BRENNAN CENTER FOR JUSTICE

STATEMENT OF

ELIZABETH GOITEIN
CO-DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

HEARING ON

REAUTHORIZING THE USA FREEDOM ACT OF 2015

NOVEMBER 6, 2019

Introduction

Chairman Graham, Ranking Member Feinstein, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law.[1] The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center's Liberty and National Security Program, which works to advance effective national security policies that respect constitutional values and the rule of law.

Three provisions of the USA PATRIOT Act ("Patriot Act") are scheduled to sunset on December 15, 2019. Primary among these is Section 215, which amended the Foreign Intelligence Surveillance Act ("FISA") to broaden the government's ability to obtain business records in foreign intelligence investigations. These records often pertain to American citizens or others inside the United States, but are generally held by third parties, such as telephone companies or banks. Although it significantly expanded the government's authority, Section 215 retained a critical protection: the government could obtain such records only if the Foreign Intelligence Surveillance Court ("FISA Court") determined that they were relevant to an authorized investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities.

In 2013, Edward Snowden's disclosures revealed that the National Security Agency ("NSA") had been indiscriminately collecting all of the cell phone records held by several large U.S. phone companies, a practice known as "bulk collection." A federal appeals court held that the NSA's program was illegal, and independent reviews concluded that it had been of little to no assistance in the government's counterterrorism efforts. Accordingly, when Section 215 came up for reauthorization in 2015, Congress passed the USA FREEDOM Act with the aim of prohibiting bulk collection. Congress also amended various other surveillance laws to ensure that the government would not simply resume bulk collection under a different authority. Finally, Congress enacted provisions to increase transparency and enhance oversight, in order to ensure that similar abuses would not occur in the future.

Unfortunately, events over the past four years have made clear that the USA FREEDOM Act is not fully serving its intended purposes. The government has failed to comply with some of the law's provisions and has interpreted others narrowly to lessen their impact. While the NSA ended its previous bulk collection program, official statistics strongly suggest that the government is continuing to collect massive amounts of personal information about Americans who are not the targets of any authorized investigation. Multiple FISA Court opinions reveal that the government has failed time and again to adhere to rules designed to protect the privacy of Americans. The government's claims that it is unable to produce certain information, which underlay significant exceptions to USA FREEDOM's reporting requirements, have proven false. And intervening Supreme Court case law has changed the legal landscape in ways that are not reflected in the government's procedures.

---

[1] This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school's institutional views on this topic. More information about the Brennan Center's work can be found at http://www.brennancenter.org.

These developments reveal gaps in the USA FREEDOM Act's protections that Congress should now fill. As discussed further in this testimony, the following reforms should accompany any reauthorization of Section 215 of the Patriot Act:

- End the call detail records program that replaced the NSA's "bulk collection" program
- Narrow "bulky" collection under other authorities
- Prohibit warrantless collection of geolocation and other particularly sensitive records
- Prohibit discriminatory surveillance or surveillance based on First Amendment-protected activities
- Establish meaningful minimization requirements
- Close the backdoor search loophole in Section 702 surveillance
- Strengthen transparency and oversight provisions

Congress should also revisit the two other Patriot Act provisions that are scheduled to expire on December 15: the so-called "lone wolf" and "roving wiretap" provisions. The lone wolf provision should be allowed to sunset, as it is both unnecessary (it has never been used) and unwise (it jettisons a critical limiting principle in the application of FISA surveillance authority). The roving wiretap provision should be amended so that it conforms to the parallel provision for criminal wiretaps.

I. Background: Section 215 and the NSA's Bulk Collection Program[2]

Under pre-Patriot Act law, the FBI could apply for an order from the FISA Court to acquire business records held by transport companies, hotels and motels, car and truck rental agencies, and storage rental facilities. To obtain such an order, the government had to certify that the records were sought for a foreign intelligence or international terrorism investigation being conducted by the FBI. Further, it had to present "specific and articulable facts giving reason to believe" that the subject of the records was a foreign power or agent of a foreign power.[3]

Section 215 of the Patriot Act greatly expanded this authority. It removed the limitation on the types of records the government could obtain, granting authority to obtain "any tangible things." In addition, connection to a foreign power or agent of a foreign power was no longer required. The government need only provide a statement of facts showing that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[4]

---

[2] Much of this section is taken from: Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, Brennan Ctr. for Justice (Mar. 18, 2015), https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court.

[3] Intelligence Authorization Act for Fiscal Year 1999, § 602, Pub. L. No. 105-272, 112 Stat. 2411 (1998) (current version at 50 U.S.C. § 1861).

[4] 50 U.S.C. § 1861(b)(2)(A). In addition, if directed at a U.S. person, the investigation could not be based solely on that person's First Amendment activities. 50 U.S.C. § 1861(a)(1).

Although Section 215 allowed the government to obtain more material with a lesser showing, it at least appeared to preserve the safeguard of prior judicial approval on a case-by-case basis. In 2013, however, Edward Snowden's first and most dramatic disclosure revealed that the FISA Court had issued orders under Section 215 allowing the NSA to collect Americans' telephone records in bulk.[5] The records in question, known as "metadata," included the numbers dialed, the numbers of those who called, and the times and lengths of calls—information that could be used to create a detailed picture of a person's associations and activities.

The FISA Court's decision to allow bulk collection of this data was based on an expansive new interpretation of the concept of "relevance." The Court acknowledged that the vast majority of phone records the NSA was collecting had no relevance to any authorized investigation. However, it noted that "information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain."[6] It also accepted the government's argument that "it is necessary to obtain the bulk collection [sic] of a telephone company's metadata to determine . . . connections between known and unknown international terrorist operatives."[7] It concluded, in short, that because collecting irrelevant data was necessary to identify relevant data, the irrelevant data could thereby be deemed relevant.

The court prohibited the NSA from looking at any of the collected phone records unless those records were pulled using search terms (generally telephone numbers) that met a higher bar. Specifically, the NSA must have a reasonable articulable suspicion, or "RAS," that the search term was associated with an international terrorist organization.[8] The FISA Court, however, disclaimed any role in the RAS determination, leaving that assessment to the NSA. In a series of decisions that were later made public as a result of Snowden's disclosures, the FISA Court recounted numerous and systemic failures by the NSA to adhere to the RAS requirement and other legal limits on accessing and sharing the data.[9] Despite these violations, the Court allowed bulk collection to continue. For a brief time, it required the government to obtain the Court's permission before querying the data, but that restriction remained in place only for a few months.

In 2013, the American public learned about the bulk collection program through Edward Snowden's disclosures. The revelation prompted public outrage and a national conversation about the appropriate limits of surveillance in a democratic society. It also triggered litigation. One federal district court held that the program violated the Fourth Amendment (the decision was reversed on standing grounds, because the plaintiff was unable to show that his own phone

[5] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[6] *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573, at *6 (FISA Ct. Aug. 29, 2013) (unpublished) [hereinafter 2013 FISA Ct. Opinion].
[7] *Id.* at *8.
[8] *Id.* at *1.
[9] *See* Part III.B, *infra*.

records had been collected).[10] In addition, the U.S. Court of Appeals for the Second Circuit held that the program went well beyond what Section 215 authorized. Rejecting the FISA Court's creative interpretation of the "relevance" standard, the three-judge panel wrote:

> The interpretation urged by the government would require a drastic expansion of the term "relevance," not only with respect to § 215, but also as that term is construed for purposes of subpoenas, and of a number of national security-related statutes, to sweep further than those statutes have ever been thought to reach . . . . The interpretation that the government asks us to adopt defies any limiting principle.[11]

The bulk collection program was also ineffective. Although the government initially sought to defend it as a necessary national security tool, that justification could not withstand scrutiny. Two groups were tasked with reviewing the program and were given access to the classified details of its implementation: the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent civil liberties watchdog within the executive branch, and a five-member commission appointed by President Obama, which included a former acting head of the CIA and a former chief counterterrorism adviser on the National Security Council. Both groups found that the program yielded little or no counterterrorism value. The PCLOB wrote in its report:

> Based on the information provided to the Board, we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. In that case, moreover, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.
>
> Even in those instances where telephone records collected under Section 215 offered additional information about the contacts of a known terrorism suspect, in nearly all cases the benefits provided have been minimal — generally limited to corroborating information that was obtained independently by the FBI. And in those few cases where some information not already known to the government was generated through the use of Section 215 records, we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records.[12]

---

[10] *See Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *rev'd on standing grounds*, 800 F.3d 559 (D.C. Cir. 2015).

[11] *ACLU v. Clapper*, 785 F.3d 787, 818 (2d. Cir. 2015).

[12] *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*, Privacy & C.L. Oversight Bd., 146 (2014) [hereinafter *PCLOB Section 215 Report*].

The review group established by President Obama echoed this finding: "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."[13]

II. Congress's Response: The USA FREEDOM Act

By the time Section 215 came up for reauthorization in 2015, it was clear that changes to the law were necessary. Many civil liberties advocates argued that the authority should be permitted to sunset, which would return the business records provision to its more limited, pre-Patriot-Act state. By contrast, a few members of Congress attempted to persuade their colleagues to reauthorize Section 215 without change. Ultimately, in May 2015, Congress passed a law that represented a considered compromise: the USA FREEDOM Act.[14]

The law aimed to end the NSA's bulk collection of Americans' telephone records under Section 215, which it accomplished through the mechanism of "specific selection terms" (discussed below). Recognizing the possibility that the NSA might simply shift its bulk collection activities to other surveillance authorities, Congress also sought to prohibit bulk collection under the laws that authorize pen registers/trap-and-trace devices ("PR/TTs"), which can be used to collect electronic communications metadata, and national security letters ("NSLs"), which can be used to collect telephone, financial, and consumer records. Congress also made several changes designed to enhance transparency and oversight of the government's foreign intelligence surveillance activities.

The USA FREEDOM Act was the most significant surveillance reform legislation in nearly four decades. However, it was also very much a compromise. In order to obtain the support of the administration and lawmakers who were opposed to sweeping changes, the bill's sponsors tempered its reforms in many instances, softening or dropping requirements included in earlier versions of the bill and in drafts of the later versions.[15] Moreover, the primary innovation of the bill—the use of "specific selection terms" to prevent bulk collection—was somewhat experimental, and the definition of "specific selection" term for Section 215 and PR/TTs was left open-ended; it therefore was not clear exactly how it would function in practice. As a result, many civil liberties advocates hailed the law as an important first step, but they warned that it contained weak points and potential loopholes, and that its success or failure depended greatly on what came next.[16]

---

[13] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communication Technologies*, President's Review Grp. on Intelligence & Commc'n Techs., 104 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[14] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23.

[15] Sina Beaghley, *The USA Freedom Act: The Definition of a Compromise*, Hill (May 29, 2015, 7:00 AM), https://thehill.com/blogs/congress-blog/homeland-security/243333-the-usa-freedom-act-the-definition-of-a-compromise.

[16] Elizabeth Goitein, *Who Really Wins from NSA Reform?*, MSNBC (June 5, 2015, 10:52 AM), http://www.msnbc.com/msnbc/freedom-act-who-really-wins-nsa-reform; Rainey Reitman, *The New USA Freedom*

The main features of the law, including the areas where reforms were omitted or watered down, are as follows.

A. Prohibiting Bulk Collection under Section 215, National Security Letters, and Pen Register/Trap-and-Trace Devices

Congress sought to prohibit bulk collection by requiring collection activities under Section 215 to be based on a "specific selection term" ("SST"). A prototypical example of such a term would be a telephone number; instead of requiring a telephone company to turn over all of its phone records, a Section 215 order might require the production of records of calls made or received by a particular number. Section 215, however, authorizes the government to obtain any "tangible thing," not just phone records. Because Congress felt it could not anticipate all of the selection terms that might apply to any tangible thing, it did not attempt to devise a comprehensive list of allowable SSTs. Instead, it provided a general definition, along with an illustrative list of terms that would and would not qualify.[17]

On first glance, most of the examples of permissible SSTs provided in the law appear to be similar to a phone number, in the sense of acting as proxies for an individual person or small number of people. But when statutory definitions are taken into account, many of these examples turn out to be significantly broader in their reach, raising the specter of Section 215 orders that could impact tens, hundreds, or even thousands of individuals. For instance, under FISA's definition, a "person" (one of the qualifying SSTs) can include "any individual . . . or any group, entity, association, corporation, or foreign power."[18] Similarly, under the definition provided in the USA FREEDOM Act, an "address" (also a qualifying SST) can include an Internet protocol (IP) address.[19] While some IP addresses can be associated with individual personal computers, IP addresses can also be associated with networks used by hundreds of people.[20]

Congress sensibly required collection activities under other authorities to be based on SSTs as well, in order to prevent the government from simply resuming bulk collection or starting new bulk collection programs using different laws. However, the definitions of SSTs in these authorities suffer from the same problem. For collection activities using PR/TT devices, the definition of SST matches the definition under Section 215.[21] For NSLs to obtain telephone toll and transactional records, the government may use a term that identifies "a person, entity, or

---

Act: A Step in the Right Direction, but More Must Be Done, Elec. Frontier Foundation (Apr. 30, 2015), https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done; *UPDATED: House Passing USA FREEDOM Act an "Important First Step" Toward Surveillance Reform*, Constitution Project (May 19, 2015), https://constitutionproject.org/documents/house-passing-usa-freedom-act-an-important-first-step-toward-surveillance-reform/.

[17] *See* 50 U.S.C. § 1861(k)(4)(A).

[18] 50 U.S.C. § 1801(m).

[19] *See* 50 U.S.C. § 1861(k)(2).

[20] At one point, the nation of Qatar used a single IP address for the entire country. *See Wikipedia Qatar Ban 'Temporary,'* BBC (Jan. 2, 2007), http://news.bbc.co.uk/2/hi/technology/6224677.stm.

[21] *See* 50 U.S.C. § 1841(4)(A).

account."[22] Financial records may be acquired using terms that identify "a customer, entity, or account,"[23] while credit and consumer records may be required using terms that identify "a consumer or account."[24]

Because of the capacious definitions of "specific selection term," civil liberties advocates were concerned that the law, while prohibiting "bulk" (i.e., indiscriminate) collection, could still allow for extremely "bulky" collection (i.e., collection of large amounts of information not reasonably believed to be relevant). Whether the SST innovation was a success or failure would therefore depend on how it was implemented.

B. Creating a New Call Detail Records Program

Although the USA FREEDOM Act effectively put an end to the NSA's bulk collection of telephone records, it created a new program that enabled collection of such records on a scale somewhere between bulk collection and what Section 215 would otherwise authorize. Under this new program, if the government has "reasonable, articulable suspicion" that an "individual, account, or personal device" is "associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor," and if the other requirements of Section 215 are met, the government can obtain an order from the FISA Court requiring ongoing production, for a period of 180 days, of all of the call detail records ("CDR") of that individual, account, or device *and* all of the CDRs of any phone numbers (or other identifying information) appearing in those records.[25] (This second set of records is commonly referred to by the government as a second "hop.")

The CDR program was controversial on a number of grounds. Needless to say, people whom the government suspects of terrorist activity may be in contact with all kinds of people for all kinds of reasons. It simply does not follow that everyone who is ever called by, or ever calls, a terrorist suspect is a terrorist himself. (Think, for example, of the automotive repairman who calls to let a customer know that his car is ready.) The second "hop" is thus certain to pull in the personal information of a large number of innocent Americans. As discussed below, the law failed to provide sufficiently strong minimization requirements for such records. Moreover, two independent review groups had found that collecting Americans' telephone records in bulk provided negligible counterterrorism value. It was therefore entirely unclear why a scaled-down version of the program was necessary, with or without strong minimization requirements.

C. Imposing Post-Collection Privacy Protections

Recognizing that the second "hop" in the CDR program would inevitably result in the collection of information with no relevance to any authorized investigation, Congress directed the government to adopt minimization procedures that would include a requirement for "the

[22] 18 U.S.C. § 2709(b).
[23] 12 U.S.C. § 3414(a)(2).
[24] 15 U.S.C. § 1681u(a)-(c); 15 U.S.C. § 1681v(a).
[25] 50 U.S.C. § 1861(k)(4)(B); 50 U.S.C. § 1861(b)(2)(C) & (c)(2)(F).

prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information."[26] The law also clarified that the FISA Court could review minimization procedures submitted in connection with Section 215 applications,[27] and could impose "additional, particularized minimization procedures" beyond what the statute specified.[28]

This is a weak protection, at best. The NSA's minimization procedures under Section 702 of FISA similarly require the agency to destroy collected communications upon a determination that they do not include foreign intelligence information. In reviewing Section 702 surveillance, the PCLOB found this requirement to be toothless in practice:

> [T]he NSA's general counsel has stated that "[i]f information is determined to not have foreign intelligence value then it is required to be purged." The NSA's general counsel, however, clarified that it is often "difficult to determine the foreign intelligence value of any particular piece of information." An NSA analyst would need to determine not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need. Thus, in practice, this requirement rarely results in actual purging of data.[29]

There is little reason to expect that the requirement has had any greater teeth when applied to CDRs collected under Section 215.

Moreover, the CDR program is not the only activity authorized by Section 215 that is likely to sweep in the personal information of innocent Americans. As noted above, the definition of "specific selection term" for other types of collection under Section 215 is broad enough to allow "bulky," if not bulk, collection. While Section 215 already required the FBI to adopt minimization procedures,[30] it did not specify any particular measures that these procedures must include, nor did it require the NSA or any other agency to adopt minimization procedures for tangible things acquired under Section 215. The USA FREEDOM Act did nothing to cure these deficiencies.

The government may also acquire communications metadata using PR/TT devices. The statutory provision authorizing PR/TTs use lacked any minimization requirement, and civil liberties advocates pushed to have one included in the USA FREEDOM Act. Instead, Congress required the Attorney General to adopt unspecified "privacy procedures," which should, "to the maximum extent practicable and consistent with the need to protect national security," include procedures "that apply to the collection, retention, and use of information concerning United States persons."[31] This is even weaker than the minimization requirement in Section 215. Not only does it fail to specify any concrete measures the procedures must include; it effectively

---

[26] 50 U.S.C. § 1861(c)(2)(F)(vii).
[27] *See* 50 U.S.C. § 1861(c)(1).
[28] 50 U.S.C. § 1861(g)(3).
[29] *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy & C.L. Oversight Bd., 62 (2014) [hereinafter *PCLOB Section 702 Report*] (internal citations omitted).
[30] *See* 50 U.S.C. § 1861(g).
[31] 50 U.S.C. § 1842(h)(1).

allows the government to opt out of the procedures altogether based on a claim that protecting Americans' privacy would be impracticable or inconsistent with national security.

D. Enhancing Transparency and Oversight

The USA FREEDOM Act contained several provisions intended to enhance transparency and oversight in the operations of foreign intelligence surveillance authorities. Major provisions in this area, as discussed below, included a disclosure requirement for certain FISA Court opinions, enhanced reporting requirements, and a FISA Court amicus provision.

Congress tackled the problem of "secret law" by requiring the Director of National Intelligence ("DNI"), in consultation with the Attorney General, to conduct declassification reviews of "each decision, order, or opinion" issued by the FISA Court "that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion."[32] The Act permitted the government to meet this requirement by issuing redacted versions of court documents; alternatively, if the government deemed it necessary to protect national security, it could release a statement "summarizing the significant construction or interpretation."[33]

The USA FREEDOM Act also contained provisions requiring the DNI to publish certain statistical information online. The clear purpose of these provisions was to provide the public with a sense of how many Americans are subject to, or otherwise caught up in, foreign intelligence surveillance activities, including those nominally targeted at foreigners overseas. Thus, for orders under Section 215, the DNI was required to report not only the number of targets of such orders, but also "the number of unique identifiers used to communicate information collected pursuant to such orders"[34]—a metric that would shed light on the number of non-targets about whom communications records were obtained.

For Section 702 surveillance, the DNI was required to report on the total number of orders issued each year.[35] However, because Section 702 operates as a program rather than as individual orders, that number is not particularly illuminating (it is almost always "one"). Civil liberties advocates pushed unsuccessfully for Congress to require a good faith estimate of the total number of communications collected, broken down by U.S. person status. The government insisted that it was not possible to estimate this number—despite the fact that it apparently reported the total number of Internet transactions collected in 2011 to the FISA Court,[36] and despite the fact that it is required to have mechanisms in place to identify whether the

[32] 50 U.S.C. § 1872(a).
[33] 50 U.S.C. § 1872(c).
[34] 50 U.S.C. § 1873(b)(4)(B).
[35] *See* 50 U.S.C. § 1873(b)(2).
[36] *See* [REDACTED], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) (unpublished).

communicants are inside the United States when conducting "upstream" collection under Section 702 (i.e., the collection of communications as they transit the Internet backbone).[37]

The law also required the DNI to report a good faith estimate of the number of times agencies performed U.S. person queries of databases containing communications content and/or metadata collected under Section 702.[38] However, it exempted the FBI from this reporting requirement.[39] The FBI is by far the most prolific user of U.S. person queries, with the PCLOB reporting that it queries databases containing Section 702 data "whenever [it] opens a new national security investigation or assessment," and "with some frequency" "in the course of criminal investigations and assessments that are unrelated to national security efforts."[40] Nonetheless, the FBI persuaded Congress that distinguishing between U.S. person and non-U.S. person queries would be impracticable.

The USA FREEDOM Act addressed the problem of a lack of adversariality in FISA Court proceedings by requiring the FISA Court to appoint at least five individuals who could serve as "amicus curiae." These individuals must possess expertise "in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise."[41] The Court is required to appoint an amicus in any case that, in the Court's view, "presents a novel or significant interpretation of law," unless the Court issues a finding that such appointment is "not appropriate."[42] Amici have access to any legal precedent the Court deems relevant; access to other classified information is permitted "only if [the amicus] is eligible for access to classified information and to the extent consistent with the national security of the United States."[43] Amici have no right to appeal a decision, although the law allows the FISA Court to certify questions to the Foreign Intelligence Court of Review ("FISCR").[44]

E. Deferring Section 702 Reform

One of the most controversial practices revealed by Snowden's disclosures was "backdoor searches." In brief, the NSA is allowed to collect communications content under Section 702 without a warrant because the "targets" of surveillance, as certified by the government, are foreigners overseas. This surveillance, however, inevitably sweeps in massive amounts of Americans' communications. Section 702 requires the government to "minimize" the retention and use of such "incidentally" collected data. Instead, the NSA shares raw Section 702 data with the FBI, which routinely searches through it looking for Americans' communications to use in ordinary criminal cases and national security cases alike. FBI agents are permitted to read Americans' emails and listen to their phone calls even during the "assessment" phase of an

[37] *See PCLOB Section 702 Report*, *supra* note 29, at 38 ("NSA is required to use other technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.").
[38] *See* 50 U.S.C. § 1873(b)(2)(A) & (B).
[39] *See* 50 U.S.C. § 1873(d)(2)(A).
[40] *PCLOB Section 702 Report*, *supra* note 29, at 59.
[41] 50 U.S.C. § 1803(i)(3)(A).
[42] 50 U.S.C. § 1803(i)(2)(A).
[43] 50 U.S.C. § 1803(i)(6).
[44] *See* 50 U.S.C. § 1803(j).

investigation—i.e., without any factual predicate to suggest criminal activity, let alone probable cause and a warrant.[45]

The first version of the USA FREEDOM Act, introduced by Senator Patrick Leahy in 2013, would have closed the backdoor search loophole, prohibiting warrantless U.S. person queries of Section 702 data.[46] There was strong support in Congress for this approach. Indeed, in 2014 and 2015, the House of Representatives overwhelmingly passed bipartisan amendments to defense appropriations bills that would have required the government to obtain a warrant before searching Section 702 data for Americans' communications (although these measures ultimately did not become law).[47] The provision was dropped from later versions of the USA FREEDOM Act, however, to obtain the administration's support and to smooth passage.

At the end of 2017, Section 702 came up for reauthorization. Once again, there was broad bipartisan support for closing the backdoor search loophole, but the perceived necessity for political compromise ultimately stymied this reform.[48] Instead, Congress required the FBI to obtain a warrant only when conducting U.S. person queries in "predicated" criminal investigations unrelated to national security.[49] Although the law's supporters portrayed this requirement as a middle ground, it was arguably a step backward. The PCLOB's report on Section 702 had made clear that backdoor searches generally occur *before* investigations reach the "predicated" stage,[50] so the law's warrant requirement would apply in exceedingly few cases. In all other cases, the law actually ratified backdoor searches—a practice that would otherwise appear contrary to Section 702's minimization requirements. Congress did require the FBI to keep track of how many U.S. person queries it performed, however.[51]

III. Post-Enactment Developments: "Bulky" Collection and Other Problems

Four years have passed since Congress passed the USA FREEDOM Act. Thanks to the additional transparency required by the law, the public and lawmakers have had some opportunity to see how it has functioned in practice, and how the surveillance authorities that it attempted to reform are operating today.

The result is decidedly mixed. As discussed below, it appears that several of the law's provisions are not having the effect that Congress intended—or, in some instances, are not being implemented at all. In addition, FISA Court opinions have revealed significant instances of non-

---

[45] *See The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties: Hearing on the FISA Amendments Act Before the S. Comm. on the Judiciary*, 115th Cong. (2017) (testimony by Elizabeth Goitein, Co-Dir., Liberty & Nat'l Security Program, Brennan Ctr. for Justice).
[46] *See* Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act, S. 1599, 113th Cong. § 301 (2013).
[47] Press Release, U.S. Congresswoman Zoe Lofgren, House Votes to Restrict Backdoor Government Surveillance Programs (June 11, 2015), https://lofgren.house.gov/media/press-releases/house-votes-restrict-backdoor-government-surveillance-programs.
[48] *See* Elizabeth Goitein, *The USA Liberty Act — aka Don't Let the Constitutional be the Enemy of the Unconstitutional*, Just Security (Nov. 9, 2017), https://www.justsecurity.org/46904/house-judiciary-committee-markup-usa-liberty-act-aka-dont-constitutional-enemy-unconstitutional/.
[49] *See* 50 U.S.C. § 1881a(f)(2)(A).
[50] *See PCLOB Section 702 Report*, *supra* note 29, at 59.
[51] *See* 50 U.S.C. § 1881a(f)(1)(B).

compliance with the rules meant to protect Americans' privacy. Separately, intervening events, including Supreme Court caselaw and factual revelations about the FBI's capabilities, have called into question some of the assumptions that shaped Congress's choices in 2015.

A. Statistics Reveal "Bulky" Collection

The main goal of the USA FREEDOM Act was to prohibit bulk collection under Section 215 and other authorities. As discussed above, certain aspects of Congress's approach—the second "hop" in the CDR program, as well as the potential breadth of "specific selection terms" for other authorities—raised questions regarding how effectively the law would meet this goal.

ODNI's annual statistical reports suggest that the government is continuing to pull in large amounts of information about people who are not themselves the targets of investigation. Under the CDR program, in particular, the government collected *more than a billion records* over the course of three years.[52] What makes this number more shocking is the fact that there were fewer than 50 "targets" of collection each year[53] (defined as "the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector"[54]). The vast majority of the records collected, therefore, ostensibly relate to people other than the targets. This was certainly foreseeable, given the existence of a second "hop." What was less intuitive was the sheer amount of information about presumptively innocent people that would be obtained through this mechanism.

Attempting to mitigate this number, the DNI's reports point out that the number of records collected includes duplicates and can reflect the same unique identifier multiple times.[55] As a threshold matter, this caveat underscores the government's lack of compliance with the law. The USA FREEDOM Act required the DNI to report the number of unique identifiers captured by the CDR program, not the total number of records. The DNI flouted this requirement for three years, claiming that "until May of 2018, the government was not technically able to isolate the number of unique identifiers"[56] in the CDRs—a point that the administration notably failed to raise when it issued a statement in support of the USA FREEDOM Act in 2015.

In any case, the DNI's most recent report includes the number of phone numbers (a type of unique identifier) captured by the CDR program between May and December 2018. That number is 19,372,544.[57] The average American owns 1.4 phones;[58] accordingly, 19 million phone numbers would translate to approximately 14 million people, which would suggest that

---

[52] *Statistical Transparency Report Regarding the Use of National Security Authorities: Calendar Year 2018*, Office of C.L., Privacy, & Transparency, 30 (2019) [hereinafter *ODNI Statistical Transparency Report*].
[53] *See id.* at 28.
[54] *Id.* at 6.
[55] *See id.* at 28-29.
[56] *Id.*
[57] *See id.* at 31.
[58] *See* Jay L. Zagorsky, *Rise and Fall of the Landline: 143 Years of Telephones Becoming More Accessible – and Smart*, Phys.org (Mar. 14, 2019), https://phys.org/news/2019-03-fall-landline-years-accessible-smart.html.

the NSA captured information about five percent of the adult population of the United States[59] in just a seven-month period. Needless to say, there are not 14 million people in this country who at any given time are reasonably suspected of having information about international terrorism or espionage.

The bulkiness of the government's collection is borne out by the statistics for other authorities. For traditional Section 215 orders (i.e., outside the CDR program), the DNI reported 88 targets in 2016, 74 targets in 2017, and 60 targets in 2018.[60] The number of unique identifiers used to communicate the information collected, however, was on an entirely different scale: there were 125,354 such unique identifiers in 2016, 87,834 in 2017, and 214,860 in 2018.[61] Similarly, there were 29 targets of PR/TT orders in 2018, but 132,690 unique identifiers were used to communicate the information collected.[62] Assuming that the "targets" of investigation are not routinely entities encompassing thousands of people, these numbers indicate that the number of non-targets whose information is being collected is orders of magnitude greater than the number of targets.

And these numbers are an undercount. The DNI's reports state that "the government does not have a process for capturing unique identifiers received by [non-electronic] means (i.e., hard copy or portable media)."[63] As an example, it notes that "the FBI could obtain, under [Section 215], a hard-copy of a purchase receipt from a company. That purchase receipt could contain a unique identifier such as a telephone number, which would not be counted."[64] Once again, the government's solution is simply to not report the information that the USA FREEDOM Act requires it to report.

In addition, while the term "unique identifier used to communicate information" would capture phone numbers, e-mail addresses, or other identifiers that commonly appear in communications records, it is not clear that it can capture identifiers in other types of records. For instance, if the government used Section 215 to obtain a passenger manifest for an airline flight, thus obtaining the names of 200 people, it's questionable whether the names would be considered "unique identifiers used to communicate information collected."

B. FISA Court Opinions Reveal Repeated Violations of Privacy Protections

Since the USA FREEDOM Act was passed, a series of FISA Court opinions and other disclosures have revealed disturbing instances of non-compliance with the rules that limit the government's collection and use of sensitive information about Americans. When viewed against the backdrop of similar pre-USA FREEDOM incidents, these episodes make clear that existing law is insufficient to protect Americans' privacy.

---

[59] There are 255,369,678 adults in the United States. *United States Population 2019*, World Population Review, http://worldpopulationreview.com/countries/united-states-population/ (last visited Nov. 4, 2019).
[60] *ODNI Statistical Transparency Report*, *supra* note 52, at 26.
[61] *See id.*
[62] *See id.* at 24.
[63] *Id*. at 24, 26.
[64] *Id*. at 26.

Violations occurring after the USA FREEDOM Act

In November 2015, the FISA Court approved the government's annual application to conduct Section 702 surveillance. In doing so, however, the Court noted several incidents of non-compliance with minimization procedures over the preceding year. Specifically, it recounted FBI violations of protections for attorney-client communications, a "failure of access controls" by the FBI, and the NSA's failure to purge certain improperly collected data.[65] The Court expressed particular displeasure at the government's long delay in reporting the infractions. "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years," the Court wrote, "was the government's failure to convey to the Court explicitly during this time that the NSA was continuing to retain this information . . . ."[66]

In 2016, the FISA Court learned that the NSA had been systematically violating certain rules that had been established in 2012 for segregating, storing, retaining, and accessing communications obtained through Section 702 "upstream" collection. Because those rules were designed to remedy a Fourth Amendment violation occurring since the start of the program, the NSA's non-compliance meant that its upstream collection activities had been operating unconstitutionally for 8 years. Moreover, the government did not report this violation for several months after discovering it, as recounted in an April 2017 opinion of the Court.[67] Once again, the Court was troubled by the delay, which it attributed to an "institutional lack of candor."[68]

In June 2018, the NSA announced that it had noticed "technical irregularities" in records it was obtaining under the Section 215 CDR program, resulting in the collection of records the agency was not legally authorized to collect. Because it could not readily identify which records were properly obtained and which were not, the NSA was deleting all of the records obtained for the past three years—i.e., since the inception of the program. The NSA stated that "the root cause of the problem has since been addressed for future CDR acquisitions,"[69] but documents obtained through Freedom of Information Act requests showed that problems were continuing as of October 2018.[70] In March 2019, the *New York Times* reported that the NSA had secretly shuttered the CDR program,[71] and the DNI confirmed this in an August 2019 letter to the congressional intelligence and judiciary committees.[72]

---

[65] *See* [REDACTED], No. [REDACTED] (FISA Ct. Nov. 6, 2015) (unpublished), https://www.intelligence.gov/assets/documents/702%20Documents/oversight/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[66] *Id.* at 58.

[67] *See* [REDACTED], No. [REDACTED] (FISA Ct. Apr. 27, 2017) (unpublished) [hereinafter *April 2017 FISA Ct. Opinion*], https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[68] *Id.* at 19 (internal quotation marks and citation omitted).

[69] Press Release, NSA, NSA Reports Data Deletion (June 28, 2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

[70] *See* Dustin Volz, *NSA Improperly Collected U.S. Phone Records a Second Time*, Wall St. J. (June 26, 2019, 5:32 AM), https://www.wsj.com/articles/nsa-improperly-collected-u-s-phone-records-a-second-time-11561541520.

[71] Charlie Savage, *Trump Administration Asks Congress to Reauthorize N.S.A.'s Deactivated Call Records Program*, N.Y. Times (Aug. 15, 2019), https://www.nytimes.com/2019/08/15/us/politics/trump-nsa-call-records-program.html.

[72] *See* Letter from Daniel R. Coats, Dir. of Nat'l Intelligence, to Richard Burr, Chairman, S. Select Comm. on Intelligence; Mark Warner, Vice Chairman, S. Select Comm. on Intelligence; Lindsey O. Graham, Chairman, S.

Finally, the government last month released a series of FISA Court opinions, including an October 2018 opinion concluding that the FBI's procedures for accessing Americans' communications that are "incidentally" collected under Section 702 of FISA violated both the statute and the Fourth Amendment. In particular, the FBI had conducted "a large number" of queries that did not meet the basic threshold for accessing Section 702 data because they "were not reasonably likely to return foreign-intelligence information or evidence of a crime."[73] These included multiple one-off incidents of FBI personnel running U.S. person queries accidentally or for improper personal purposes.[74] They also included several incidents indicative of more systemic problems. For instance, in March 2017, the FBI, against the advice of the FBI's Office of General Counsel, conducted queries using 70,000 identifiers "associated with" people who had access to FBI facilities and systems. In addition, on a single day in December 2017, the FBI conducted over 6,800 U.S. person queries using Social Security Numbers.[75]

These latter queries were based on the government's theory that "an aggregation of individual queries"—also referred to as a "batch query"—"can satisfy the querying standard, even if each individual query in isolation would not be reasonably likely to return foreign-intelligence information or evidence of a crime."[76] This argument is alarmingly similar to the one used to justify the NSA's bulk collection of telephone records under Section 215. Although the Court observed that the government's approach was in tension with the FBI's internal procedures, it subsequently approved the FBI's revised procedures, which notably do not prohibit batch queries.[77] Indeed, in conversations with civil liberties advocates, government officials have indicated that batch queries are still permitted.

The opinions released last month also revealed that the FBI was not keeping track of how many U.S. person queries it performed, as Congress had expressly required when it reauthorized Section 702 in January 2018. At the same time, the opinions provided a window into how often these searches occur: the Court noted that 3.1 million queries were run on one FBI system alone, and that a significant portion of these were likely to be U.S. person queries, given that the FBI is a domestic law enforcement agency.[78] The Court ordered the FBI to begin tracking U.S. person queries, and the FBI incorporated this requirement into its procedures.

Comm. on the Judiciary; and Dianne Feinstein, Ranking Member, S. Comm. on the Judiciary (Aug. 14, 2015), https://int.nyt.com/data/documenthelper/1640-odni-letter-to-congress-about/20bfc7d1223dba027e55/optimized/full.pdf#page=1.

[73] [REDACTED], No. [REDACTED], 68 (FISA Ct. Oct. 18, 2018) (unpublished) [hereinafter *Oct. 2018 FISA Ct. Opinion*], https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.

[74] *See id.* at 71.

[75] *See id.* at 69.

[76] *Id.* at 78.

[77] *See* [REDACTED], No. [REDACTED] (FISA Ct. Sept. 4, 2019) (unpublished), https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf.

[78] *Oct. 2018 FISA Ct. Opinion*, *supra* note 73, at 66.

Previous violations

The instances of non-compliance described above must be considered in a broader context. Put simply, the government has a long history of failing to comply with legal limits on collecting, accessing, and sharing information about U.S. persons. Most of these incidents reflect unintentional violations, and in each case, the government has attempted to explain away the infraction (although in some cases, the explanation merely underscores the problem—such as the government's statement that improper FBI queries of Section 702 data resulted from "fundamental misunderstandings by some FBI personnel [about] what the standard 'reasonably likely to return foreign intelligence information' means"[79]). Regardless, the result is a staggering accumulation of non-compliance incidents; Section 702 violations alone are numerous enough to fill a single-spaced 63-page chart.[80] Looking at this history, it is impossible to escape the conclusion that the government is simply incapable of maintaining consistent compliance with the rules designed to safeguard Americans' rights in a surveillance system that is collecting billions of their records and communications.

As noted above, the FISA Court issued a series of opinions in 2009 concluding that the NSA had been querying phone records obtained in bulk without meeting the necessary "reasonable articulable suspicion" standard. The following excerpts from a March 2, 2009 decision capture the level of the NSA's noncompliance, along with the Court's frustration (although the Court nonetheless allowed the program to continue):

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[81]
- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[82]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[83]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[84]

---

[79] *Id.* at 69.
[80] *Section 702 Compliance Violation Chart*, Open Tech. Inst. (Sept. 27, 2017), https://na-production.s3.amazonaws.com/documents/Categorized_Compliance_Violation_Document_9.27.17.pdf.
[81] *In re* Production of Tangible Things from [REDACTED], No. BR 08-13, 2009 WL 9150913, at *5 (FISA Ct. Mar. 2, 2009) (unpublished).
[82] *Id.* at *3.
[83] *Id.* at *5.
[84] *Id.* at *7.

The government fared no better in its operation of a program to collect Americans' Internet metadata in bulk using PR/TT devices—a program that was first approved by the FISA Court in 2004 and ultimately terminated by the government in 2011. In an opinion issued several years into the program's operation, the FISA Court wrote that the NSA had "exceeded the scope of authorized collection continuously" since the program's initial approval, and that "virtually every" record collected "included some data that had not been authorized for collection."[85] Once again, the Court's comments reveal how problematic—and systemic—the violations were:

- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[86]
- "As far as can be ascertained, the requirement [to determine, prior to sharing U.S. person information with other agencies, that it related to counterterrorism information and was necessary to understand the counterterrorism information or assess its importance] was simply ignored."[87]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[88]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[89]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[90]
- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition . . . presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[91]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained. . . . The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor."[92]

---

[85] [REDACTED], No. PR/TT [REDACTED], at 2, 21, 22 (FISA Ct. [REDACTED]) (unpublished), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[86] *Id*. at 4.
[87] *Id*. at 19.
[88] *Id*. at 20.
[89] *Id*. at 21.
[90] *Id*. at 22.
[91] *Id*. at 77.
[92] *Id*. at 95.

- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[93]

Despite its deep concerns, the Court once again approved the program. Shortly thereafter, the government ended it.

In 2011, the FISA Court discovered serious problems with yet another program: Section 702. Specifically, the Court learned that the government had misrepresented its activities under the program, and that its method of collecting Internet transactions off the Internet backbone resulted in the acquisition of tens of thousands of purely domestic communications (despite the law's requirement that the government target only foreigners overseas). The Court held that the government's failure to properly handle these communications violated the Fourth Amendment. It noted: "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[94] To fix the Fourth Amendment violation, the Court required the government to adopt certain procedures for segregating, storing, retaining, and accessing communications obtained through "upstream" collection. Four years later, as discussed above, the FISA Court learned that the NSA had been systematically violating these rules.

In short, it appears that none of the government's "programmatic" collection activities—including the bulk collection of telephone metadata under Section 215, the bulk collection of Internet metadata under PR/TT authority, the collection of communications content under Section 702, and the collection of phone records under the new Section 215 CDR authority—has *ever* operated in full compliance with the laws and rules designed to ensure the protection of Americans' privacy. This is a sobering fact that must inform Congress's choices as it contemplates the reauthorization of Section 215.

C. Transparency and Oversight Provisions Fall Short

Without the USA FREEDOM Act, it is doubtful that the American public would have learned about the compliance problems that have occurred since then or the deficiencies in the government's procedures that are described above. There is no question that the Act's disclosure requirements, combined with the work of the PCLOB and public pressure for intelligence agencies to be more forthcoming in the wake of Snowden's revelations, have made the government's foreign intelligence surveillance activities more transparent.

Nonetheless, it has become apparent that these transparency provisions are inadequate in some respects. With regard to the requirement to disclose FISA Court opinions, the government has interpreted this requirement to apply only to decisions issued after the law's enactment, although the law itself contains no such limitation. Accordingly, significant opinions issued before June 2015 have been declassified and released slowly and selectively. In a report on secret

[93] *Id.* at 115.
[94] [REDACTED], 2011 WL 10945618, at *5 n.14 (FISA Ct. Oct. 3, 2011) (unpublished).

law published in 2016, the Brennan Center determined that 25-30 such decisions remained classified;[95] although many have since been declassified, others are still not public.[96]

In addition, the lack of a deadline for disclosure of significant FISA Court opinions has proven problematic. The opinions released last month included an opinion from October 2018 concluding that the FBI's procedures violated the law and the Fourth Amendment. The government appealed this decision to the FISCR, and did not release the opinion until after it lost its appeal and developed procedures that the Court approved in September 2019. The timing strongly suggests that the government was delaying release in the hope that it would prevail on appeal, mitigating the impact of disclosure. Nothing in the USA FREEDOM Act, however, suggests that the government's public relations concerns should be allowed to dictate the timing of release.

With regard to reporting requirements, a key statistic omitted from the USA FREEDOM Act was the number of U.S. person queries performed by the FBI. The FBI had represented to Congress that producing an estimate of this number would be prohibitively difficult. In 2018, however, Congress required the FBI to track this number internally. The FBI at first did not comply, but the FISA Court did not accept the Bureau's claims of impracticability. To the contrary, the FISCR concluded that counting U.S. person queries is not "a burdensome substantive requirement," and that it would simply mean "adding one (largely ministerial) item to the checklist that FBI personnel most likely already work through when conducting queries for investigative purposes."[97] The FBI has now agreed to begin tracking these queries.

This incident also calls into question other claims by the government that it cannot report information. In particular, the NSA maintains that it cannot even estimate how many communications it collects under Section 702 that involve at least one U.S. person. This claim has always been dubious. When conducting upstream collection under Section 702, the NSA is required to filter out purely domestic communications.[98] That means it has the capability to determine when the communicants are inside the United States, a fact that can serve as an imperfect but reasonable proxy for U.S. person status. As for collection of phone calls, the government can easily determine the area codes, which also constitute a rough but adequate proxy. Given these facts, and the fact that the FBI is now engaged in a tracking process it previously described as unworkable, the NSA's contention that it is unable to produce an estimate should be viewed as deeply suspect.

Finally, certain weaknesses in the amicus provisions of the USA FREEDOM Act have been revealed. While FISA Court opinions suggest that amici have occasionally presented forceful arguments for strong civil liberties protections, they have at other times taken positions

---

[95] *See* Elizabeth Goitein, *The New Era of Secret Law*, Brennan Ctr. for Justice, 61 (Oct. 18, 2016).
[96] *See Public Filings – U.S. Foreign Intelligence Surveillance Court*, U.S. FISA Ct., https://www.fisc.uscourts.gov/public-filings (last visited Nov. 4, 2019).
[97] *In re* DNI/AG 702(h) Certifications 2018 [REDACTED], No. [REDACTED], at 37 (FISA Ct. Rev. July 12, 2018) (unpublished), https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.
[98] *See PCLOB Section 702 Report*, *supra* note 29, at 38.

that fall far short of what an advocate for the target of surveillance would have argued.[99] This is perhaps unsurprising, as some of the appointed amici have no significant background in civil liberties, and the law does not require them to assume the role of the government's adversary. Moreover, when amici's arguments have been rejected by the Court, there has been no way for amici to secure review by the FISCR, regardless of the novelty of significance of the issue.

It also appears that the FISA Court does not always appoint amici when it should. As of the end of 2018, according to reports required by the USA FREEDOM Act, the FISA Court had appointed amici on 14 occasions.[100] It had exercised its prerogative to determine that appointment of amici was "not appropriate" on five occasions, although on three of those occasions, it ended up appointing amici under a different authority.[101] While this record may seem encouraging, there is at least one known instance in which the Court considered a clearly significant question (i.e., the government's failure to adhere to protections designed to protect the Fourth of Amendment rights of Americans) and neither appointed amici nor issued a writing finding that such appointment was not appropriate.[102] In addition, the Court has interpreted "not appropriate" to include instances in which the Court feels that it can resolve the matter at hand without amici's assistance[103]—an interpretation which substantially undermines the appointment requirement.

D. The Government Has Seemingly Ignored Intervening Case Law

In 2018, the Supreme Court decided the seminal case of *Carpenter v. United States*,[104] in which it held that the warrantless collection of 127 days' worth of cell site location information ("CSLI") violated the Fourth Amendment. The government had argued that, under the "third party" doctrine, a person loses any reasonable expectation of privacy (and therefore any Fourth Amendment protection) in information that she shares with a third party, such as a cell phone service provider. This is the same theory that underlies the government's warrantless collection of a broad range of business records and other information under Section 215 and the provisions authorizing PR/TTs and NSLs.

---

[99] For instance, in a case involving Section 702, amicus argued that the backdoor search loophole should be addressed by strengthening procedural requirements on the agency's access to U.S. person communications, rather than by imposing the much stronger protection of a warrant requirement. *See* Transcript of Proceedings Held Before the Honorable Thomas F. Hogan, *In re* the 2015 FISA Section 702 Certifications [REDACTED], at 8 (FISA Ct. Oct. 20, 2015) (unpublished), https://www.aclu.org/foia-document/transcript-fisc-proceedings-judge-hogan; Brief of Amicus Curiae, *In re* the 2015 FISA Section 702 Certifications [REDACTED], at 11-13 (FISA Ct. Oct. 15, 2015) (unpublished), https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress.

[100] *Director's Report on Foreign Intelligence Surveillance Courts' Activities*, U.S. Cts. (Apr. 25, 2019), https://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts.

[101] Dir., Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2015*, U.S. Cts. (2016), https://www.uscourts.gov/sites/default/files/fisc_annual_report_2015.pdf.

[102] *See April 2017 FISA Ct. Opinion*, *supra* note 67.

[103] *See* Elizabeth Goitein, *The FISC's Newest Opinion: Proof of the Need for an Amicus*, Just Security (June 23, 2015), https://www.justsecurity.org/24134/fiscs-newest-opinion-proof-amicus/.

[104] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

The Court emphatically disagreed with the government's absolutist view of the third-party doctrine. It noted that historical CSLI can provide "an intimate window into a person's life, revealing not only his particular movements, but his familial, political, professional, religious, and sexual associations."[105] Under these circumstances, the Court concluded, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[106]

The Court was careful to limit its holding to the facts of the case before it, noting the dangers of trying to issue broad rulings in the context of rapidly evolving technologies: "As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'"[107] For that reason, the Court stated, "[w]e do not . . . call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security."[108]

While the question of how the principles articulated in *Carpenter* apply in other contexts was not before the Supreme Court, it is squarely before the government. There is little question that the government, before *Carpenter* at least, was using Section 215 to obtain geolocation information without a warrant. It is also likely collecting other types of business records, such as medical records, that include extremely sensitive information, as well as aggregations of documents that together provide "an intimate window into a person's life." Now that the Court has made clear that the third-party doctrine does not always overcome the Fourth Amendment's warrant requirement, it is incumbent upon the government to revisit these practices. Yet as of March 2019, the government had issued no official guidance on how intelligence or law enforcement agencies should apply *Carpenter* to their collection activities,[109] and since that time the government has not responded to congressional requests for information on this point.[110]

IV. Reauthorization of Section 215: An Opportunity to Fill the Gaps in the USA FREEDOM Act

The discussion above demonstrates several ways in which the USA FREEDOM Act has fallen short of its intended goals or is otherwise failing to address current problems. Congress now has the opportunity to fill the gaps in this law, in order to ensure that it adequately protects Americans' privacy while maintaining those surveillance capabilities that have been shown to have value. Congress should make the following changes as a prerequisite to reauthorization of Section 215. (The other expiring Patriot Act provisions are discussed in Part V.)

---

[105] *Id*. at 2217 (internal quotation marks and citation omitted).
[106] *Id*. at 2231.
[107] *Id*. at 2220.
[108] *Id*.
[109] *See Worldwide Threats: Hearing before the S. Select Comm. on Intelligence*, 116th Cong. (2019) (Unclassified Responses of Director of National Intelligence Daniel Coats to Questions for the Record).
[110] *See, e.g.,* Letter from Sen. Ron Wyden to Dir. of Nat'l Intelligence Daniel R. Coats (July 30, 2019), https://int.nyt.com/data/documenthelper/1528-wyden-letter-to-dni-re-215-and/6e12df714de6eb7df542/optimized/full.pdf#page=1.

A. End the Call Detail Records Program

There is no possible justification for reauthorizing the CDR Program. Although this program was meant to replace bulk collection, we now know that it is collecting half a billion records each year. We also know that the NSA has been consistently unable to comply with collection limitations, to the point where it had to end the program. Replacing the ineffective and invasive bulk collection program with "bulk collection lite" was a flawed concept from the beginning, but it is now clear beyond any doubt that the program cannot be operated in a manner that is consistent with Americans' privacy rights.

Moreover, the very fact that the NSA was willing to stop collection and purge all the records confirms that the CDR program was providing little value. Although the administration is now asking Congress to reauthorize the program permanently, it appears that the NSA itself took a very different view. In late April, sources told the *Wall Street Journal* that the NSA had recommended that the White House not seek renewal of the program, on the ground that "the logistical and legal burdens of keeping it outweigh its intelligence benefits."[111] A former senior intelligence official described it this way: "The candle is not worth the flame."[112] The Director of the NSA carefully dodged the issue in his public comments, stating that "the administration will make the decision," but hinted at his own view: "I think the question becomes, is this a tool that we continue to need to have for our nation's security?"[113]

Congress should end this failed experiment once and for all, and remove the CDR program authority from any legislation that reauthorizes Section 215.

B. Narrow "Bulky" Collection Under Other Authorities

The DNI's annual statistical reports suggest that the "specific selection term" mechanism is failing to limit collection as Congress had anticipated, and is still allowing the collection of a large amount of information about people who are not the targets of any authorized investigation. This is, admittedly, one of the most difficult problems Congress faces as it considers reauthorization of Section 215, but it is also one of the most critical to solve.

For Section 215, one way to address this problem is to restore the requirement that the target of collection must be a foreign power or agent of a foreign power. The term "foreign power" is defined extremely broadly in the statute. It encompasses not only foreign governments, but also factions of foreign nations or governments, entities directed or controlled by foreign governments, foreign political organizations, and groups engaged in international terrorism or the international proliferation of weapons of mass destruction.[114] Americans may be deemed agents of a foreign power if they engage in various illegal activities on behalf of a foreign power or if they aid or abet those activities.[115]

---

[111] Dustin Volz & Warren P. Strobel, *NSA Recommends Dropping Phone Surveillance Program*, Wall St. J. (Apr. 24, 2019, 5:31 PM), https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.
[112] *Id.*
[113] *Id.*
[114] *See* 50 U.S.C. § 1801(a).
[115] *See* 50 U.S.C. § 1801(b)(2).

Intelligence officials will no doubt argue that this change would constrain the government's investigative capabilities. It is important to remember, however, that many of the types of information the government can obtain under Section 215 (including phone, Internet, and financial records) would still be available through other authorities, including PR/TTs and NSLs, that would continue to employ the lower "relevance" standard. It makes sense to require a higher standard in the case of Section 215 orders due to the extraordinary breadth of what the government can acquire under that authority, which authorizes collection of "any tangible things."

For the PR/TT authority, Congress should revisit the definition of SST. In the context of Section 215, there is some justification for Congress to leave the definition open-ended, as it is difficult to predict all the selection terms that could be associated with "any tangible things." There is no similar justification for an open-ended definition when it comes to communications records. Congress should thus remove the words "or any other specific identifier" from the list of permissible SSTs, which includes terms that specifically identify "a person, account, address, or personal device."

These changes will not necessarily solve the problem of "bulky" collection. In the case of PR/TT and NSL authorities, for instance, the use of capacious SSTs like "person" (defined to include any "entity" of any size) and "address" (defined to include IP addresses that can encompass hundreds of people) could still pull in large amounts of information about innocent Americans. For that reason, it is important to obtain better information about the types of SSTs that are being used, as described in Part IV.G, below. If it turns out that the government is frequently using SSTs that encompass large numbers of people, Congress should take action either to narrow the definition of SST or to implement a more effective approach to limiting collection.

C. Prohibit the Warrantless Collection of Geolocation and Other Particularly Sensitive Records

Congress should prohibit the use of Section 215 or any other authority to engage in the warrantless collection of CSLI. That much is required by the Supreme Court's holding in *Carpenter*. Although the Court did not consider the question of "other collection techniques involving foreign affairs or national security," the central principle that *Carpenter* articulated was that a warrant may be required to obtain records that reveal intimate information about a person's life, even if those records are held by third parties. Like all branches of government, Congress has a duty to uphold the Constitution, and that sometimes requires taking general principles that the Court has articulated and applying them to particular situations that have not yet come before the Court.

Congress should thus bar warrantless collection, through *any* means, of geolocation information pertaining to Americans or others inside the United States. In the past, when the Supreme Court has determined that information is sensitive enough to require warrant protection in the "ordinary" criminal context, that protection has been extended to national security and foreign intelligence cases (as long as the target is a U.S. person). For instance, after the Supreme

Court held that a warrant is generally required to obtain communications content,[116] it held that this requirement also applied in domestic national security cases,[117] and Congress imposed a modified warrant requirement (i.e., FISA Title I) for foreign intelligence investigations. Congress should take the same approach here: In national security and foreign intelligence investigations, Americans deserve the protection of a probable-cause warrant when the government seeks to obtain their most sensitive information.

Congress should also recognize that other types of third-party records can be so inherently sensitive that they should not be collected without a warrant under the logic of *Carpenter*. The law currently limits the FBI Director's ability to delegate the authority to seek access to certain types of records under Section 215, based on the sensitivity of those particular records. They include library circulation records, library patron lists, books sales records, book customer lists, firearm sales records, tax return records, educational records, and medical records containing information that would identify a person.[118] Having acknowledged their sensitivity, Congress should require the government to obtain a warrant to obtain these records. In addition, Congress should require a warrant for any records that shed light on Americans' exercise of constitutional rights, such as records of participation in political organizations or events.

For other types of records, Congress should ensure that the government's authority under Section 215 does not exceed the legal authority it would have in a criminal investigation, excluding grand jury subpoena authority. (Grand jury subpoena authority is an inapt comparison because it involves protections that do not exist in foreign intelligence investigations, including the limited function of the grand jury itself and its role as a check on law enforcement powers.[119]) Finally, Congress should specify that the application of *Carpenter*'s principles to any particular type of record or information constitutes a "significant construction or interpretation" of law for purposes of triggering the appointment of amici in FISA Court proceedings.

D. Prohibit Discriminatory Surveillance or Surveillance Based on First Amendment-Protected Activities

An important gap in the legal safeguards for Patriot Act authorities—one that the USA FREEDOM Act did not attempt to fill—is the lack of any explicit anti-discrimination provision, and the failure to provide robust First Amendment protection. Congress should rectify that omission now.

Throughout this country's history, surveillance has frequently been abused to target minority communities and political dissidents.[120] As long as racial, ethnic, religious, and

---

[116] *See Katz v. United States*, 389 U.S. 347 (1967).
[117] *See United States v. U.S. Dist. Court for E. Dist. of Mich. (Keith)*, 407 U.S. 297 (1972).
[118] *See* 50 U.S.C. § 1861(a)(3).
[119] *See* Michael German et al., *National Security Letters: Building Blocks for Investigations or Intrusive Tools?*, ABA J. (Sept. 1, 2012, 11:10 AM), http://www.abajournal.com/magazine/article/national_security_letters_building_blocks_for_investigations_or_intrusive_t.
[120] *See generally* Mike German, *Disrupt, Discredit, and Divide* (2019); Elizabeth Goitein, Faiza Patel, & Frederick A.O. Schwarz, Jr., *Lessons from the History of National Security Surveillance*, *in The Cambridge Handbook of Surveillance Law* (David Gray & Stephen E. Henderson eds., 2017).

ideological biases continue to exist, there will be a need for strong safeguards against discrimination and targeting of unpopular viewpoints in surveillance laws. Yet the Patriot Act contains no express prohibition on discriminatory surveillance. It does prohibit surveillance based "solely" on activities protected by the First Amendment, but this language suggests that the government is free to conduct surveillance based partly or even *mostly* on First Amendment activities. This is not consistent with the Constitution.

Congress should leave no wiggle room for unconstitutional practices. It should prohibit the government from using race, religion, ethnicity, nationality, or any other constitutionally protected characteristic as a consideration in deciding whether to conduct surveillance. This prohibition should extend to using particular selection terms as proxies for any of these characteristics.[121] Congress should also prohibit surveillance that is motivated or predicated to any degree on conduct, expression, or other activity that is protected by the First Amendment. This would still leave the government free to consider threats, incitement to violence, and other forms of expression that do not receive full First Amendment protection.

E. Establish Meaningful Minimization Requirements

Even with the changes suggested in Part IV.A, the incidental collection of innocuous information, including information about people not suspected of any wrongdoing, is inevitable. This is particularly so given that collection is authorized based on standards significantly lower than "probable cause," and given that some of the permissible "specific selection terms" can capture information hundreds or thousands of people. For these reasons, it is critical to have in place strong minimization procedures.

Currently, statutory minimization requirements for Patriot Act authorities range from weak to nonexistent. As noted above, Congress has specified no particular measures that must be included in Section 215 minimization rules, and the "privacy protections" it required for PR/TT collection are essentially optional. There are no minimization requirements *or* post-collection privacy protections for NSLs.

Congress should impose concrete minimization requirements for all of these authorities. Most important, it should require the destruction, within a reasonable period of time, of any records or data that have not been determined by the government to contain foreign intelligence information or evidence of a crime (and should prohibit the dissemination of such records or data in the interim). If the government has made no determination by the age-off deadline, the data should be destroyed. The alternative is effectively a license for the government to keep the data indefinitely, "just in case."

This age-off period should be no more than two or three years. When reviewing the NSA's bulk collection of phone records under Section 215, the PCLOB recommended ending the

[121] *See* Letter from Ronald Newman, Nat'l Pol. Dir., ACLU, & Neema Singh Guliani, Senior Legis. Couns., ACLU to Sen. Jerrold Nadler, Chairman, H. Comm. on the Judiciary, & Sen. Doug Collins, Ranking Member, S. Comm. on the Judiciary, at 5 (Sept. 17, 2019), https://www.aclu.org/letter/aclus-statement-record-house-judiciary-committee-hearing-fisa-oversight.

program; more immediately, however, it recommended lowering the period for retention of records from five years to three years. It based this number on the government's own representations: "Government officials have already said that reducing the retention period from five years to three would preserve the greatest value that the program offers."[122] The review group appointed by President Obama also recommended ending the bulk collection program, but suggested that phone companies might be required to maintain data for longer than the 18 months required by Federal Communications Commission regulations. It concluded, however, that the new retention period should not exceed two years.[123] Both groups, in other words, saw two or three years as the tipping point, past which the downsides of retaining this sensitive data would outweigh the benefits. Congress should heed their assessment and adopt a retention period in this range.

F. Close the Backdoor Search Loophole

The FISA Court opinions that were released in October 2019 underscore the urgent need for Congress to finally close the legal loophole that allows FBI agents to read Americans' texts and e-mails and listen to their telephone calls without obtaining a warrant. These opinions revealed that the FBI runs literally *millions* of queries each year against databases containing Section 702-acquired communications, most of which are likely to be U.S. person queries. They also revealed that the FBI conducts "batch queries," spreading its net as wide as it deems necessary to get a "hit." Perhaps most important, they revealed that the government has once again engaged in numerous violations of the rules limiting access to Americans' communications, to the point where the FISA Court concluded that the government's procedures violated the Fourth Amendment.

It is time to end the insidious practice of warrantless backdoor searches. In analogous circumstances, several courts have ruled that a warrant may be constitutionally required to run searches on data that government agencies already have collected.[124] But even if a warrant is not *constitutionally* required, Congress can and should require one. In light of the repeated failure of the government, over the course of more than a decade, to adhere to the procedural requirements that the Fourth Amendment unquestionably *does* require, it has become clear that nothing short of a warrant requirement will guard against breaches of Americans' constitutional rights.

G. Strengthen Transparency and Oversight Provisions

The transparency and oversight provisions of the USA FREEDOM Act were among its most important reforms. Nonetheless, their effectiveness is undermined by ambiguities, unnecessary exemptions, and the omission of key requirements. Congress should enact the following changes.

---

[122] *PCLOB Section 215 Report*, *supra* note 12, at 170.

[123] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communication Technologies*, President's Review Grp. on Intelligence & Commc'n Techs., 119 n.118 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[124] *See, e.g.*, *United States v. Ganias*, 755 F.3d 125 (2d. Cir. 2014), *rev'd on other grounds*, 824 F.3d 199 (2d. Cir. 2016); *United States v. Hulscher*, No. 4:16-CR-40070-01, 2017 WL 657436 (D.S.D. 2017) (unpublished).

Clarify requirement of prompt disclosure of significant FISA Court opinions. Congress should clarify that the requirement to declassify and release significant FISA Court opinions applies to opinions issued before the USA FREEDOM Act was passed, and should specify a reasonable period of time for the completion of this process. Congress should also clarify that future opinions must be released as soon as a declassification review can be completed. As a backstop, Congress should provide that, if a declassification review cannot be completed within six months, the DNI must issue an interim public statement that discloses the existence of the ruling and as fulsome a summary as the DNI is able to provide at that time.

Remove unnecessary exemptions for FBI reporting. The USA FREEDOM Act exempted the FBI from reporting how many U.S. person queries it conducts, based on the Bureau's representation that counting these queries would be prohibitively difficult. That has proven to be false, and the FBI is now counting these queries on the order of the FISA Court. Congress should require the DNI to include this number in annual statistical reports.

Congress should also require the DNI to include a good faith estimate of how many communications are collected under Section 702 in which at least one of the communicants is a U.S. person. In other contexts, the NSA is able to count communications obtained under Section 702 and to determine whether the communicants are inside the U.S.;[125] there is no reason why it cannot apply these capabilities in the service of providing an estimate to Congress and the American people.

Require public reporting regarding the scope of SSTs and "tangible things." Specific selection terms are an innovation in the USA FREEDOM Act, and it was clear at the time the law was passed that the success or failure of that innovation would depend on implementation. As of now, however, we lack certain important details about that implementation—in particular, the breadth of the SSTs chosen by the government.

The USA FREEDOM Act required the Attorney General to report to the congressional intelligence and judiciary committees "the total number of applications for orders approving requests for the production of tangible things under [Section 215] in which the specific selection term does not specifically identify an individual, account, or personal device."[126] Congress should add a modified version of this requirement, directing the Attorney General to report publicly (1) the number of applications and orders, broken down by Section 215, PR/TTs, and NSLs, in which the SST is likely associated with more than one individual; and (2) how many individuals, in bands of 100, are likely associated with the SSTs in those applications and orders (e.g., "10 orders based on SSTs that are likely associated with 2-100 people; 3 orders based on SSTs that are likely associated with 100-200 people; 1 order based on an SST that is likely associated with 200-300 people," etc.). This will help Congress and the public to assess whether the SSTs employed by the government are sufficiently specific, or whether they are contributing to excessively "bulky" collection.

Relatedly, Congress should require the DNI's annual report to disclose a listing of the specific types of "tangible things" collected. Given the limitless nature of the term, it is

[125] *See* Part II.D, *supra*.
[126] 50 U.S.C. § 1862(c)(1)(C).

impossible for Congress or the public to obtain a true picture of Section 215 collection without this information.

Revise or supplement the requirement to report "unique identifiers." In the USA FREEDOM Act, Congress sought to obtain a sense of how many Americans are impacted by collection activities. Its solution was to require the DNI to report the number of "unique identifiers used to communicate information collected" under Section 215, the CDR program, and PR/TTs. Whether intentionally or not, this language—depending on how the government interprets it—could have the effect of excluding non-communications records from the reporting requirement. This would provide an incomplete impression of Section 215's impact. Congress should either replace or supplement this requirement with a requirement for the government to provide an estimate, based on any type of unique identifier contained in the records, of the number of individuals about whom information was collected under Section 215 orders.

Require the government to provide notification when using Section 215-derived information. By statute, the government must provide notice to individuals when using information derived from Section 702 surveillance in criminal, civil, or administrative proceedings.[127] This requirement, at least in theory,[128] allows the target to challenge the lawfulness of the surveillance. No such statutory notice requirement exists, however, when the government uses information derived from collection activities under Section 215.

The government has argued that notification is unnecessary in the Section 215 context because there are no constitutional interests at stake when the government collects records held by third parties.[129] In the wake of the *Carpenter* decision, that position is untenable. The Court has affirmed that sharing information with third parties does not necessarily eviscerate Fourth Amendment protections. It is up to the courts—not the executive branch—to decide whether those protections apply in any given case. Congress should therefore require the government to provide notice when using evidence derived from Section 215 collection.

In addition, Congress should clarify that evidence is "derived from" Section 215 collection when the evidence would not have been obtained but for the use of Section 215. In applying this standard, the government should not be allowed to evade the notification requirement by claiming that the evidence would inevitably have been discovered through other means. These parameters are necessary to prevent the well-documented practice of "parallel construction," wherein the government avoids disclosing particular surveillance practices by recreating the evidence using other techniques or authorities.[130]

Strengthen FISA Court amicus provisions. There are several steps Congress should take to ensure that the full potential of the USA FREEDOM Act's amicus provisions is realized. First,

---

[127] *See* 50 U.S.C. § 1806(c).
[128] *But see* Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, Just Security (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.
[129] *See* William Ford, *The House Judiciary Committee's FISA Oversight Hearing: An Overview*, Lawfare (Sept. 20, 2019, 9:00 AM), https://www.lawfareblog.com/house-judiciary-committees-fisa-oversight-hearing-overview.
[130] *See generally Dark Side: Secret Origins of Evidence in US Criminal Cases*, Hum. Rts. Watch (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

as written, the law allows the FISA Court to appoint an amicus with no background or expertise in civil liberties, and nothing in the law requires the amicus to make arguments in opposition to the government's position. Such an arrangement does not cure the fundamental problem it was meant to address: the lack of adversariality in the proceedings as a result of the fact that the target of surveillance is not represented.

Congress should require the FISA Court, in every significant case, to appoint at least one amicus with expertise in civil liberties. While that person would not be representing the target of surveillance, Congress should specify that his or her role is to articulate any constitutional or other civil liberties concerns with the government's position. That person should also have full access to the materials before the Court. The law already limits amici to "persons who are determined eligible for access to classified information necessary to participate in matters before the [FISA Court]."[131] There is no legitimate reason to deny access to amici who have been given the necessary clearances.

The definition of significant cases is also too narrow under current law. In addition to appointing amici in cases raising "a novel or significant interpretation of the law," the FISA Court should be required to appoint amici in cases involving applications of new surveillance technologies or novel uses of existing technologies. Amici should also be appointed for any approvals of programmatic collection activities (e.g., the annual certification reviews under Section 702), as the approval of program-wide policies—unlike the approval of individual warrant applications—is not the type of activity courts normally conduct *ex parte*. And Congress should specify certain matters that should be deemed to qualify as "novel or significant interpretations of the law," including discussions of the application of *Carpenter* and discussions of First Amendment or Equal Protection issues.

Finally, Congress should establish a mechanism for appellate review of significant cases in which the government has prevailed. Otherwise, erroneous decisions against the government will be corrected, but erroneous decisions in the government's favor will remain on the books, undermining the integrity and quality of the case law. One way to provide for appellate review is to require the FISA Court judges to certify cases to the FISCR for review if the Court has rejected arguments made by amici.

V. Reauthorization and Reform of Other Patriot Act Provisions

In addition to Section 215, two other Patriot Act authorities—neither of which was addressed in the USA FREEDOM Act—are scheduled to sunset on December 15. These are Section 6001 (the "lone wolf" provision) and Section 206 ("roving wiretaps"). For the reasons set forth below, the Brennan Center believes that the first of these provisions should be allowed to expire, while the second should be amended to more closely match the parallel criminal authority.

[131] 50 U.S.C. § 1803(i)(3)(B).

A. The "Lone Wolf" Provision

The so-called "lone wolf" provision amended FISA's definition of "agent of a foreign power" to include any person other than a U.S. person who "engages in international terrorism or activities in preparation therefore."[132] Prior to this amendment, if the government wanted to obtain a FISA Court order to collect the communications of a non-U.S. person who was located inside the United States, it had to show that the target of surveillance had some connection to a foreign power.[133] As mentioned above, "foreign power" is broadly defined to include (among other entities) foreign political organizations and international terrorist groups.

This provision expands the scope of FISA's intentionally limited surveillance power. FISA was enacted to permit surveillance of foreign powers or their agents, not to facilitate any and all national security investigations against non-U.S. persons. The less stringent procedural protections contained within FISA were justified, in part, by the fact that its scope was limited to satisfy foreign counterintelligence requirements.[134] Once the limiting principle of connection to a foreign power is removed, there is little to constrain potential future expansion of FISA authority and further diminution of the legal rights of non-U.S. persons inside the United States.

In addition to conflicting with FISA's intended purpose, the lone wolf provision is unnecessary. It is commonly understood to have been prompted by the FBI's belief that it did not have sufficient basis for seeking either a criminal or FISA warrant to search Zacharias Moussaoui's laptop computer prior to 9/11, thereby missing an opportunity to discover and derail the plot. It has emerged, however, that the FBI's belief was based on a misunderstanding of the law as it existed in 2001.[135] The FBI likely could have gotten either a criminal or a FISA warrant to search Moussaoui's computer.

The lack of any need for the "lone wolf" provision is underscored by the fact that the provision has never been used during the entire fifteen years it has been in place. Although government officials say the authority might still prove necessary to go after "lone wolves" who are radicalizing online,[136] the government has been focused on the phenomenon of online radicalization for well over a decade.[137] If the "lone wolf" provision hasn't been used even once during this time period, that strongly suggests the government is able to conduct the necessary surveillance using other authorities. The lone wolf provision should therefore be permitted to sunset.

---

[132] 50 U.S.C. § 1801(b)(1)(C).
[133] *See* 50 U.S.C. § 1801(b)(1)(A)-(B) & (D)-(E).
[134] *See* S. Rep. No. 95-694, at 14-16 (1978).
[135] *See The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* 273-76 (2004), http://govinfo.library.unt.edu/911/report/911Report.pdf; Sens. Patrick Leahy, Charles Grassley, & Arlen Specter, *FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, An Interim Report*, at 17 (2003).
[136] Ford, *supra* note 129.
[137] *See, e.g.*, Carol Dyer et al., *Countering Violent Extremism*, FBI L. Enf't Bull., Dec. 2007, at 3, 6.

B. "Roving Wiretaps"

A roving wiretap allows the government, when conducting electronic surveillance under Title I of FISA (including surveillance of U.S. persons), to acquire communications from any device that may be used by the target, rather than identifying a particular device. Proponents of this provision note that advancements in communications technology make roving wiretap capability an important investigative tool. Section 206, however, lacks procedural protections that are necessary to ensure sufficiently narrow targeting and constitutional particularity.

There are two main problems with section 206 (which permits surveillance to focus on the target, rather than on a particular communications device, when "the actions of the target of the application may have the effect of thwarting the identification"[138] of a specific device). First, the provision contains no requirement for the government to know the target is actually using the device before surveillance is initiated. Instead, the government may place under surveillance all devices that the target might use, regardless of whose communications are actually captured. This deficiency exposes the communications of countless innocent people to interception.

The second concern stems from the combination of Section 206 and another provision of FISA stating that an order approving electronic surveillance must specify "the identity, if known, or a description of the specific target."[139] Under this latter provision, surveillance may be authorized without actually identifying a target by name; the statute does not indicate the level of specificity required in describing a target whose identity is unknown. Taken together, these two provisions permit the government to obtain an order authorizing surveillance that fails to identify either the target or the device to be tapped. It is highly doubtful that such orders comply with the Fourth Amendment, under which a warrant must specify with particularity the place to be searched.

There is a simple way to cure Section 206's current deficiencies. Amending the provision so that it resembles more closely the roving wiretaps permitted in the criminal context would not only provide necessary privacy protections, but would do so in a way that is familiar to both law makers and investigators. This could be accomplished through two modifications.

First, in criminal cases, roving wiretaps are subject to what is known as an "ascertainment requirement." Surveillance may be set up in advance on any device that the target may use, but the surveillance cannot actually be activated until the investigators ascertain that the target is using that particular device.[140] A similar requirement can and should be introduced in the FISA context.

Second, any reauthorization of section 206 should unequivocally bar the use of so-called "John Doe roving wiretaps," or wiretaps that specify neither the target nor the device to be tapped. Instead, as in the criminal context, the statute should require specific identification of either the person or the place to be surveilled.[141] This does not necessarily mean that

---

[138] 50 U.S.C. § 1805 (c)(2)(B).
[139] 50 U.S.C. § 1805 (c)(1).
[140] *See* 18 U.S.C. § 2518(11), (12).
[141] *See* 18 U.S.C. § 2511(b)(ii).

investigators must identify a target by name. The statute could preserve its language requiring identification of the target "if known," so long as it requires sufficient other indicia of identity.

Thank you again for this opportunity to testify.