December 9, 2020

"Updates to U.S. Foreign Intelligence Law Since 2016 Testimony"

Appendix 2 to U.S. Senate Commerce Committee Testimony on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows"

Peter Swire[1]

This Appendix supplements written testimony I am submitting to the Senate Committee on Commerce, Science, and Transportation for the December 9, 2020 hearing on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows." This Appendix presents updates on the U.S. legal and regulatory regime for foreign intelligence surveillance that have occurred since testimony I provided to the Irish High Court in 2016 on the same subject (the "2016 Testimony").[2] Taken together, the 2016 Testimony and this Appendix seek to present an integrated set of references that may inform ongoing assessments, under European Union law, of the adequacy of protection of personal data related to U.S. foreign intelligence law.

My 2016 Testimony was submitted in November 2016, several months after the EU Commission adopted the finalized Privacy Shield in July 2016. At that time, I listed over twenty significant privacy-protective changes that had been made to US foreign intelligence laws since the Snowden disclosures in 2013.[3] My 2016 Testimony then discussed the systemic safeguards present in US law for foreign intelligence, including: (a) safeguards anchored in the statutes governing foreign intelligence surveillance by US agencies,[4] (b) interlocking executive, legislative, and independent oversight mechanisms that are in place for surveillance activities;[5] (c) transparency mechanisms implemented since the Snowden disclosures that offered a level of transparency into US surveillance practices unparalleled in other nations;[6] and (d) privacy safeguards implemented within the executive branch to protect personal information of non-US persons.[7] Chapter 5 of my 2016 Testimony also contained a detailed discussion of declassified opinions of the Foreign Intelligence Surveillance Court (FISC), including my assessment that the FISC has exercised careful and effective oversight over foreign intelligence surveillance.[8]

---

[1] Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Research Director, Cross-Border Data Forum; senior counsel, Alston & Bird LLP. The opinions expressed here are my own, and should not be attributed to the Cross-Border Data Forum or any client. For research assistance on this appendix I thank Daniel Felz and Sara Guercio. This Appendix is based on publicly available information; I have not had access to any relevant classified information since 2016. The views expressed here are my own.

[2] PETER SWIRE, TESTIMONY OF PETER SWIRE (submitted to High Court of Ireland Nov. 3, 2016), *available at* https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony/.

[3] *See id.* at 3-10 – 3-12.

[4] *See id.* at 3-12 – 3-26.

[5] *See id.* at 3-26 – 3-34.

[6] *See id.* at 3-34 – 3-38.

[7] *See id.* at 3-39 – 3-49.

[8] *See id.* at 5-1 – 5-53.

This Appendix highlights updates that have occurred since the 2016 period in which Privacy Shield and my Testimony was finalized. As an overview of what will be discussed in this Appendix, the following represents a summary of intervening developments that have resulted in greater safeguards, or the continued effectiveness of safeguards in place, since the 2016 period in which Privacy Shield and my prior Testimony were finalized:

1. The FISA Amendments Reauthorization Act of 2017 (FARA) introduced new safeguards for Section 702 programs, including:
   (a) mandating querying procedures for 702-acquired information,
   (b) codifying the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) practice of appointing Privacy and Civil Liberties Officers,
   (c) expanding whistleblower protections to Intelligence Community (IC) contractors,
   (d) increasing disclosure and transparency requirements for Section 702 programs, and
   (e) imposing significant restrictions on the recommencement of Abouts collection.

2. The FISC has continued to annually evaluate Section 702 surveillance as required under Section 702, and its reauthorization orders have resulted in new protections for Section 702 programs.

3. As a result of FISC's continued supervision of Abouts collection the NSA (a) voluntarily terminated Abouts collection and (b) segregated and deleted all Internet transactions previously acquired through its Upstream program.

4. The Office of Director of National Intelligence (ODNI) has continued to declassify significant documents relating to Section 702 surveillance, such as publishing the Section 702 trainings that NSA provides to its internal personnel that conduct Section 702 programs on a day-to-day basis.

5. Due in part to compliance incidents reported to the FISC, NSA decided to delete three years' worth of Call Detail Records (CDRs) obtained under the USA FREEDOM Act. NSA then decided to suspend its CDR program in early 2019.

6. The Privacy and Civil Liberties Oversight Board (PCLOB) issued new oversight reports on (a) the NSA's Call Detail Records program under the USA FREEDOM Act, as well as (b) the implementation of Presidential Policy Directive 28 (PPD-28) in US intelligence agencies. PCLOB also recently announced it concluded an oversight review of the US Treasury Department's Terrorist Finance Training Program.[9]

[9] *See generally* U.S. Privacy and Civil Liberties Oversight Bd., *Press Release: Privacy and Civil Liberties Oversight Board Concludes Review of Treasury Department's Terrorist Finance Tracking Program*, (Nov. 19, 2019) *available at* https://documents.pclob.gov/prod/Documents/EventsAndPress/de7972f6-03f1-48fd-8acd-b719a658e4a0/TFTP%20Board%20Statement.pdf. PCLOB Chairman Adam Klein also issued a statement describing EU decisions to rely on TFTP instead of building its own equivalent program, and identifying privacy protective measures in place for EU citizens within TFTP, such as storage of EU bank customer data in the EU. *See* U.S. Privacy and Civil Liberties Oversight Bd., *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*, (Nov. 19, 2020) *available at*: https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

7. The ODNI has continued to publish annual Statistical Transparency Reports showing numerical statistics that provide transparency on the extent to which US agencies are requesting data under FISA authorities, including Section 702 authorities.

8. The Department of Justice (DOJ) and ODNI continue to publish Semiannual Reports on the NSA's, FBI's, and CIA's compliance with Section 702 requirements, including statistics and descriptions of instances of non-compliance. These Reports continue to be created as a result of DOJ/ODNI's regular on-site reviews of the intelligence agencies.

9. US foreign intelligence law continues to permit companies to publish transparency reports. My review of leading technology companies' recent transparency reports shows that, as in 2016, US intelligence appears to affect a vanishingly small percentage of their active users.

10. ODNI has continued to publish significant quantities of declassified documents related to US foreign intelligence activities on the "IC on the Record" website. It also facilitated greater access to these documents by launching a text-searchable capability on Intel.gov.

11. FISC has continued to declassify opinions and publish statistics on its handling of government surveillance applications. The percentage of applications that the FISC has modified or denied has increased since 2016.

This Appendix discussed the above developments in eight Sections that track the structure of my 2016 Testimony: 1) updates to systemic safeguards for US foreign intelligence, 2) updates to Section 702 programs, 3) updates to the former 215 program, 4) updates to oversight safeguards, 5) updates to transparency safeguards, 6) updates to executive safeguards, 7) updates to Foreign Intelligence Surveillance Court (FISC) testimony, 8) updates to surveillance-related standing cases.

1. Updates to Systemic Safeguards for US Foreign Intelligence:

A significant portion of my 2016 Testimony discussed the systemic safeguards built into the structure of foreign intelligence in the United States.[10] The core and structure of these safeguards has remained unchanged since I testified in 2016. The US remains a constitutional democracy committed to the rule of law in conducting foreign-intelligence surveillance.[11] Further, US surveillance remains subject to an interconnected system of statutory safeguards,[12] oversight mechanisms,[13] transparency mechanisms,[14] and executive branch safeguards.[15] My detailed

[10] *See generally* SWIRE, *supra* note 2 at 3-2 – 3-49.

[11] *See id.* at 3-2 – 3-6.

[12] *See id.* 3-12 – 3-26.

[13] *See id.* at 3-26 – 3-34.

[14] *See id.* at 3-34 – 3-38.

[15] *See id.* at 3-39 – 3-49.

discussion of these safeguards can be read in my 2016 Testimony, as outlined in the introduction above.

2. Updates to Section 702 Programs.

Section 702 of FISA is the basis for significant foreign intelligence collection by US intelligence agencies, and was discussed at length in my 2016 Testimony.[16] Since 2016, the legal structure of Section 702 has remained largely unchanged. Section 702 requires the Attorney General and DNI to annually apply to the Foreign Intelligence Surveillance Court (FISC) to authorize Section 702 surveillance programs.[17] In doing so, the FISC reviews and authorizes the targeting, minimization, and (since 2018) querying procedures under which the intelligence agencies conduct Section 702 surveillance.[18] Throughout the ensuing year, the agencies' conduct of Section 702 programs is monitored by internal procedures, external audits, and regular reporting to the FISC and Congress.[19] The primary programs that exist under Section 702 remain (a) the Prism program, in which agencies such as the NSA serve directives on communications providers compelling the disclosure of communications to or from a tasked selector; and (b) the Upstream program, in which Internet backbone providers acquire communications to or from a tasked selector as they traverse the Internet.[20] My 2016 Testimony discusses the structure of Section 702 as well as its primary programs in detail.[21]

Despite broad continuity in Section 702 practice since my 2016 Testimony, a number of significant updates have occurred. This Section briefly summarizes a selection of these changes: (a) the FISA Amendments Act Reauthorization Act of 2017 and its privacy-protective aspects; (b) the FISC continues to reauthorize the Section 702 programs annually; (c) NSA terminated Upstream's Abouts collection in connection with 2017 FISC Reauthorization; (d) statistics on 702 programs continue to be released by the US government; (e) the US government continues to publish the Semiannual Assessment of compliance for 702 programs; and, (f) NSA declassified its internal guidance and training manuals for 702 programs.

a. FISA Amendments Reauthorization Act of 2017 (FARA)

In 2018, the FISA Amendments Reauthorization Act of 2017 (FARA) was passed, reauthorizing FISA for a five-year term and providing additional oversight and privacy protections.[22] Specifically, FARA i) mandated that intelligence agencies adopt querying procedures governing how they may access and use Section 702 intelligence; ii) codified the appointment of Privacy and Civil Liberties Officers in the NSA and FBI; iii) expanded whistleblower protections;

[16] *See id.* at 3-18 – 3-24.

[17] *See id.* at 3-18 – 3-21.

[18] *See id.*

[19] *See generally id.*at 3-2 – 3-49.

[20] *See generally id.*at 3-18 – 3-24.

[21] *See id.*

[22] *See* FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, (2018) [*hereinafter* "FARA"].

iv) increased agency disclosure requirements; and v) required an approval process if the NSA wishes to restart Abouts collections.[23]

i. *Mandatory Querying Procedures*

Before FARA, Section 702 mandated that intelligence agencies adopt "targeting" and "minimization" procedures, which collectively provided the standards by which individuals are targeted for foreign intelligence surveillance and how subsequently acquired communications may be retained and used. FARA added a requirement that the NSA, FBI, CIA, and NCTC adopt "querying" procedures governing how these agencies are permitted to access and search 702-acquired communications.[24] Like targeting and minimization procedures, Section 702 querying procedures must be annually submitted to the FISC for approval, and FISC must evaluate them for consistency with FISA and "the requirements of the Fourth Amendment."[25] While FARA set forth specific requirements for US person queries,[26] the querying procedures adopted by US intelligence agencies contain safeguards for all individuals regardless of nationality. For example, the NSA's 2019 Querying Procedures state that "[e]ach query of NSA systems containing unminimized content or noncontent information acquired pursuant to section 702 … must be reasonably likely to retrieve foreign intelligence information."[27] These requirements, and FISC's annual review of how they are followed by US intelligence agencies, help support proportional use of communications acquired under Section 702.

ii. *Ratification of Appointment of PCLOs within Agencies*

Under its Section 109, FARA expressly required the NSA and FBI to appoint Privacy and Civil Liberties Officers (PCLOs).[28] This change represented more of a change in law than in practice, since both NSA and FBI already had active PCLOs in place as a matter of internal policy before FARA was enacted.[29] Nonetheless, FARA's express codification of NSA's and FBI's prior practice represents Congress's approval of the IC practice of installing oversight and privacy protection offices directly within the agencies that conduct foreign intelligence surveillance.

---

[23] *See generally id.*

[24] *Id.* § 101.

[25] *Id.* § 101(a)(1)(B)(f)(1) (2018).

[26] *Id.* § 109 (2018).

[27] Nat'l Sec. Agency, *Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, 3 (Sept. 16, 2019), *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf.

[28] FARA § 106.

[29] Office of the Dir. of Nat'l Intelligence,, *The FISA Amendments Reauthorization Act of 2017: Enhanced Privacy Safeguards for Personal Data Transfers Under Privacy Shield*, 3 (Oct. 15, 2018) *available at*: https://www.dni.gov/files/documents/icotr/Summary-FISA-Reauthorization-of-2017---10.15.18.pdf [*hereinafter* "DNI FARA Summary"].

iii. *Expansion of Whistleblower Protections*

FARA extended available whistleblower protections to contract employees working within US intelligence agencies.[30] Prior to FARA, "contractors were protected from agency management retaliation," but not from retaliation from the contractor's direct employer.[31] FARA thus extended whistleblower protections to prohibit retaliation against a whistleblowing IC contractor by the contractor's employer.[32] As a result, IC contractors can report deficiencies or violation to the inspectors general of US intelligence agencies and, as permitted by law, to the Senate and House intelligence committees.[33]

iv. *Increased Disclosure Requirements*

FARA introduced a number of new disclosure requirements for intelligence agencies. First, FARA requires future ODNI Statistical Transparency Reports agencies to separately state the number of US persons and non-US persons that were targets of electronic surveillance.[34] Second, FARA formally mandates that agencies' Section 702 minimization procedures be published.[35] Third, FARA requires the Attorney General to provide new reporting to Congress on the number of surveillance applications and emergency authorizations,[36] and to make each report publicly available and unclassified "to the extent consistent with national security."[37]

v. *Requirements for Resuming Abouts Collections*

Abouts collection was an aspect of the NSA's Upstream program. As discussed more fully in Section 2(d) below, following significant interaction with the FISC on the lawfulness of Abouts communication, the NSA voluntarily discontinued Abouts collections in March 2017. FARA now ensures that both the FISC and Congress must be informed before Abouts collection can be revived. If the NSA wishes to resume "intentional acquisition of [A]bouts communication," several requirements must be met.[38] First, FISC must issue a certification approving the program and "a summary of the protections in place to detect any material breach."[39] Second, the NSA must notify Congress in writing 30 days before resuming Abouts collection, and cannot begin Abouts collection within that thirty-day window.[40] The FISC's order approving the recommencement of Abouts

[30] FARA § 110.

[31] DNI FARA Summary, *supra* note 29.

[32] *See id.*

[33] *See* SWIRE, *supra* note 2 at 3-28 – 3-29.

[34] FARA § 102(b).

[35] *Id.* § 104 (2018). Although agencies' minimization procedures have already been declassified and published for each year in which the corresponding Section 702 reauthorization was published, this change may result in minimization procedures being published even when the underlying reauthorization is not.

[36] *Id.* § 107.

[37] *Id.*

[38] *Id.* § 103.

[39] *Id* § 103(b)(3).

[40] *Id.* § 103(b)(2).

collection must be attached to the notice provided to Congress.[41] Third, if Abouts collection resumes after having satisfied the prior two requirements, the NSA must report all material breaches to Congress.[42] Finally, any FISC opinion certifying the recommencement of Section 702 Abouts collection will be designated as a "novel or significant interpretation of the law," thus requiring appointment of an amicus curiae during authorization proceedings, as well as public release of the opinion.[43] The presence of these requirements within the amended Section 702 adds another level of oversight to the NSA's collection of Section 702 data.

b. FISC Continued to Evaluate 702 Compliance During Annual Reauthorizations

As stated above, FISC must annually review and reauthorize Section 702 programs. Since my prior testimony, FISC has reauthorized Section 702 programs on at least three occasions: in April 2017,[44] October 2018,[45] and December 2019.[46] For each of these reauthorizations, the US government declassified and published (a) the FISC order evaluating and reauthorizing Section 702 programs; and (b) the targeting, minimization, and (starting in 2018) querying procedures approved by the FISC to govern the conduct of Section 702 surveillance.[47] For the 2016 reauthorization, the government also declassified the ODNI/Attorney General certification and the NSA Director's affidavit submitted to FISC.[48]

The FISC reauthorization opinions show the FISC conducting the careful and detailed oversight over Section 702 surveillance I discussed in my 2016 Testimony.[49] FISC continued to examine how Section 702 programs "have been and will be implemented" in practice.[50] It also crafted new requirements for compliance with Section 702. As brief examples of FISC's review:

---

[41] *Id.* § 103(b)(3).

[42] *Id.* § 103(b)(5). Material breaches include "significant noncompliance with applicable law or an order of the FISC concerning any acquisition of abouts communication," *see id.* § 103(b)(1)(B). It can be presumed that other compliance incidents, whether material or not, would be reported to the FISC, as this is the FISC's current requirement for Section 702 programs.

[43] *Id.* § 103(b)(6); *see also* USA FREEDOM Act, Pub. L. 114-23, § 602(a) (2017).

[44] *See generally Mem. Op. & Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Apr. 26, 2017) *available at*: https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf [*hereinafter* "FISC 2016/2017 Reauthorization"].

[45] *See generally Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Oct. 18, 2018) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf [*hereinafter* "FISC 2018 Reauthorization"].

[46] *See generally Mem. Op. & Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Dec. 6, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf [*hereinafter* "FISC 2019 Reauthorization"].

[47] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44; FISC 2018 Reauthorization, *supra* note 45; FISC 2019 Reauthorization, *supra* note 46.

[48] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44.

[49] *See generally* SWIRE, *supra* note 2 at 5-1 – 5-53.

[50] *Mem. Op. & Order [Redacted]*, Case Caption [Redacted], 3 (F.I.S.C. Aug. 26, 2014), *available at* https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf; *See also* SWIRE, *supra* note 2 at 5-12 – 5-14.

- The 2016 reauthorization opinion is 99 pages long.[51] The FISC evaluated the NSA's reports of compliance incidents relating to Abouts collection, and the NSA's decision to terminate Abouts collection in response (discussed immediately below). Further, the FISC evaluated the NCTC receiving access to Section 702 information, NSA data deletion questions, and potential issues relating to NSA's Upstream program that had occurred in the past year. The FISC also evaluated the NSA's use of automated tools for tasking decisions; determined that reliance on these tools was not sufficient to task a selector; and required the NSA to begin reporting incidents where the NSA did not conduct post-tasking review of acquired communications to determine whether a tasking decision has been proper.

- The 2018 reauthorization opinion is 138 pages long.[52] In its most lengthy discussion, the FISC found FBI querying practices involving US person identities were inconsistent with the Fourth Amendment; this finding was appealed to the FISA Court of Review, which affirmed the FISC,[53] resulting in the FBI modifying its minimization and querying procedures.[54] Additionally, in a novel and significant decision, the FISC held that FARA restrictions on Abouts collection also applied to certain non-Abouts collection. Although the precise collection technique at issue remained redacted, FISC ordered the NSA to report each time it tasked a selector using this technique within 10 days to FISC, presumably to monitor on an ongoing basis that NSA's acquisitions complied with the restrictions of FARA.[55] For this decision, the FISC invited and received amicus briefing.

- The 2019 reauthorization opinion is 83 pages long.[56] It addressed questions about whether the NSA may share information with FBI for targeting purposes, as well as the retention period for Upstream collection after termination of Abouts collection. Additionally, FISC addressed whether 702-acquired information could be captured by intelligence agencies' "user-activity monitoring" (AUM) activities, such as insider threat protection. The FISC preliminarily

---

[51] *See* FISC 2016/2017 Reauthorization, *supra* note 44; Due to extensions granted to review Abouts collection which extended reauthorization proceedings, the 2016 reauthorization appears to have covered Section 702 surveillance in both the years 2016 and 2017. The Attorney General and ODNI filed certifications to reauthorize Section 702 surveillance on September 26, 2016. *See also Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications [Redacted]*, (F.I.S.C. Sept. 26, 2016) *available at:* https://www.dni.gov/files/documents/icotr/51117/2016_Certification_Cover_Filing_Sep_26_2016_part_1_and_2_-merged.pdf. In evaluating Abouts collection issues, FISC granted extensions into March 2017, at which point NSA announced it was terminating Abouts collection. FISC then issued its reauthorization order on April 26, 2017. This reauthorization thus appears to have authorized Section 702 programs for 2016 and 2017.

[52] *See* FISC 2018 Reauthorization, *supra* note 45.

[53] *See In Re: DNI/AG 702(h) Certifications 2018 [Redacted]*, Dkt. No. [Redacted] (F.I.S.A. Ct. Rev. July 12, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

[54] *See Mem. Op. & Order [Redacted]*, Case No. [Redacted] (F.I.S.C. Sept. 4, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf

[55] *See* FISC 2018 Reauthorization, *supra* note 45 at 136-138.

[56] *See* FISC 2019 Reauthorization, *supra* note 46.

approved AUM activities, but required all agencies to provide further reporting on the extent of their AUM activities and the amount of 702-acquired information affected by it.

c. NSA Terminated Upstream's Abouts Collection in Connection with FISC's 2017 Section 702 Reauthorization

The NSA's termination of Abouts collection represents a significant development that has occurred since my 2016 Testimony and illustrates the effectiveness of the US system of safeguards for foreign intelligence surveillance. Abouts collection referred to an aspect of the NSA's Section 702 Upstream program. It acquired communications that were not to or from a tasked selector, but which instead mentioned the selector (and were thus described as being "about" that selector). An example would be the NSA receiving an email where the selector email address of the target is included in the body or text of the email, but neither sent nor received that email.[57]

Abouts collection first came to FISC's attention in 2011, when it raised concerns due to acquisition of Multi-Communication Transactions (MCTs).[58] Emails and similar communications are often not transmitted through the Internet as discrete communications, but instead as part of MCT clusters,[59] what is often called a "thread" of emails. This resulted in Upstream acquiring not just communications containing a tasked selector, but also a further cluster of attached communications in which the selector did not appear.[60] For Abouts communication, FISC found this raised heightened privacy concerns, since it resulted in the NSA acquiring communications that did not contain selectors.[61] FISC thus imposed a number of restrictions on Abouts collection, such as requiring the NSA to segregate Abouts collection from other 702-acquired data, to restrict other agencies' access to Upstream collection, to restrict NSA analysts' use of Upstream-collected data, and to purge Upstream collection on a more expedited basis than other 702-acquired information.[62] These restrictions were memorialized in NSA's Section 702 minimization beginning in 2011.[63]

It appears that in 2016, NSA's Inspector General reviewed NSA's querying of Upstream collections and identified "significant noncompliance" with the FISC's restrictions.[64] This was reported to FISC, which held a hearing and required the government to submit a report on the full extent of querying practices affecting Upstream data as well as a remediation plan.[65] The government provided several rounds of updates to the FISC; however, the FISC on several occasions

---

[57] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities*, PA-014-18, (Apr. 28, 2017), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/.

[58] *See generally* SWIRE, *supra* note 2 at 5-31 – 5-34.

[59] *See Id.*

[60] *See Id.*

[61] *See Id.*

[62] *See Mem. Op. [Redacted]*, Case No. [Redacted] (F.I.S.C. Oct. 3, 2011) *available at*: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf

[63] *See Mem. Op. [Redacted]*, Case No. [Redacted] (F.I.S.C. Nov. 30, 2011) *available at*: http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf

[64] FISC 2016/2017 Reauthorization, *supra* note 44 at 4.

[65] *See id.*

expressed dissatisfaction with the state of the government's investigation into how querying practices were not complying with existing FISC orders.[66]

Ultimately, on March 30, 2017, the NSA reported to FISC that it would "eliminate 'abouts' collection altogether."[67] In addition, NSA stated it would "sequester and destroy raw Upstream Internet data previously collected," and "destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process."[68] Going forward, NSA stated that any communications obtained by Upstream "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures … will be destroyed upon recognition," and that NSA "will report any acquisition of such communications to [FISC] as an incident of non-compliance."[69] The NSA proffered updated minimization procedures to the FISC that memorialized these changes to Upstream.[70]

The FISC accepted the NSA's updated minimization procedures that prohibited Abouts collection.[71] Further, as described above, FARA now requires the NSA to obtain FISC authorization, and provide notification to Congress, prior to recommencing Abouts communication.[72] The NSA also publicly announced its termination of Abouts collection.[73]

The termination of Abouts communication underscores the effectiveness of the US system of safeguards for foreign intelligence. The FISC recognized privacy risks in Abouts collection and imposed heightened requirements on the NSA. Those requirements could not be met, in part due to technical challenges . Internal reviews identified the noncompliance; and it was reported to FISC. FISC insisted on compliance with its privacy restrictions, and the NSA determined this required Abouts collection to end.

d. Statistics on 702 Programs Continue to be Released by the US Government

ODNI publishes annual Statistical Transparency Reports that identify the number of non-US persons who are the targets of tasked selectors under Section 702.[74] My 2016 Testimony referenced that in 2015, there had been 94,368 targets of Section 702 programs.[75] Since then, the

[66] *See id.* at 4-6.
[67] *Id.* at 6.
[68] *Id.* at 23-24.
[69] *Id.*
[70] *Id.* at 26.
[71] *See id.*
[72] FARA § 103.
[73] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities*, PA-014-18 (Apr. 28, 2017), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/)
[74] *See* 50 U.S.C. § 1873(b)(2)(A); SWIRE, *supra* note 2 at 3-36 – 3-37.
[75] *See* SWIRE, *supra* note 2 at 3-21 – 3-24.

Statistical Transparency Reports have provided targeting statistics for subsequent years.[76] The following table provides statistics for targeting of non-US persons under Section 702 since 2016:[77]

Calendar Year	2016	2017	2018	2019
Estimated Number of Section 702 Targets for Non-US Persons	106,469	129,080	164,770	204,968

I add one comment relevant to current discussions about possible changes in US surveillance practices after *Schrems II*. One proposal I have heard would be to end the Section 702 program and have each selector be subject to the one-at-a-time prior approval by a judge under Title I of FISA, the sort of approval that applies to individuals in the US where there is probable cause that they are "agents of a foreign power."[78] There are currently 11 federal district judges on the FISC; processing over 100,000 individual orders per year would simply not be possible with anything like current staffing with the care and attention to each application that DOJ documents and a judge assesses. As discussed in my 2016 Testimony, Section 702 was created in 2008 as an increase in legal process compared to prior collection done outside of the US.[79] Adding one-at-a-time prior approval by a judge for each selector would thus appear to be a greater change to current practice than some may have realized. That is not a conclusion about what changes the US might contemplate in discussions with the EU, but instead an observation about the nature of the current 702 program.

e. The US Government Continued to Publish Semiannual Assessments of Compliance for 702 Programs

Section 702 requires the AG and ODNI to jointly assess intelligence agencies' compliance with FISA Section 702 and publish their assessment semiannually in a declassified report (the "Semiannual Assessments").[80] The AG (through its National Security Division) and ODNI conduct regular on-site reviews of NSA, FBI, and CIA on at least a bimonthly basis, and they review agencies' targeting and minimization decisions.[81] Using the results of these reviews, the Semiannual

[76] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016* (Apr. 2017) *available at*: https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017* (Apr. 2018) *available at*: https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018*, (Apr. 2019) *available at*: https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019* (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

[77] Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019*, 14 (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf [*hereinafter* "2019 Statistical Transparency Report"].

[78] 50 U.S.C. § 1801(b).

[79] *See* SWIRE, *supra* note 2 at 3-18 – 3-19.

[80] 50 U.S.C. § 1881(a)(l)(1).

[81] *See* SWIRE, *supra* note 2 at 5-20 – 5-23.

Assessments describe types, percentages, and trends of 702 non-compliance issues. The table below summarizes the overall compliance rates, as well as compliance rates for each category of non-compliance, from December 2014 to November 2017. Note that Semiannual Assessments are published on a lag, meaning that although the statistics below date back to 2014, all of the below statistics have been published since the 2016 period in which my prior Testimony and Privacy Shield were finalized.

Intelligence Agencies Compliance Statistics	Report 14 (Dec. 2014 - May 2015)[82]	Report 15 (June 2015 - Nov. 2015)[83]	Report 16 (Dec. 2015 - May 2016)[84]	Report 17 (June 2016 - Nov. 2016)[85]	Report 18 (Dec. 2016 - May 2017)[86]	Report 19 (June 2017 to Nov. 2017)[87]
Overall Non-Compliance Rate	0.35%	0.53%	0.45%	0.88%	0.37%	0.42%
Tasking Non-Compliance Rate	42.3%	58.%	50.8%	35.3%	24.9%	28.7%
Detasking Non-Compliance Rate	24.3%	21.5%	13.7%	5.9%	7.5%	7.3%
Notification Non-Compliance Rate	8.7%	5.2%	6.4%	6.8%	11.2%	22.1%
Documentation Non-Compliance Rate	4.9%	2.2%	12.9%	7.5%	14%	23.6%
Minimization Non-Compliance Rate	14.8%	9.9%	14.3%	42.5%	39.1%	17.3%

[82] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 26-30 (Feb. 2016), available at here: https://www.dni.gov/files/documents/icotr/14th-Joint-Assessment-Feb2016-FINAL-REDACTED.pdf

[83] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 27-31 (Nov. 2016), found here: https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf

[84] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 27-31 (Aug. 2017), found here: https://www.dni.gov/files/icotr/16th_Joint_Assessment_Aug_2017_10.16.18.pdf

[85] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 26-30 (Dec. 2017), found here: https://www.dni.gov/files/icotr/17th_Joint_Assessment_Dec_2017_10.16.18.pdf

[86] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 28-32 (Oct. 2018); found here: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf [*hereinafter* "Semiannual Report 18"].

[87] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 30-36 (Dec. 2019)., found here: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/19th%20Joint%20Assessment%20for%20702%20Dec%202019%20-%20Final%20for%20release%20(002)OCR.pdf [*hereinafter* "Semiannual Report 19"].

Intelligence Agencies Compliance Statistics	Report 14 (Dec. 2014 - May 2015)[82]	Report 15 (June 2015 - Nov. 2015)[83]	Report 16 (Dec. 2015 - May 2016)[84]	Report 17 (June 2016 - Nov. 2016)[85]	Report 18 (Dec. 2016 - May 2017)[86]	Report 19 (June 2017 to Nov. 2017)[87]
Miscellaneous/Other Non-Compliance Rate	4.9%	2.5%	2%	1.9%	0.9%	0.7%
Overcollection Non-Compliance Rate	Not reported	Not reported	Not reported	0.1%	Not reported	0.3%

Overall, AG/ODNI concluded in each Semiannual Assessment that "the agencies have continued to implement [targeting and minimization] procedures and follow [applicable] guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702."[88] Only two incidents of intentional non-compliance were identified in the six Semiannual Assessments that have been published since my 2016 Testimony, each of which was remedied.[89] The Semiannual Assessments enable transparency into the conduct of foreign intelligence surveillance that, to the best of my knowledge, remains unique among leading nations.

f. NSA Declassified its Internal Training Manuals for 702 Programs

Since my 2016 Testimony, NSA has released internal guidance and training documents related to Section 702.[90] The documents show the multi-level training NSA provides to personnel on Section 702 compliance. They include trainings NSA provides to analysts who task selectors to be used in Section 702 surveillance, detailing the process through which NSA analysts must document their rationale for targeting a selector and submit it to an NSA "Adjudicator" for review.[91] The documents also include trainings provided to Adjudicators on reviewing analyst requests to task

[88] This conclusion is from the October 2018 Semiannual Assessment, but is representative of the conclusion of prior Semiannual Assessments. *See, e.g.*, Semiannual Report 18, *supra* note 86 at 48, ("[T]he agencies continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702.").

[89] In Semiannual Report 19, there were two issues of intentional non-compliance. The first issue involved FBI running batch queries under proposed, but unapproved, query procedures. These query procedures were eventually approved, but this incident still counted as intentional non-compliance. The second issue involved traditional intentional non-compliance where an FBI analyst queried his name and the name of his co-worker in the FBI database. This analyst was fired, and his security clearance was terminated. *See* Semiannual Report 19, *supra* note 87.

[90] *See* Office of the Dir. of Nat'l Intelligence, *IC on the Record: IC on the Record Guide to Posted Documents*, ICONTHERECORD.TUMBLR.COM, (Oct. 2020), *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.

[91] *See* Nat'l Sec. Agency, *Updated FAA 702 Targeting Review Guidance [Redacted]*, (May 15, 2017), *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2010.%20NSA%E2%80%99s%20702%20Targeting%20Review%20Guidance.pdf; NSA's Practical Applications Training. *See also* Nat'l Sec. Agency, *CRSK1304: FAA Section 702 Practical Applications [Redacted]*; https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2011.%20NSA%E2%80%99s%20702%20Practical%20Applications%20Training.pdf

specific selectors, and the checklists used in selector evaluations.[92] Finally, NSA published a comprehensive Section 702 training covering aspects of NSA personnel's compliance duties relating to collecting, processing, analysis, retention, and dissemination of 702-acquired information, as well as obligations to immediately report compliance incidents.[93]

As one comment on possible reforms that may address EU legal concerns, the US government might consider codifying training requirements and other aspects of compliance. Such codification might be done through either statutory or non-statutory means, to address European legal concerns that Section 702 and other safeguards be "required by law."

3. Updates to the Former 215 Program.

In my 2016 Testimony, I discussed "[p]erhaps the most dramatic change in US surveillance law" since the Snowden disclosures: The termination of a bulk telephone record collection program that had been operated under Section 215 of the USA PATRIOT Act, and its replacement with a targeted call records program.[94] This change began when President Obama's Review Group, in which I participated, reviewed the 215 program and found it "not essential to preventing attacks."[95] The USA FREEDOM Act was passed soon thereafter, and prohibited bulk collection under Section 215, as well as under pen register, trap-and-trace, and national security letter authorities. NSA terminated the bulk phone records program on November 29, 2015.[96]

The USA FREEDOM Act thus introduced a targeted telephone call detail records program (the "CDR Program") that operated as I described in my 2016 Testimony.[97] The government had to identify a specific selector that is reasonably suspected of being associated with terrorism (such as a phone number), and obtain a FISC order requiring a communications provider to produce records associated with that selector. The government could only obtain records that were no more than two "hops" from the identified selector.

Since my 2016 Testimony, the NSA voluntarily terminated the CDR Program due to compliance and data-integrity issues it did not believe could be resolved. This section briefly describes the significant events relating to the CDR Program: (a) the NSA's deletion of years' worth

---

[92] *See* Nat'l Sec. Agency, *FAA702 Adjudicator Training [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2012.%20NSA%E2%80%99s%20702%20Training%20for%20NSA%20Adjudicators.pdf; Nat'l Sec. Agency, *FAA 702 Adjudication Checklist [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2013.%20NSA%E2%80%99s%20702%20Adjudication%20Checklist.pdf

[93] *See* Nat'l Sec. Agency, *OVSC1203: FISA Amendments Act Section 702 [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2017.%20NSA%E2%80%99s%20Training%20on%20FISA%20Amendments%20Act%20Section%20702.pdf

[94] SWIRE, *supra* note 2 at 3-16 – 3-18.

[95] *See id.*

[96] *See* Office of the Dir. of Nat'l Int., *ODNI Announces Transition to a New Telephone Metadata Program*, (Nov. 27, 2015), *available at*: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2015/item/1292-odni-announces-transition-to-new-telephone-metadata-program.

[97] *See* SWIRE, *supra* note 2 at 3-16 – 3-18.

of CDRs, followed by its decision to terminate the CDR Program, and (b) the PCLOB's ensuring report on the CDR Program. These NSA actions are another example of the oversight and correction mechanisms built into the US legal system governing foreign intelligence.

a. NSA Voluntarily Deleted 3 Years' Worth of USA FREEDOM Act CDRs, then Discontinued the CDR Program Altogether

The CDR Program was affected by a number of compliance issues that resulted in the NSA deciding to delete years' worth of CDR Program data, then to discontinue the program. Between 2016 and 2019, the NSA provided a number of notices to FISC detailing issues of non-compliance and data-integrity issues.[98] Generally, the non-compliance issues included information omitted from FISA applications, providers transmitting CDRs on expired orders, and training and access incidents involving NSA personnel.[99] The data-integrity issues generally involved the NSA receiving erroneous data from certain telecom providers.[100] NSA notified FISC of these incidents, and deleted CDRs associated with these incidents.

In a further incident, when a provider produced inaccurate data, NSA searched for "anomalous data from the other providers," and found data-accuracy issues distributed across providers.[101] Further discussions by the NSA with another provider confirmed it also provided inaccurate data.[102] Ultimately, NSA determined "the providers could not identify for NSA all the affected records, and NSA had no way to independently determine which records contained inaccurate information."[103]

In response, starting on May 23, 2018, the NSA began deleting all CDRs obtained since 2015.[104] As required under FISA, the NSA also notified the PCLOB, Department of Justice (DOJ), and Congressional Oversight committees of its decision.[105] In June 2018, NSA released a statement notifying the public that it had deleted all of its call records under the CDR program due to "technical

---

[98] *See* Privacy and Civil Liberties Oversight Bd., *Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act*, 20 (Feb. 2020), *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/87c7e900-6162-4274-8f3a-d15e3ab9c2e4/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf [*hereinafter* "PCLOB CDR Report"].

[99] *See id.* at 21.

[100] First, a telecom provider pushed "inaccurate first-hop numbers to the NSA," which the NSA's system could not detect. "Instead, [the system] requested second-hop records using the erroneous first-hop response." Subsequently, the provider fixed the issue and the NSA purged the CDRs containing inaccurate numbers. Second, a telecom provider pushed produced a number of CDRs with inaccurate data to the NSA. The NSA took immediate action to stop receipt of CDRs from the provider. The NSA also found there were four FISA applications that relied on the inaccurate information, which it quickly reported to the FISC. The NSA then deleted associated CDRs and "recalled one disseminated intelligence report generated based on inaccurate CDRs." *Id.* at 22.

[101] *Id.* at 23.

[102] *See id.*

[103] *Id.* at 24.

[104] *See* Nat'l Sec. Agency, *NSA Reports Data Deletion*, Release No: PA-010-18, (June 18, 2018), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/

[105] The DOJ subsequently notified FISC. *See id.*

irregularities in some data received from telecommunications service providers" that had resulted in the NSA having access to some CDRs that NSA was not authorized to receive.[106]

Shortly after, in early 2019, the NSA allowed its last FISC order authorizing CDR collection to expire, thus discontinuing the CDR Program under the USA FREEDOM Act.[107] This decision was based on a balancing of "the program's relative intelligence value, associated costs, and compliance and data-integrity concerns."[108] Accordingly, the number of CDRs collected by the NSA fell from over 434 million in 2018 to approximately 4.2 million in 2019.[109]

b. PCLOB Assessed the USA FREEDOM Act CDR Program

In February 2020, the PCLOB issued a report reviewing the CDR program under the USA Freedom Act (the "CDR Program Report").[110] Since the CDR program had been discontinued by the time the PCLOB's Report was issued, the PCLOB made no recommendations regarding the Act, but did issue five key findings. First, the Board found that the CDR program had been constitutional, and second, that the NSA's collection of two hops of CDR data on an ongoing basis was statutorily authorized.[111] Third, PCLOB found no agency abuse of the CDR Program prior to the NSA's decision to stop CDR collection, and, fourth, no evidence that the NSA received statutorily prohibited categories of information such as name, address, or financial information related to a selector. [112] Finally, the Board found the NSA did not use its authority granted under the USA Freedom Act to attempt to gather certain kinds of metadata (the specifics of which remain redacted).[113] More broadly, the PCLOB agreed with the NSA's decision to stop CDR collection.[114]

In March 2020, Congress reauthorized the USA FREEDOM Act, extending it through December 2023.[115] Thus, there is the possibility that NSA could revive the CDR Program in the future. However, to do so, the NSA would have to obtain FISC orders authorizing the collection of CDRs, and the FISC – as it does in other contexts – could impose safeguards on CDR collection based on the past experience of the now-discontinued CDR Program.

---

[106] PCLOB CDR Report, *supra* note 98 at 24.

[107] As a part of the discontinuation, the NSA deleted remaining data collected under the CDR Program, but not data "that had been used in disseminated intelligence reporting or data that was considered 'mission management related information.'" PCLOB CDR Report, *supra* note 98 at 24.

[108] PCLOB CDR Report, *supra* note 98 at 24.

[109] Semiannual Report 19 *supra* note 87 at 32.

[110] *See generally* PCLOB CDR Report, *supra* note 98.

[111] Some of the members of the Board did not join on the constitutional analysis provided in the report. *See id.* at 70-77.

[112] *See* PCLOB CDR Report, *supra* note 98 at 2.

[113] *See id.*

[114] *See* Privacy and Civil Liberties Bd., *Fact Sheet: Report on the NSA's Call Detail Records Program Under the USA Freedom Act*, 2, *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/e37f0efb-c85d-4053-b4c1-4159ccbf100f/CDR%20Fact%20sheet%20FINAL.pdf

[115] *See* USA FREEDOM Reauthorization Act of 2020, H.R. 6172, 116th Congress (May 14, 2020), *available at*: https://www.congress.gov/bill/116th-congress/house-bill/6172/text

4. Updates to Oversight Safeguards.

My 2016 Testimony describes a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency Inspectors General, Privacy and Civil Liberties offices in the agencies, and ongoing review by the independent Privacy and Civil Liberties Oversight Board.[116] The structure of these oversight safeguards remains unchanged since 2016. This section briefly discusses updates occurring within the existing oversight framework: (a) PCLOB issuing its PPD-28 report, and (b) activities by Inspectors General.

a. PCLOB Issued its PPD-28 Report

On October 16, 2018, PCLOB published its report on Presidential Policy Directive 28 (PPD-28) (the "PPD-28 Report").[117] To produce the Report, PCLOB reviewed the PPD-28 targeting procedures of the CIA, NSA, and FBI, reviewed ODNI reports on changes to signals intelligence under PPD-28,[118] took comments from the public and NGOs, and held classified briefings and discussions with IC elements. PCLOB found PPD-28 resulted in greater memorialization and/or formalization of privacy protections that had inhered in existing practices.[119] For example, prior to PPD-28, NSA had limited its uses of signals intelligence collected in bulk to the six permissible purposes listed in PPD-28 (such as espionage and threats to US armed forces); PPD-28 resulted in these limitations being memorialized and codified.[120] Additionally, PPD-28 resulted in extending protections previously reserved for US persons to all individuals regardless of nationality. For example, NSA and CIA used PPD-28 procedures to refocus on protecting "personal information of all individuals regardless of nationality."[121] Similarly, NSA, CIA, and FBI minimization procedures now require that "personal information of non-US persons shall only be retained if comparable information of US persons may be retained pursuant to" EO 12333.[122]

Based on its review, PCLOB issued four recommendations for PPD-28's implementation:

1) The National Security Council (NSC) and ODNI should issue criteria for determining which activities or types of data will be subject to PPD-28 requirements;

---

[116] *See* SWIRE, *supra* note 2 at 3-26 – 3-34.

[117] This report was issued on the basis of Section 5 PPD-28, which encouraged PCLOB to provide a report on any matters within PCLOB's mandate, such as the implementation of executive branch regulations or policies like PPD-28. *See* Privacy and Civil Liberties Bd., *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities*, (Oct. 16, 2018), *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/16f31ea4-3536-43d6-ba51-b19f99c86589/PPD-28%20Report%20(for%20FOIA%20Release).pdf [*hereinafter* "PCLOB PPD-28 Report"].

[118] *See* Office of the Dir. of Nat'l Intelligence, *A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28*, (July 2014), *available at*: https://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf; *See also* Office of the Dir. of Nat'l Intelligence, *2016 Progress Report on Changes to Signals Intelligence Activities* (Jan. 22, 2016), *available at*: https://www.intelligence.gov/index.php/ic-on-the-record-database/results/12-odni-releases-2016-signals-intelligence-reform-progress-report.

[119] *See generally* PCLOB PPD-28 Report, *supra* note 117.

[120] *See id.* at 6.

[121] *Id.* at 6-7.

[122] *Id.* at 7-8.

2) IC elements should consider both the mission and privacy implications of applying PPD-28 to multi-sourced systems;
3) NSC and ODNI should ensure that any IC elements obtaining first-time access to unevaluated signals intelligence update their PPD-28 use, retention and dissemination practices, procedures, and trainings before receiving such data; and
4) To the extent consistent with the protection of classified information, IC elements should promptly update their public PPD-28 procedures to reflect any pertinent future changes in practices and policy.[123]

These recommendations were later reviewed by ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT) in an October 2018 report on the status of implementation of the PCLOB's PPD-28 Report.[124] The CLPT found that the agencies had already implemented all four of these recommendations to the extent possible to maintain national security.[125]

b. Inspectors General

My 2016 Testimony described federal inspectors general (IGs) as an oversight component that provides a well-staffed and significant safeguard to ensure that federal agencies comply with internal administrative privacy mandates, including exercising privacy watchdog responsibilities[126]. Since my 2016 Testimony, as is widely known, the Department of Justice Inspector General issued a report on traditional FISA warrants issued in connection with an FBI investigation into a US citizen associated with the Trump campaign;[127] however, this report was not related to Section 702 or surveillance targeting non-US persons. The IG for the ODNI has continued to issue semiannual reports relating to the IC as a whole.[128] The IGs for surveillance agencies have also issued semiannual reports to Congress,[129] and have published on an ongoing basis reports on various investigations relating to intelligence agency activities.[130]

---

[123] *See id*. at 12-18.

[124] *See* Office of the Dir. of Nat'l Intelligence, *Status of Implementation of PPD-28: Response to the PCLOB's Report*, (Oct. 2018), *available at*: https://www.dni.gov/files/icotr/Status_of_PPD_28_Implementation_Response_to_PCLOB_Report_10_16_18.pdf [*hereinafter* "CLPT PPD-28 Implementation Report"].

[125] *See id*.

[126] *See* SWIRE, *supra* note 2 at 3-26 – 3-28.

[127] *See* Office of the Inspector Gen., *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, US Dept. of Justice, (Dec. 2019), *available at* https://www.justice.gov/storage/120919-examination.pdf

[128] *See* Office of the Dir. of Nat'l Intelligence, *ICIG Semiannual Report*, *available at*: https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports

[129] *See, e.g.* Office of the Inspector Gen., *Semiannual Report to Congress*, National Security Agency, (Oct. 1, 2019 to Mar. 31, 2020), *available at*: https://oig.nsa.gov/Portals/71/Reports/SAR/OCT-MAR%202020%20OIG%20SAR.pdf?ver=2020-09-02-094002-550

[130] For a sample of reports from the NSA's Office of Inspector General, see, e.g., Office of the Inspector Gen. of the Nat'l Sec. Agency, OFFICE OF INSPECTOR GENERAL: REPORTS, *available at*: https://oig.nsa.gov/reports/.

5. Updates to Transparency Safeguards.

My 2016 Testimony discussed how, in the wake of the Snowden disclosures, the US government focused on increasing transparency measures relating to US surveillance, both for companies subject to orders and for government agencies that have requested orders.[131] The transparency safeguards I identified in 2016 have remained in place, and continue to provide valuable information about how foreign intelligence surveillance is conducted by US agencies. This section discusses transparency efforts since 2016: (a) additional releases of Statistical Transparency Reports, (b) continued corporate transparency reporting, (c) the creation of a second, text-searchable IC on the Record database, and (d) continued public release of declassified IC documents.

a. Additional Releases of Statistical Transparency Reports.

As discussed in Section 2(e) above, ODNI produces annual Statistical Transparency Reports that cover the IC's use of multiple types of intelligence.[132] Above, I discussed the numbers of Section 702 targets discussed in Statistical Transparency Reports. I note here that Statistical Transparency Reports go well beyond Section 702 and disclose statistics on the number of governmental requests made under other FISA foreign-intelligence authorities, including traditional individual FISA warrant authorities for electronic surveillance or physical searches, pen-register and trap-and-trace authorities, the "business records" authorities used to obtain Call Detail Records, and national security letter authorities. These reports also disclose the number of criminal proceedings in which a notice was provided that the government intended to use or disclose FISA-acquired information. The Statistical Transparency Report is also unique in that it explains the development of US surveillance programs, limitations placed on programs by FISC, and even instances of the NSA discontinuing programs – such as the 2020 Statistical Transparency Report describing the NSA's decision to suspend the CDR Program.[133]

b. Continued Corporate Transparency Reporting

My 2016 Testimony highlighted corporate transparency reporting as an important transparency safeguard that arose shortly after the Snowden disclosures.[134] Five leading US technology companies (Facebook, Google, LinkedIn, Microsoft, and Yahoo!) filed suit with the FISC to gain rights to provide transparency reporting, resulting in a DOJ policy change permitting

---

[131] *See* SWIRE, *supra* note 2 at 3-34 – 3-38.

[132] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016*, (Apr. 2017) *available at*: https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017*, (Apr. 2018) *available at*: https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018*, (Apr. 2019) *available at*: https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019*, (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

[133] *See* 2019 Statistical Transparency Report, *supra* note 77 at 29 - 30.

[134] *See* SWIRE, *supra* note 2 at 3-37 - 3-39.

reporting on ranges of governmental foreign intelligence requests. The USA FREEDOM Act codified the right of companies to issue transparency reports.

Since my 2016 Testimony, corporate transparency reporting has continued as permitted under the USA Freedom Act, with large companies regularly publishing reports on government access requests.[135] As in my 2016 Testimony, this Appendix examines the most recent transparency reports of Facebook and Google – the percentages of users whose records were accessed in the most recent six-month period is smaller than in 2016. In total, the number of customer accounts accessed by the US government for national security in the most recent time period is no more than (1) 118,997[136] for Facebook, out of approximately 2.5 billion[137] active users per month; and (2) approximately 109,497[138] for Google, out of approximately 1.17 billion[139] active users per month. The charts below, similar to the ones provided in my 2016 Testimony, reflect the current data above.

I make the following observation – these percentages are very, very small. Government surveillance requests are far from "pervasive" or "unlimited," as some have suggested.

Facebook	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0-499	0-499	.0000002%
Content Requests	0-499	117,000-117,499	.000047%
National Security Letters	0-499	500-999	.0000004%

[135] *See id.*

[136] For the time period from July 2019 - December 2019, Facebook received the following: 0-499 non-content requests (affecting the same number of accounts); 0-499 content requests (affecting between 117,000 and 117,499 accounts); and 0-499 national security letters (affecting the same number of accounts). *See* FACEBOOK, *United States Law Enforcement Requests for Data*, GOVERNMENT REQUESTS REPORT (2020), https://govtrequests.facebook.com/country/United%20States/2015-H1.

[137] *See* STATISTA, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019* (2020), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=With%20over%202.7%20billion%20monthly,the%20biggest%20social%20network%20worldwide.

[138] For the time period from January 2019 - June 2019, Google received the following: 0-499 non-content requests (affecting the same number of accounts); 0-499 content requests (affecting between 107,000 and 107,499 accounts); and 500-999 national security letters (affecting between 1000 and 1499 accounts). *See* GOOGLE, *Transparency Report – United States* (2020), https://transparencyreport.google.com/user-data/us-national-security?hl=en.

[139] *See* Craig Smith, *365 Google Search Statistics and Much More (2020)*, EXPANDEDRAMBLINGS.COM (Nov. 30, 2020), http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts.

Google	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0-499	0-499	.0000004%
Content Requests	0-499	107,000-107,499	.00009%
National Security Letters	0-499	1000-1499	.0000012%

c. The Government Has Launched New Transparency Websites

In 2013, the ODNI created "IC on the Record," a website on which ODNI posts declassified documents relating to United States foreign intelligence surveillance practices. In doing so, the US government became the first government in the world to maintain a running repository of declassified documents from its foreign intelligence agencies and oversight organs.[140] Since its appearance in 2013 and my 2016 Testimony, IC on the Record has accumulated a substantial amount of NSA internal records, FISC opinions, and other documents and records relating to foreign intelligence surveillance. The IC states that it has disclosed hundreds of documents comprising thousands of pages, including "hundreds of documents relating to Section 702."[141]

Further, since 2016, the publicly-available online channels through which the public has access to intelligence-related documents and court decisions has increased. For one, the FISC maintains an online "Public Filings" database containing a substantial number of its declassified opinions and orders, which has added usefulness in being searchable by docket number.[142] Second, ODNI has created "Intel.gov," a new repository on an official IC website that creates the capability to conduct full text searches on all documents posted on IC on the Record.[143] These resources make the transparency offered by the US government significantly more actionable for researchers, civil-rights organizations, and civil society in monitoring how foreign intelligence surveillance is being conducted.

6. Updates to Executive Safeguards

a. Presidential Policy Directive 28 (PPD-28)

My 2016 Testimony discussed Presidential Policy Directive 28 (PPD-28) as a significant new safeguard that creates an extensive system of privacy protection for signals intelligence activities involving non-US persons.[144] Since my prior testimony, PPD-28 has remained unchanged in substance. As discussed above, PPD-28 has resulted in intelligence agencies codifying PPD-28

[140] *See* SWIRE, *supra* note 2 at 3-36 - 3-37.

[141] Office of the Dir. of Nat'l Intelligence, *IC on the Record Guide to Posted Documents*, INTEL.GOV, (Oct. 2020), *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.

[142] *See* U.S. Foreign Intelligence Surveillance Ct., *Public Filings – US Foreign Intelligence Surveillance Court*, *available at*: https://www.fisc.uscourts.gov/public-filings. [*hereinafter* "FISC Public Filings Website"].

[143] *See* INTEL.GOV, *IC on the Record Database*, *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents [*hereinafter* "Intel.gov"].

[144] *See* SWIRE, *supra* note 2 at 3-41 - 3-46.

protections into targeting and minimization procedures governing their conduct of signals intelligence. More significantly, PPD-28 remained in place during the transition between the Obama and Trump administrations.[145] The Biden administration is reportedly expected to continue or increase current protections under PPD-28.[146] This demonstrates significant continuity among US presidential administrations to maintain the United States' commitment to PPD-28 and the protections it offers to non-US persons.

b. Privacy Shield

My 2016 Testimony discussed Privacy Shield as a significant safeguard for the protection of data relating to EU citizens, since it introduced commitments from the US government to provide remedies to EU citizens, to act promptly and effectively to address EU data protection concerns, and to subject compliance to an ongoing review process.[147] After the *Schrems II* judgment, Secretary of Commerce Ross stated that the Department of Commerce would "continue to administer the Privacy Shield program," and that the ECJ decision "does not relieve participating organizations of their Privacy Shield obligations."[148] This indicated the US government continues to require Privacy Shield organizations to apply Privacy Shield protections to data received under the Shield until the data is deleted.

7. Updates to Foreign Intelligence Surveillance Court (FISC) Testimony.

Chapter 5 of my 2016 Testimony contained an evaluation of the significant number of FISC opinions that had been declassified following the Snowden disclosures, in a number of cases at the FISC's own order. My assessment reached four primary conclusions:

1. The newly declassified FISC materials support the conclusion that the FISC today provides independent and effective oversight over US government surveillance.
2. The FISC monitors compliance with its orders and has enforced with significant sanctions in cases of noncompliance.
3. In recent years, both the FISC on its own initiative and new legislation have greatly increased transparency.
4. The FISC now receives and will continue to benefit from briefing by parties other than the Department of Justice in important cases.

Since my prior testimony, additional FISC opinions have been published, but I am not aware of any reason to alter these conclusions. This section briefly describes updates that have occurred since 2016 and support the above conclusions: (a) FISC decisions continue to be declassified and

[145] *See* CLPT PPD-28 Implementation Report, *supra* note 124 at 4.

[146] *See* Kristen Bryan et. al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NATIONAL LAW REVIEW, (Nov. 12, 2020), *available at*: https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and

[147] *See* SWIRE, *supra* note 2 at 3-49.

[148] U.S. Dept. of Commerce, *US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-US Data Flows* (July 16, 2020), *available at* https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

published; (b) the FISC and FISA Court of Review have issued further decisions in ACLU litigation discussed in my prior Testimony; and (c) FISC transparency statistics continue to show FISC exercising considerable oversight over government surveillance applications.

a. New and Significant FISC Opinions Continue to be Declassified and Published

The transparency in regard to FISC opinions that I discussed in my 2016 Testimony has continued to the present. Opinions have been published under the USA FREEDOM Act's requirement to publish every FISC "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law" to the greatest practicable extent.[149] Others have been published in connection with litigation pursued by civil-rights organizations.[150] On the whole, a considerable quantity of FISC opinions have been published and can be accessed through IC on the Record,[151] the FISC's own "Public Filings" website,[152] and in text-searchable form on the Intel.gov repository.[153]

b. Updates to ACLU Litigation Discussed in Prior Testimony

My 2016 Testimony discussed litigation brought by the ACLU following the Snowden disclosures in which the ACLU requested that FISC publish its opinions authorizing the bulk telephone records program under Section 215.[154] The FISC found that the ACLU had Article III standing to seek publication of FISC opinions, and ordered the publication of certain Section 215 program authorizations. Since my 2016 Testimony, the FISA Court of Review confirmed that the ACLU and similar public-interest organizations have Article III standing to bring petitions for publication of FISC opinions.[155] However, in a subsequent decision, FISCR held that the FISC does not have subject-matter jurisdiction to hear challenges by public-interest organizations to the withholding of redacted, nonpublic materials in those opinions.[156]

---

[149] 50 U.S.C. § 1872.

[150] *See, e.g.*, IC ON THE RECORD, *Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents* (May 11, 2017), available at: https://icontherecord.tumblr.com/post/160561655023/release-of-the-fisc-opinion-approving-the-2016 (listing "Other FISA Section 702 and Related Documents" produced in response to Freedom of Information Act litigation).

[151] *See* IC ON THE RECORD, *available at*: https://icontherecord.tumblr.com/.

[152] *See* FISC Public Filings Website., *supra* note 142.

[153] *See* Intel.gov, *supra* note 143.

[154] *See* SWIRE, *supra* note 2 at 5-39 – 5-41.

[155] *See In Re: Certification of Questions of Law to the Foreign Intelligence Surveillance Court of Review*, No. 18-01 (F.I.S.C. Mar. 16, 2018), https://www.fisc.uscourts.gov/sites/default/files/FISCR%2018-01%20Opinion%20March%2016%202018.pdf.

[156] *See In Re Op.s & Orders by the FISC Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act*, No. 18-02 (F.I.S.A. Ct. Rev. Mar. 24, 2020), *available at*: https://www.fisc.uscourts.gov/sites/default/files/FISCR%2020%2001%20Opinion%20200424.pdf.

c. FISC Transparency Statistics

My 2016 Testimony assessed a description of the FISC, in the wake of the Snowden disclosures that FISC acted as a "rubber stamp" for government surveillance requests.[157] The FISC itself had disputed this characterization, stating in a letter to the Senate that "24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."[158] The USA FREEDOM Act permitted the Administrative Office of US Courts to issue new statistics on FISC practice that – unlike prior DOJ reporting – did not merely state the number of applications that FISC had denied in full, but rather accounted for all applications that FISC procedures significantly modified, denied in part, or denied in full.[159] This reporting enabled a more complete view of the extent to which FISC subjects government surveillance requests to scrutiny resulting in changes or denial. My 2016 Testimony evaluated the first of these new FISC reports and found that "the FISC either rejected or modified just over 17% of all surveillance applications it received in the latter half of 2015."[160]

Since 2016, the FISC has continued to publish its statistics on the number of applications and certifications for surveillance it modifies or denies.[161] These reports show the FISC modifying or denying a greater percentage of governmental surveillance requests than it did during my prior review. The following table summarizes the FISC statistics for each year since my 2016 Testimony:

Year	Total Number Applications Modified	Total Number of Applications Denied in Part	Total Number of Applications Denied	Sum of Applications Modified, Denied in Part, and Denied	Total Number of Applications and Certifications	Percentage of Applications Modified or Denied by FISC
2017[162]	391	50	26	**467**	**1,614**	**29%**
2018[163]	261	42	30	**333**	**1,318**	**25%**
2019[164]	234	38	20	**292**	**1,010**	**29%**

[157] SWIRE, *supra* note 2 at 5-9 – 5-18.

[158] Letter dated July 29, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the US Senate Judiciary Committee 2, http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf.

[159] *See* SWIRE, *supra* note 2 at 5-43 – 5-48.

[160] *Id.* at 5-14 – 5-17.

[161] *See* U.S. COURTS, *Director's Report on Foreign Intelligence Surveillance Courts' Activities, available at* https://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts.

[162] 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 2017*, 4, (Apr. 25, 2018), *available at* https://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf

[163] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the US Courts on Activities of the Foreign Intelligence Surveillance Courts for 2018*, 4, (Apr. 25, 2019), *available at* https://www.uscourts.gov/sites/default/files/fisc_annual_report_2018_0.pdf.

[164] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the US Courts on Activities of the Foreign Intelligence Surveillance Courts for 2019*, 4, (Apr. 27, 2020), *available at* https://www.uscourts.gov/sites/default/files/fisc_annual_report_2019_0.pdf.

8. Updates to Surveillance-Related Standing Cases

My 2016 Testimony briefly discussed the role that Article III standing may play in attempts to challenge surveillance programs before US courts.[165] This section briefly describes the state of select US cases seeking court review of surveillance programs.

a. Civil Challenges – The two primary attempts to file a civil challenge to Section 702 programs are both actively appealing dismissals on standing grounds.[166] In each case, the plaintiffs were granted discovery to prove they had standing and proffered either documents or experts as evidence. However, both suits were ultimately dismissed on standing ground because plaintiffs could not show a significant probability, or show evidence the government would authenticate, that the plaintiffs' communications had been affected by 702 programs or their predecessors. My understanding is that both proceedings are currently on appeal to a federal circuit court.

b. Challenges in Criminal Cases – In at least two criminal cases, defendants have asserted challenges to the constitutionality and lawfulness of Section 702 programs when 702-obtained evidence was proffered against them.[167] The challenges have been heard and adjudicated, in each instance with Section 702 programs being found lawful. In each instance, the defendant was a US person whose communications had been incidentally collected via 702 programs. In both cases, the lawfulness of incidentally acquiring communications of US persons via Section 702 programs was affirmed on at the appellate level.[168] In one case, following this appellate finding, the case was remanded to the district court to evaluate whether any querying of databases containing such incidentally-acquired Section 702 information by the government was constitutional.[169]

[165] *See* SWIRE, *supra* note 2 at 5-9 – 5-10. .

[166] *See Jewel v. NSA*, No. C 08-04373, 2019 U.S. Dist. LEXIS 217140 (N.D. Cal. 2019); *Wikimedia Found. v. NSA/Central Sec. Serv.*, 427 F. Supp. 3d 582 (D. Md. 2019).

[167] *See U.S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).

[168] *See U.S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).

[169] *See .S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018) (finding that incidental acquisition of US person communications through Section 702 is lawful, but remanding to district court to determine if querying of databases containing 702-acquired information by the government occurred and if so, whether it violated the defendant's constitutional rights).

Annex to Swire Testimony:
Acronyms used in this Appendix

ACLU	American Civil Liberties Union
AG	Attorney General
DNI	US Director of National Intelligence
DOD	US Department of Defense
DOJ	US Department of Justice
DOJ NSD	US Department of Justice, National Security Division
EU	European Union
FBI	US Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	US Foreign Intelligence Surveillance Court
FISCR	US Foreign Intelligence Surveillance Court of Review
FTC	US Federal Trade Commission
IC	US Intelligence Community
IG	Inspector General
ISP	Internet Service Provider
MCT	Multiple Communication Transactions
NSA	US National Security Agency
NSD	National Security Division
NSL	National Security Letters
OCR	US Department of Health and Human Services Office for Civil Rights
ODNI	US Office of the Director of National Intelligence
OIG	US Office of the Inspector General
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
SIGINT	Signals Intelligence
US	United States of America
USA FREEDOM	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism