numbers) 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," adding fuel to a debate about whether and how to reauthorize Section 215, then slated to sunset on June 1, 2015.<sup>56</sup>
- On June 2, 2015, President Obama signed the FREEDOM Act into law, which prohibited bulk collection of call detail records in exchange for statutory authorization for the government to programmatically collect records within two degrees of a target on an ongoing basis under Section

---

<sup>54</sup> See *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), at 59, available at <https://www.aclu.org/legal-document/aclu-v-clapper-appeals-court-ruling>.

<sup>55</sup> We provide a brief(er) overview of how Section 215 currently functions in a separate report, Overview of Section 215 of the USA PATRIOT Act/USA FREEDOM Act, available at: [https://s3.amazonaws.com/demandprogress/reports/Section\\_215\\_Overview\\_Report.pdf](https://s3.amazonaws.com/demandprogress/reports/Section_215_Overview_Report.pdf) and <http://www.Section215.org>.

<sup>56</sup> *American Civil Liberties Union v. Clapper* at 59.

215. In addition, this new authority for the first time permitted the government to compel technical assistance from providers. The final product is the Call Detail Records program.

### **A. More Overproduction and Overcollection Issues**

In 2018, the NSA revealed it would destroy all of the records collected under the CDR program because at least one communications service provider — the companies that hold billions of records of people’s activity — was giving the government more records than permitted under the FREEDOM Act.<sup>57</sup> The government has provided few additional details to the public, but a subsequent NSA Inspector General investigation into the incident concluded that the agency had failed to delete all of the affected records.<sup>58</sup> The government has not announced which provider overproduced data and why, or if that provider will face any accountability for violating the privacy of potentially millions of innocent Americans.

Intake minimization procedures are specifically designed to identify this kind of overproduction, but it took 31 months for the NSA to recognize the error. Clearly, these procedures did not work.

The public would later learn, thanks to a Freedom of Information Act request filed by the American Civil Liberties Union, that another overproduction incident occurred later in 2018 after the NSA restarted the program.<sup>59</sup> The government has yet to make any official statement on the second incident, but it coincides closely with a significant recent development: the NSA shut down the CDR program in late 2018.<sup>60</sup>

In August 2019, while confirming for the first time that the program had been halted, the Trump administration nevertheless asked Congress to permanently reauthorize the authority.

### **B. Amicus Curiae Review**

By the agency’s own admission, the NSA’s CDR program unlawfully acquired data from 2015 to 2018. However, it was not the only violation of FISA. The FREEDOM Act included language stating that the FISC “shall appoint” an amicus curiae — an advisor to the court — “to assist such court in the consideration of any

---

<sup>57</sup> See “NSA Reports Data Deletion,” June 28, 2018, available at

<https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/>.

<sup>58</sup> See “Report on the Review of the National Security Agency/Central Security Service’s Deletion of Certain USA FREEDOM Act Data (ST-18-0008) - Special Study,” Office of the Inspector General of the National Security Agency (March 22, 2019), at 1, available at <https://int.nyt.com/data/documenthelper/1541-nsa-oig-report-on-the-deletion/b05ad69c26ac1259ab53/optimized/full.pdf>.

<sup>59</sup> See <https://www.nytimes.com/2019/06/26/us/telecom-nsa-domestic-calling-records.html>.

<sup>60</sup> See <https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html>.

application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate.”<sup>61</sup>

The purpose of the amicus was to inch toward having an independent voice represented before the FISC that could challenge arguments made by the government. While the FREEDOM Act allows the FISC to exercise discretion over what constitutes a significant interpretation of law, and the statute does not oblige the amicus to represent privacy concerns, it does mandate a report from the FISC when a judge chooses not to appoint one. The FISC has failed to honor this obligation on at least one occasion.

In 2018, the FISC’s yearly reauthorization of NSA surveillance conducted under Section 702 of the FISA Amendments Act for the first time permitted the NSA to query information collected pursuant to the Upstream program for U.S. persons. Upstream acquires the content and metadata of communications directly from, among other entities, email service providers.<sup>62</sup> This type of query, often called a “backdoor search,” is particularly troubling to privacy advocates because it produces for analysts communications that the government would have needed a warrant to intentionally collect, namely those that belong to a U.S. person and are protected by the Fourth Amendment.

When she considered this new surveillance practice, FISC Judge Rosemary Collyer neither appointed an amicus nor explained why such a significant change in the law didn’t merit one. The reauthorization was delayed by months, which provided more time than is usually available for such a review.

Collyer’s decision not to use the amicus related to surveillance under Section 702 of FISA, not Section 215. However, it violated an important provision in the FREEDOM Act that surveillance reformers secured during the 2014 and 2015 debates over whether to reauthorize Section 215. Further, the decision may be symptomatic of other issues. In 2017, the government withdrew three requests (or parts thereof) after the FISC informed the government it might appoint an amicus, and another in 2018.<sup>63</sup> The report doesn’t say what kind of orders were withdrawn, but Section 215 submissions were among those fully or partially withdrawn in 2017. This may mean that the government is avoiding amicus review precisely for the kind of applications that Congress anticipated might most benefit from an amicus curiae.

---

<sup>61</sup> 50 U.S.C. § 1803(i)(2).

<sup>62</sup> Rosemary Collyer, Memorandum Opinion and Order, April 26, 2017, at 27-30, available at [https://www.dni.gov/files/documents/icotr/51117/2016\\_Cert\\_FISC\\_Memo\\_Opin\\_Order\\_Apr\\_2017.pdf](https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf).

<sup>63</sup> Administrative Office for United States Courts letter to Bob Goodlatte, April 25, 2018, at 4-5. Available at <https://assets.documentcloud.org/documents/4446927/FISA-court-annual-report-2017.pdf>.

## VI. INADEQUATE DISCLOSURES TO CONGRESS (2001 - PRESENT)

From 2001 forward, the executive branch has failed to adequately inform Congress about its mass surveillance of Americans. These failures range from failing to inform Congress to lying to Congress under oath. Relatedly, as described above, the government has also spied on and prosecuted people who went to Congress to blow the whistle. Because these failings arguably walk the line between statutory violations and issues of candor with regards to Congress, we discuss them separately from the other violations identified so far.

### **A. Avoiding Congress**

When the DOJ first pushed the FISC to permit collection under FISA that had previously been conducted under STELLARWIND, in this case for the purpose of collecting email metadata in bulk under a provision closely related to Section 215, the DOJ argued that Congress could not be allowed to know about the interpretation of the law for which the executive advocated. “In almost all cases of potential constitutional conflict, if a statute is construed to restrict the executive, the executive has the option of seeking additional clarifying legislation from Congress,” the DOJ wrote in their memo urging FISC Judge Colleen Kollar-Kotelly to approve the first dragnet.

“In this case, by contrast,” the government continued, “the Government cannot pursue that route because seeking legislation would inevitably compromise the secrecy of the collection program the Government wishes to undertake.”<sup>64</sup> The refusal to brief Congress was all the more problematic given that the government was proposing a statutory interpretation well outside the scope envisioned by Congress.

In 2006, after Congress added the requirement that Section 215 orders be “relevant to” an investigation, the DOJ acknowledged that language was intended to impose new protections. A fact sheet about the new law published by the DOJ stated: “The reauthorizing legislation’s amendments provide significant additional safeguards of Americans’ civil liberties and privacy,” in part by clarifying, “that a section 215 order cannot be issued unless the information sought is relevant to an authorized national security investigation.”<sup>65</sup> Yet just months later, the DOJ convinced the FISC that “relevant to” meant “all” in the first Section 215 bulk dragnet order. In other words, the language inserted by Congress to *limit* the scope of what information could be gathered was used by the government to say that there were *no limits*.

---

<sup>64</sup> John Ashcroft, Jim Comey, James Baker, Jack Goldsmith, Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes, July 2004, at 61, available at <https://www.dni.gov/files/0808/Final%20056.Memorandum%20of%20Law%20and%20Fact%20in%20Support%20of%20Application%20for%20Pen%20Registers%20and%20Trap%20and%20Trace%20Devices%20for%20Foreign%20I~1.pdf>.

<sup>65</sup> Fact Sheet: USA Patriot Act Improvement and Reauthorization Act of 2005, March 2, 2006, available at [https://www.justice.gov/archive/opa/pr/2006/March/06\\_opa\\_113.html](https://www.justice.gov/archive/opa/pr/2006/March/06_opa_113.html).

The refusal to fully brief Congress continued. For example, the DOJ did not provide the Intelligence and Judiciary Committees with some of the pre-July 10, 2008 FISC rulings that contained significant legal conclusions pertaining to FISA until after the next PATRIOT Act reauthorization in 2010.<sup>66</sup>

## **B. Capturing the House Permanent Select Committee on Intelligence**

Sometimes, however, the failure to fully brief Congress has come from within Congress. In February 2011, House Intelligence Chair Mike Rogers did not invite GOP members of Congress to read the 2011 notice — provided by the Obama administration — regarding the phone and Internet dragnets established pursuant to the PATRIOT Act. Approximately 86 freshmen members — 65 of whom subsequently voted to reauthorize the PATRIOT Act, a sufficient number to flip the vote — had no opportunity to read that notice.<sup>67</sup> We discuss structural problems with the House Permanent Select Committee on Intelligence, as well as problems with the rules regarding staff clearances, in a separate report, “Strengthening Congressional Oversight of the Intelligence Community.”<sup>68</sup>

The briefings themselves were unresponsive to concerns raised by members of Congress. During a May 13, 2011, briefing by then-FBI Director Robert Mueller and then-FBI General Counsel Valerie Caproni, an unidentified member of Congress asked why “[Senator] Russ Feingold said that Section 215 authorities have been abused.”<sup>69</sup> In response to that question, clearly designed to elicit a description of the legal and logistical problems with the program, an FBI respondent said, “To the FBI’s knowledge, those authorities have not been abused.”<sup>70</sup> While much of that briefing remains redacted, this suggests the FBI did not brief House Republicans about known violations of FISA relating to the bulk telephone metadata program. As the U.S. Court of Appeals for the Second Circuit noted: “The House Intelligence Committee did not share the papers at all with non-members, leaving the non-committee Representatives in the dark as to the program.”<sup>71</sup>

---

<sup>66</sup> Ronald Weich, Cover Letter for significant decisions to Patrick Leahy et al, August 16, 2010, available at <https://www.dni.gov/files/documents/501/16%20August%202010%20Cover%20Le...cation%20markings%20struck%5D-FINAL.pdf>.

<sup>67</sup> See <https://www.emptywheel.net/2013/08/12/65-2010-house-freshmen-re-authorized-patriot-with-no-notice-of-section-215-dragnet/>.

<sup>68</sup> Available at [https://s3.amazonaws.com/demandprogress/reports/Strengthening\\_Congressional\\_Oversight\\_of\\_the\\_IC\\_White\\_Paper\\_Sept\\_2016.pdf](https://s3.amazonaws.com/demandprogress/reports/Strengthening_Congressional_Oversight_of_the_IC_White_Paper_Sept_2016.pdf).

<sup>69</sup> Congressional Affairs Office report on May 18, 2011 briefing, at 10, available at <http://www.emptywheel.net/wp-content/uploads/2013/08/091019-Records-of-various-215-briefings.pdf>.

<sup>70</sup> *Id.*

<sup>71</sup> See *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), at 79-80, available at <https://www.aclu.org/legal-document/aclu-v-clapper-appeals-court-ruling>.



In 2011, the NSA similarly failed to provide notice to the House Judiciary Committee about its testing of geolocation data collection under Section 215 until after the reauthorization of the PATRIOT Act, in spite of the fact that it had been conducting such tests throughout the 2010 and 2011 debates about the statute.<sup>72</sup>

### C. Misleading Congress

Perhaps the most famously dishonest exchange between the executive branch and Congress occurred shortly before the Snowden revelations. In March 2013, Senator Ron Wyden asked then-Director of National Intelligence James Clapper whether the NSA “collects any type of data at all on millions or hundreds of millions of Americans?” Clapper responded, “No, sir.” After being asked to clarify, he added “Not wittingly.”<sup>73</sup>

Wyden had sent Clapper the question one day in advance, and later asked Clapper if he would correct the public record. Clapper refused.<sup>74</sup> Clapper would later describe this as the “least untruthful answer possible.”<sup>75</sup> The first Snowden revelations, showing that Clapper had publicly lied under oath, would begin less than three months later.

The failure to adequately inform Congress about the bulk dragnet formed a key part of the U.S. Court of Appeals for the Second Circuit’s opinion ruling the program was not authorized by law. As noted, that court found that “Congress cannot reasonably be said to have ratified a program of which many members of Congress – and all members of the public – were not aware.”<sup>76</sup>

Two more recent failures to be candid with Congress should be noted. First, in December 2016, a bipartisan group of House Judiciary Committee members memorialized an understanding with Director Clapper that his office would provide an estimated number of Americans affected by Section 702 surveillance in time for the reauthorization debate the following year.<sup>77</sup> But in the first public hearing on Section 702 reauthorization that

---

<sup>72</sup> See Ethan Bauman letter to House Committee on the Judiciary, “Congressional Notification — NSA Acquisition and Use of Telephony Metadata from Cellular Network Call Detail Records — Information Memorandum,” (September 1, 2011), available at <https://www.dni.gov/files/documents/501/HJC%20SJC%20Mobility%20Records%20CN%201Sept11-Sealed-FINAL.pdf>. Conversely, the NSA informed a Senate Intelligence Committee staffer about it in communications dating to March and April 2011. See Office of the General Counsel (Intelligence Law) of the National Security Agency to the Senate Select Committee on Intelligence (April 1, 2011), available at [https://www.dni.gov/files/documents/501/NSA%20CSLI%20Gottzman%20Response\\_SealedFINAL.pdf](https://www.dni.gov/files/documents/501/NSA%20CSLI%20Gottzman%20Response_SealedFINAL.pdf). Section 215 was reauthorized on May 26, 2011.

<sup>73</sup> The exchange is available at <https://www.youtube.com/watch?v=QwiUVUJmGjs>.

<sup>74</sup> See <https://www.npr.org/sections/thetwo-way/2013/07/02/198118060/clapper-apologizes-for-answer-on-nsas-data-collection>.

<sup>75</sup> See <https://www.foxnews.com/politics/dni-chief-clapper-apologizes-for-erroneous-answer-on-nsa-surveillance>.

<sup>76</sup> See *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), at 79, available at <https://www.aclu.org/legal-document/aclu-v-clapper-appeals-court-ruling>.

<sup>77</sup> Committee on the Judiciary letter to James Clapper, December 16, 2016, available at <https://judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance>.

year, Clapper’s successor, Dan Coats, reneged on that promise, stating that it would take “scores of analysts” to come up with such an estimate.<sup>78</sup>

Second, as one of his last moves as Director of National Intelligence, Dan Coats sent a letter to the Senate intelligence and judiciary committees on August 14, 2019. In calling for the permanent reauthorization of the PATRIOT Act authorities set to expire on December 15, including Section 215, he asserted that the laws “have no history of abuse after more than 18 years.”<sup>79</sup>

---

<sup>78</sup> Senate Intelligence Committee, Open Hearing on FISA Legislation, June 7, 2017, at 00:54:06, available at <https://www.intelligence.senate.gov/hearings/open-hearing-fisa-legislation-0>.

<sup>79</sup> Director of National Intelligence letter to Senators Burr, Graham, Feinstein, and Warner, August 14, 2019, available at <https://int.nyt.com/data/documenthelper/1640-odni-letter-to-congress-about/20bfc7d1223dba027e55/optimized/full.pdf>.



## **VII. CONCLUSION**

Since September 11, 2001, the government has been collecting and surveilling massive amounts of telephone and other records relating to millions of people in the United States who are not suspected of wrongdoing. By unlawfully acquiring these records and disobeying the rules set by the Foreign Intelligence Surveillance Court regarding how the government may analyze, retain, and share them, the executive branch's surveillance has been in nearly continuous violation of the Foreign Intelligence Surveillance Act for 18 years.

The authority cited by the government for this collection has shifted during that time, but today this deeply problematic surveillance is authorized by Section 215 of the PATRIOT Act.

This report is not a comprehensive accounting of every known Section 215 or FISA violation, yet those identified in this report show the serious need for further engagement by Congress.<sup>80</sup> In addition to showing the executive branch's institutional lack of candor with regards to its overseers in Congress and in the courts, we have identified three periods of deeply flawed and unlawful surveillance of telephone records affecting massive numbers of innocent people in the United States. It is up to Congress to determine if there will be a fourth.

For any questions or comments, please contact Sean Vitka at [sean@demandprogress.org](mailto:sean@demandprogress.org) or Jason Pye at [jpye@freedomworks.org](mailto:jpye@freedomworks.org).

---

<sup>80</sup> We identify additional FISA violations with a focus on Section 702 in our 2017 report, "Institutional Lack of Candor," named after a Foreign Intelligence Surveillance Court judge's admonishment of the government, available at [https://s3.amazonaws.com/demandprogress/reports/Institutional\\_Lack\\_of\\_Candor.pdf](https://s3.amazonaws.com/demandprogress/reports/Institutional_Lack_of_Candor.pdf).