SUMMARY OF U.S. FOREIGN INTELLIGENCE SURVEILLANCE LAW, PRACTICE, REMEDIES, AND OVERSIGHT

ASHLEY GORSKI
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

AUGUST 30, 2018

TABLE OF CONTENTS

QUALIFICATIONS AS AN EXPERT

1. I am a U.S.-qualified attorney and an expert in U.S. surveillance law. I am currently employed by the National Security Project of the American Civil Liberties Union Foundation. The ACLU is a U.S. nationwide, non-profit, nonpartisan organization with more than 1,700,000 members dedicated to protecting the fundamental rights guaranteed by the U.S. Constitution, the laws of the United States, and the international laws and treaties by which the United States is bound.

2. In my position as an attorney with the National Security Project, I litigate civil and criminal cases in U.S. court, challenging the U.S. government's foreign intelligence surveillance and seeking transparency about its surveillance practices. These cases include *Wikimedia Foundation v. National Security Agency*, No. 15-cv-662-TSE (D. Md.), a challenge to "Upstream" surveillance under Section 702 of the Foreign Intelligence Surveillance Act, and *ACLU v. National Security Agency*, No. 17-3399 (2d Cir.), a suit seeking key legal interpretations governing surveillance under Executive Order 12333.

3. In addition to the cases I am currently litigating or advising on, I have provided expert testimony on U.S. surveillance law and practice to the German Bundestag's First Committee of Inquiry, which is tasked with investigating the U.S. National Security Agency's surveillance in the wake of the disclosures by Edward Snowden. I have also provided expert testimony on U.S. surveillance law and redress mechanisms to the Irish High Court in connection with this litigation, and to the General Court of the Court of Justice in connection with *La Quadrature du Net contre Commission Européenne*, Affaire T-738/16, a pending challenge to the validity of the U.S.–E.U. Privacy Shield.

4. I received my Bachelor of Arts degree *magna cum laude* from Yale University and my Juris Doctor degree *cum laude* from Harvard Law School. I am a member of the Bar of the State of New York and am admitted to practice in several federal courts. Following law school, I worked at a commercial law firm in New York City; clerked for the Honorable Miriam Goldman Cedarbaum, United States District Court Judge, Southern District of New York; and clerked for the Honorable Jon O. Newman, United States Circuit Court Judge, Second Circuit Court of Appeals.

INTRODUCTION

5. I have been instructed by Mr. Max Schrems to summarize the facts regarding (1) material U.S. government surveillance law and practice, (2) redress for rights violations resulting from U.S. foreign intelligence surveillance, and (3) U.S. government oversight mechanisms.

6. Throughout my opinion, I refer to and rely on a number of U.S. laws, judgments, policies, an executive order, and other documents concerning U.S. surveillance law.

I. U.S. SURVEILLANCE LAW AND PRACTICE

7. The High Court of Ireland has made numerous findings concerning U.S. foreign intelligence surveillance. Its opinion focused on two of the most significant U.S. surveillance authorities: Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which authorizes warrantless surveillance that takes place on U.S. soil and targets foreigners; and Executive Order ("EO") 12333, which authorizes warrantless electronic surveillance that largely takes place outside the United States.[1]

8. This section of the report first summarizes the legal framework governing U.S. foreign intelligence surveillance, to provide necessary context for the U.S. government's claim that this surveillance is conducted in accordance with the law and is "duly authorized."[2] The report then describes the scope of surveillance conducted under Section 702 and EO 12333, and it discusses Presidential Policy Directive-28 ("PPD-28"), a directive issued by President Barack Obama in 2014 that has resulted in some very modest reforms.

9. In describing the parameters of surveillance conducted under Section 702 and EO 12333, I note that the constitutionality of these two authorities is deeply contested. For the reasons I discuss in the second part of this report, there are significant barriers to challenging the lawfulness of this surveillance in civil litigation.

10. Under Section 702 and EO 12333, the U.S. government claims legal authority to obtain extraordinary access to the private communications and data of persons around the world. Although there are guidelines governing the collection, retention, and use of this

[1] In the United States, a "warrant" is an order that authorizes a search or seizure. It must be issued by a neutral and detached magistrate, and be based on probable cause that the search or seizure will reveal evidence of a crime. It must also describe with particularity the place to be searched and the things to be seized. The warrant process helps ensure that deprivations of privacy or property are limited and justified. *See, e.g.*, *United States v. Karo*, 468 U.S. 705, 718 (1984); *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297, 316 (1972).

[2] Letter from Robert Litt, General Counsel, Office of the Director of National Intelligence, to Justin Antonipillai, Counselor, U.S. Dep't of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration, at 18 (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F ("ODNI Privacy Shield Letter").

information, the U.S. government maintains that it is authorized to engage in what is known as "bulk collection" when it is operating outside of the United States under EO 12333. *See infra* ¶¶ 50–51, 56–57. Even when the government conducts so-called "targeted" surveillance under Section 702 or EO 12333, the standards for targeting a non-U.S. person located abroad are extraordinarily low. *See infra* ¶¶ 26, 29, 37, 48. In addition, in order to locate its targets' communications, the government routinely searches the contents of countless communications in bulk.

11. As discussed below, under Section 702 and EO 12333, the U.S. obtains generalized access to the content of E.U.–U.S. communications. *Cf. Schrems v. Data Protection Commissioner* (C-362/14), 2000 EUR-Lex 520 (Oct. 6, 2015) ("*Schrems*").

A. LEGAL FRAMEWORK

1. *Presidential Power to Conduct Foreign Intelligence Surveillance*

12. The U.S. Constitution is the starting point for understanding surveillance law. The President's powers are set out in Article II of the U.S. Constitution. Article II allocates to the Office of the President the role of executive and commander-in-chief. Stemming from this authority, the President is authorized to gather foreign intelligence, subject to other provisions of the U.S. Constitution—including the Fourth Amendment—and statutory limitations.

13. The Fourth Amendment to the U.S. Constitution provides the baseline legal protection for privacy from government surveillance. Yet the U.S. government contends that the Fourth Amendment typically does not protect non-U.S. persons outside the United States. *See infra* ¶ 83. It also contends that the Fourth Amendment's warrant requirement does not apply to surveillance undertaken for foreign intelligence purposes because such surveillance falls within an exception known as the "special needs" doctrine.[3]

[3] *See, e.g.*, Gov. Unclassified Resp. at 32–34, *United States v. Mohamud*, No. 10-cr-00475 (D. Or. May 3, 2014), ECF No. 509. Under the Fourth Amendment, warrantless searches are "per se unreasonable"—and therefore unlawful—with only "a few specifically established and well-delineated exceptions," such as the special needs doctrine. *Katz v. United States*, 389 U.S. 347, 357 (1967).

14. Separately, consistent with Congress's enumerated powers in Article I of the Constitution, the U.S. legislative branch generally has the power to authorize and to restrict the conduct of surveillance. Congress has imposed such restrictions, specifically through the passage of FISA in 1978, and in amendments to the act over the past four decades. Section 702, which is part of FISA, was adopted in 2008 and reauthorized in 2012 and 2018.

2. *The Expansion of U.S. Government Surveillance*

15. Under the administration of former President George W. Bush, the executive branch conducted surveillance in violation of laws passed by Congress. After the terrorist attacks of September 11, 2001, President Bush ordered the National Security Agency ("NSA") to monitor and collect communications between foreigners and U.S. persons inside the United States without first obtaining judicial authorization, as FISA required at the time. The Bush administration claimed that under the President's Article II powers, he had broad inherent authority to conduct foreign intelligence surveillance, and that FISA "cannot restrict the President's ability to engage in warrantless searches that protect the national security."[4] The Bush administration also claimed that when Congress passed the Authorization to Use Military Force ("AUMF") following September 11, 2001, it effectively authorized the President to conduct whatever surveillance he deemed necessary in fighting international terrorism, regardless of the constraints of FISA or other statutory law.[5] The AUMF is still in force today.[6]

---

[4] Letter from John C. Yoo, Deputy Assistant Attorney General, Dep't of Justice Office of Legal Counsel, to Judge Colleen Kollar-Kotelly, at 5, 7 (May 17, 2002), https://www.dni.gov/files/documents/OLC%209-with%20attachment.pdf ("It might be thought, therefore, that a warrantless surveillance program, even if undertaken to protect the national security, would violate FISA's criminal and civil liability provisions. Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities.").

[5] *See* Ellen Nakashima, *Legal Memos Released on Bush-era Justification for Warrantless Wiretapping*, Wash. Post, Sept. 6, 2014, https://www.washingtonpost.com/world/national-security/legal-memos-released-on-bush-era-justification-for-warrantlesswiretapping/2014/09/05/91b86c52-356d-11e4-9e92-0899b306bbea_story.html.

[6] *See* Sheryl Gay Stolberg, *Senate Rejects Bipartisan Effort to End 9/11 Military Force Declaration*, N.Y. Times, Sept. 13, 2017, https://www.nytimes.com/2017/09/13/us/politics/senate-rejects-rand-paul-effort-to-end-military-force-declaration.html.

16. Section 702 of FISA is in part the result of President Bush's authorization of surveillance in violation of U.S. law. When this warrantless wiretapping program was disclosed to the American public in December 2005, it generated enormous public outcry. Nonetheless, Congress largely approved the practice of warrantless surveillance of international communications for foreign intelligence purposes in Section 702, and even expanded the government's ability to conduct warrantless surveillance, while imposing certain narrow limitations.[7]

17. Many of the U.S. government's other foreign intelligence surveillance activities are not governed by any statutory law, such as electronic surveillance conducted solely pursuant to EO 12333 and its associated directives and policies. As context for the discussion below of EO 12333 and PPD-28, it is essential to understand that, according to the U.S. Department of Justice, a President can modify or revoke executive orders or policy directives at any time—even in secret.[8]

18. One must also be aware of the risk that the U.S. President secretly has decided or will again decide that she or he need not follow limitations set by Congress on surveillance powers, much as the Bush administration did.

B. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

19. In 1978, largely in response to congressional investigations of decades of improper surveillance by U.S. intelligence agencies, Congress enacted FISA to partially regulate surveillance conducted for foreign intelligence purposes. The statute created a secret

[7] I use the term "international" to describe communications that either originate or terminate outside the United States, but not both.

[8] The Federal Register Act requires the President to publish any executive orders that have general applicability and legal effect. However, in December of 2007, Senator Sheldon Whitehouse discovered classified Office of Legal Counsel ("OLC") memos indicating that it had taken the position that a President can "waive" or "modify" any executive order simply by not following it—without notice to the public or Congress. *See* Congressional Record S15011–12 (Dec. 7, 2007) (statement of Sen. Whitehouse), https://www.congress.gov/crec/2007/12/07/CREC-2007-12-07-pt1-PgS15011-2.pdf. OLC is part of the Department of Justice and provides legal advice to the President and executive branch agencies. "OLC's legal advice is treated as binding within the Executive Branch until withdrawn or overruled." *See, e.g.*, Trevor Morrison, *Stare Decisis in the Office of Legal Counsel*, 110 Colum. L. Rev. 1448, 1464, 1469 (2010).

court, known as the Foreign Intelligence Surveillance Court ("FISC"), and empowered it to review government applications for surveillance in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). The public has limited insight into the conduct of the FISC—and thus the conduct and scope of surveillance under FISA—because the government's filings to the court and the court's rulings are classified by default.[9]

1. *Traditional FISA: Individual Orders*

20. As originally enacted, FISA generally required the government to obtain an individualized order from a FISC judge before conducting certain kinds of "electronic surveillance" on U.S. soil. *See id.* §§ 1801(f) (defining "electronic surveillance"), 1805, 1809(a)(1).[10] To obtain what is known as a "traditional" FISA order, the government must make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—such as a telephone line—to be monitored. *See id.* § 1804(a).

21. The FISC may issue an order authorizing electronic surveillance only if a judge finds that, among other things, there is "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power," and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).

22. The basic framework established by FISA remains in effect today, but it has been significantly altered by 2008 amendments to the statute that permit the acquisition of international communications without probable cause or individualized suspicion, as

[9] In 2015, Congress enacted a law that requires government officials to "conduct a declassification review of each decision, order, or opinion issued" by the FISC "that includes a significant construction or interpretation of any provision of law." 50 U.S.C. § 1872. Declassification reviews typically result in the release of partially redacted opinions, which can still obscure important facts and analysis from the public. Moreover, the executive branch has argued in litigation that it is not obligated to conduct declassification reviews of significant FISC opinions issued prior to the enactment of this law. *See* Aaron Mackey, *USA Freedom Act Requires Government to Declassify Any Order to Yahoo*, Elec. Frontier Found. (Oct. 7, 2016), https://www.eff.org/deeplinks/2016/10/usa-freedom-act-requires-government-declassify-any-order-yahoo.

[10] Some kinds of foreign intelligence surveillance were left unregulated by FISA and are conducted under the auspices of EO 12333. *See infra* Section I.E.

described below. These amendments include the provision known as Section 702 of FISA. *See* 50 U.S.C. § 1881a.

2. *Bulk Searches Under Traditional FISA*

23. Although the traditional FISA framework is more privacy-protective than Section 702, news reports indicate that even traditional FISA orders, issued under Title I of the statute, have authorized the bulk searching of the contents of communications in order to locate specific information. In 2015, a FISC judge apparently issued an order pursuant to traditional FISA that compelled Yahoo to scan *all incoming email traffic*, in real time, for a digital "signature" of a communications method purportedly associated with a foreign power. The search was reportedly performed on all messages as they arrived at Yahoo's servers.[11] Such a massive scan, conducted at the behest of the U.S. government, belies the claim that surveillance under traditional FISA is always meaningfully targeted.[12]

24. As discussed in greater detail below, analogous forms of real-time "bulk searching" are common to both Section 702 and EO 12333 surveillance.

---

[11] *See, e.g.*, Joseph Menn, *Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence—Sources*, Reuters, Oct. 4, 2016, http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT; Charlie Savage & Nicole Perlroth, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. Times, Oct. 5, 2016, http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html; Lorenzo Franceschi-Bicchierai, *Yahoo's Government Email Scanner Was Actually a Secret Hacking Tool*, Motherboard, Oct. 7, 2016, https://motherboard.vice.com/en_us/article/53dkdk/yahoo-government-email-scanner-was-actually-a-secret-hacking-tool.

[12] *See* ODNI Privacy Shield Letter at 10 n.12 (discussing traditional FISA). The ODNI Privacy Shield Letter also explains that the USA FREEDOM Act specifically prohibits the use of other portions of FISA—the pen register and "business record" authorities—for bulk collection. *See id.* However, in 2017, even "targeted" collection under FISA's business record authority, 50 U.S.C. § 1861(b)(2)(C), resulted in the acquisition of more than 534,000,000 "call detail records." ODNI, *Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2017* at 35 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf ("ODNI Statistical Transparency Report").

C. SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

25. In 2008, Congress enacted Section 702 of FISA, a statute that radically revised the FISA regime by authorizing the government's warrantless acquisition of U.S. persons' international communications from companies—such as telecommunications and Internet service providers—inside the United States.[13] *See* 50 U.S.C. § 1881a. Like FISA surveillance, surveillance conducted under Section 702 takes place on U.S. soil. However, surveillance under Section 702 is far more sweeping than surveillance historically conducted under FISA, and it is subject to only a very limited form of judicial oversight. The role that the FISC plays under Section 702 bears no resemblance to the role it has traditionally played under FISA.

26. First, unlike traditional FISA, Section 702 allows the government to warrantlessly monitor communications between people inside the United States and non-U.S. persons abroad.[14] Specifically, it authorizes the government to intercept communications when:

- At least one party to a phone call or Internet communication is a non-U.S. person abroad; and
- A "significant purpose" of the surveillance is "foreign intelligence" collection. *See* 50 U.S.C. § 1881a(a) (authorizing "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information"); *id.* § 1881a(g)(2)(A)(v) ("significant purpose" requirement).

Importantly, surveillance conducted under Section 702 may be conducted for many purposes, not just "national security."[15] The statute defines "foreign intelligence

[13] In August 2007, Congress passed a predecessor statute, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007). Those authorities expired in February 2008.

[14] *See* 50 U.S.C. § 1801(i) (defining "United States person").

[15] The U.S. government's foreign intelligence surveillance is not limited to national security purposes. *See* ODNI Privacy Shield Letter at 17 ("The United States only uses signals intelligence to advance its national security *and foreign policy interests*[.]" (emphasis added)); *id.* at 1 (explaining that intelligence collection focuses on "*foreign intelligence* and national security priorities" (emphasis added)). Yet the Privacy Shield Adequacy Decision elides the distinction between "national security" and broader "foreign intelligence" purposes. *See* European Commission, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the E.U.–U.S. Privacy Shield* ¶¶ 76, 88 &

information" broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e). This definition could be read by the U.S. government to encompass communications concerning, for example, the evasion of U.S. sanctions, the future of the North Atlantic Treaty Organization, responses to U.S. tariffs, and the Paris Agreement on climate change. "Foreign intelligence information" could also be read by the U.S. government to encompass any information related to political and economic developments in E.U. member states.

27. Second, whereas surveillance under traditional FISA is subject to individualized judicial authorization, surveillance under Section 702 is not. The FISC's role in authorizing Section 702 surveillance is "narrowly circumscribed" by the statute.[16] Rather than individually review the executive branch's targets or selectors, the FISC instead reviews, on an annual basis, U.S. government "certifications" that identify broad categories for foreign intelligence surveillance. *See* 50 U.S.C. § 1881a(i). Although the ODNI Privacy Shield Letter states that the government's certifications identify "specific categories" of foreign intelligence,[17] documents show that these categories are in fact quite expansive, covering "foreign governments and similar entities," "counterterrorism," and "weapons of mass destruction."[18] According to a leaked version of the "foreign governments" certification, the FISC has permitted U.S. intelligence agencies to exercise their discretion in conducting surveillance related to more than 190 different countries.[19]

---

n.97 (2016), https://publications.europa.eu/en/publication-detail/-/publication/c183d956-57a6-11e6-89bd-01aa75ed71a1/language-en ("Adequacy Decision"). It also characterizes the acquisition of foreign intelligence information as a "legitimate policy objective" within the meaning of *Schrems*, *see id.* ¶ 89 & n.97, despite the fact that the *Schrems* opinion referred more specifically to "national security" as a legitimate policy objective. *See Schrems* ¶ 88.

[16] *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

[17] ODNI Privacy Shield Letter at 10.

[18] *See* NSA Office of the General Counsel, *FISA Amendments Act of 2008 Section 702 Summary Document* (Dec. 23, 2008), https://www.eff.org/files/2014/06/30/fisa_amendments_act_summary_document_1.pdf.

[19] In the Matter of Foreign Governments, Foreign Factions, Foreign Entities, and Foreign-Based Political Organizations, DNI/AG 702(g) Certification 2010-A, July 16, 2010, *available at* https://www.washingtonpost.com/apps/g/page/world/list-of-foreign-governments-and-organizations-authorized-for-surveillance/1133. News reports indicate that the NSA has relied on the foreign governments certification to search for addresses and

28. Each year, the FISC reviews the general procedures the government proposes to use in carrying out Section 702 surveillance. *See* 50 U.S.C. § 1881a(i). The purpose of these procedures is to facilitate surveillance of non-U.S. persons abroad who are likely to communicate foreign intelligence information, and to provide some limited protections for U.S. persons. Critically, these "targeting" and "minimization" procedures are not designed to provide any safeguards for E.U. persons outside the United States. Targeting procedures must be reasonably designed to ensure that government agents are "targeting persons reasonably believed to be located outside the United States," and are avoiding the "intentional acquisition" of purely domestic communications. *Id.* § 1881a(d). Minimization procedures must be reasonably designed to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting *United States persons* consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* §§ 1801(h) (emphasis added), 1881a(e). Although the ODNI Privacy Shield Letter cites to these procedures as privacy safeguards, the procedures do not even acknowledge the privacy interests of non-U.S. persons located outside the United States.[20] Moreover, in practice,

---

cybersignatures associated with computer hacking—further evidence of the breadth of this certification. *See* Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border*, N.Y. Times, June 4, 2015, https://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.

[20] *See, e.g.*, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (Mar. 30, 2017) (approved Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf ("NSA Section 702 Targeting Procedures"); Minimization 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 (Mar. 30, 2017) (approved Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf ("NSA Section 702 Minimization Procedures").

Although the European Commission's first annual review of Privacy Shield states that the FISC examines how targeting and minimization procedures are being implemented, the FISC does not, as a routine matter, obtain information from agencies concerning implementation of the procedures. *See* Commission Staff Working Document, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield* 26 (Oct. 18, 2017), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0344&from=EN ("First Annual Review"). The executive branch has, in the past, twice provided information to the FISC about a random sampling of targeting decisions; however, as of February 2016, "the

the procedures give the government broad latitude to analyze and disseminate both U.S. and non-U.S. persons' communications. *Id.* § 1881a(d)–(g). *See infra* ¶¶ 37–39.

29. Third and relatedly, unlike traditional FISA, Section 702 authorizes surveillance that is not predicated on the probable cause standard. When government analysts make targeting decisions, they need not demonstrate that their surveillance targets are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, Section 702 permits the government to target **any** non-U.S. person located outside the United States to obtain foreign intelligence information.

30. Fourth, Section 702 does not require the government to identify to the FISC the specific "facilities, places, premises, or property at which" its surveillance will be directed. 50 U.S.C. § 1881a(g)(4). Thus, under the statute, the government may direct its "targeted" surveillance at major junctions on the Internet, through which flow the communications of millions of people, rather than at individual telephone lines or email addresses.[21]

31. Because the legal threshold for targeting non-U.S. persons is extremely low, and because the minimization requirements are so permissive, Section 702 effectively exposes every international communication—that is, every communication between an individual or entity in the United States and a non-U.S. person in the European Union—to potential surveillance. The statute contains no express protections for the privacy of non-U.S. persons located abroad.

Court ha[d] not requested additional tasking sheets or queries beyond what was provided in January and May 2015." Privacy & Civil Liberties Oversight Board ("PCLOB"), *Recommendations Assessment Report* 19 (Feb. 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

[21] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 36–37 (2014), https://www.pclob.gov/library/702-Report.pdf ("PCLOB Report").

D. HOW THE U.S. GOVERNMENT USES SECTION 702 IN PRACTICE

1. *Data Collection: PRISM and Upstream Surveillance*

32. Official government disclosures show that the government uses Section 702 to conduct at least two types of surveillance: "Upstream" surveillance and "PRISM" surveillance.[22] Given the broad parameters of Section 702, the government may rely on the statute to conduct other still-secret surveillance programs as well.

33. As the Irish High Court correctly found, "On the basis of . . . the evidence in relation to the operation of the PRISM and Upstream programmes authorized under s. 702 of FISA, it is clear that there is mass indiscriminate **processing** of data by the United States government agencies[.]"[23]

34. PRISM surveillance involves the acquisition of communications content and metadata directly from U.S. Internet and social media platform companies like Facebook, Google, and Microsoft under Section 702.[24] The government identifies the user accounts it wishes to monitor, and then orders the provider to disclose to it all communications and data to or from those accounts.[25] Through PRISM surveillance, the U.S. government acquires both real-time and stored communications.[26]

---

[22] *See* PCLOB Report 33–41. The government has recently started referring to PRISM surveillance as "downstream" surveillance. Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml (describing "downstream" surveillance as "previously referred to as PRISM").

[23] Oct. 3, 2017 Judgment ¶ 190, *Data Prot. Comm'r v. Facebook Ireland* [2017] IEHC 545.

[24] *See* PCLOB Report 33–34; [*Redacted*], No. [Redacted], 2011 WL 10945618, at *9–10 & n.24 (FISC Oct. 3, 2011); *NSA Program Prism Slides*, Guardian, Nov. 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (slide describes "Collection directly from the servers" of U.S. service providers).

[25] The PCLOB Report states that under PRISM, the FBI, on behalf of the NSA, sends selectors to United States-based electronic communication service providers. PCLOB Report 33. According to media reports, the FBI's Data Intercept Technology Unit (DITU) then gathers information from companies, which is subsequently disseminated to other government agencies. *See, e.g.*, Shane Harris, *Meet the Spies Doing the NSA's Dirty Work*, Foreign Policy, Nov. 21, 2013, http://foreignpolicy.com/2013/11/21/meet-the-spies-doing-the-nsas-dirty-work ("But having the DITU act as a conduit provides a useful public

35. Upstream surveillance involves the mass copying and searching of Internet communications flowing into and out of the United States. With the help of telecommunications companies like Verizon and AT&T, the NSA conducts this surveillance by tapping directly into the Internet backbone inside the United States—the physical infrastructure that carries the communications of hundreds of millions of persons around the world. When conducting this surveillance, the NSA searches the **metadata and content** of international Internet communications transiting the links that it monitors.[27] The agency searches for key terms, called "selectors," that are associated with its many non-U.S.-person targets. Selectors used in connection with this particular form of surveillance include identifiers such as email addresses or phone numbers. The Department of Justice appears to have secretly authorized the NSA to use IP addresses and certain malware signatures as selectors as well.[28] Thus, through Upstream surveillance, the NSA has generalized access to the content of communications, as it indiscriminately copies and then searches the vast quantities of personal metadata and content passing through its surveillance devices.[29] As the Irish High Court correctly found, "under UPSTREAM there is mass surveillance in the sense that there is mass searching of

---

relations benefit: Technology companies can claim — correctly — that they do not provide any information about their customers directly to the NSA, because they give it to the DITU, which in turn passes it to the NSA.").

[26] *NSA Program Prism Slides*, Guardian, Nov. 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.

[27] *See, e.g.*, [*Redacted*], 2011 WL 10945618, at *10, *15; PCLOB Report 35–41; Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. Times, Apr. 28, 2017, https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html; Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

[28] *See, e.g.*, Savage, *supra* note 19.

[29] *See, e.g.*, PCLOB Report 35–39, 41, 111 n.476; [*Redacted*], 2011 WL 10945618, at *10–11. Although data in transit may be encrypted, that would not prevent the NSA from copying, examining, and seeking to decrypt the intercepted data through Upstream surveillance. When the agency collects encrypted communications under Section 702, it can retain those communications indefinitely, and public disclosures indicate that the NSA has succeeded in circumventing encryption protocols in various contexts. *See, e.g.*, *Inside the NSA's War on Internet Security*, Der Spiegel, Dec. 28, 2014, http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.

communications."[30] Following the mass searching of communications, those to and from selectors—as well as those that happen to be bundled with them in transit—are retained on a long-term basis for further analysis and dissemination.[31]

2. *Scope of Section 702 Collection*

36. The U.S. government uses Upstream and PRISM to access and retain huge volumes of communications. In 2011, Section 702 surveillance resulted in the retention of more than 250 million Internet communications—a number that does not reflect the far larger quantity of communications whose contents the NSA searched before discarding them.[32] Although the precise number of communications retained today under Section 702 is not public, the Privacy and Civil Liberties Oversight Board ("PCLOB") observed in 2014 that "[t]he current number is significantly higher."[33] Given the rate at which the number of Section 702 targets is growing, the government today likely collects over a billion communications under Section 702 each year. In 2011, the government monitored approximately 35,000 "unique selectors";[34] by contrast, in 2017, the government targeted the communications of 129,080 individuals, groups, and organizations—most of whom are undoubtedly associated with multiple Internet accounts or "unique selectors."[35] Whenever the communications of these targets—who may be journalists, academics, or human rights advocates—are stored in, routed through, or transferred to the United States,

[30] Oct. 3, 2017 Judgment ¶ 189, *Data Prot. Comm'r v. Facebook Ireland* [2017] IEHC 545.

[31] *See, e.g.*, Mem. Op. & Order at 23–30, [*Redacted*] (FISC Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf; PCLOB Report 35–41.

[32] *See* [*Redacted*], 2011 WL 10945618, at *9–10; PCLOB Report 111 n.476.

[33] PCLOB Report 116.

[34] Glenn Greenwald, *No Place to Hide* 111 (2014), http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf (referencing NSA documents showing that 35,000 "unique selectors" were surveilled under PRISM in 2011).

[35] 2017 ODNI Statistical Transparency Report at 14 (disclosing that the government targeted 129,080 different individuals, groups, and organizations under Section 702 in 2017).

they are subject to interception and retention by communications providers acting at the direction of the U.S. government.[36]

37. The U.S. government has recently published partially redacted versions of its Section 702 targeting procedures for the NSA and the Federal Bureau of Investigation ("FBI").[37] As contemplated by the statute, these procedures provide the government with broad authority to target non-U.S. persons located abroad to acquire foreign intelligence information. For example, the NSA's procedures state that the agency must "reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or *is likely to communicate* foreign intelligence information concerning a foreign power or foreign territory" (emphasis added).[38] Again, the target need not be involved in any wrongdoing or even involved in a foreign intelligence matter; rather, the target need only be a non-U.S. person abroad who is likely to discuss foreign intelligence information. This is a very low threshold in light of the statute's broad definition of "foreign intelligence information." 50 U.S.C. § 1801(e).

38. In the course of acquiring targets' communications, the U.S. government also "incidentally" collects the communications of non-targets, as well as untold volumes of communications that have nothing to do with foreign intelligence. According to an analysis of a large cache of Section 702 interceptions that was provided to the *Washington Post*, nine out of ten account holders in the NSA's surveillance files "were not the

[36] The European Commission's first annual review of Privacy Shield cites various transparency figures from Internet companies to support the proposition that the number of accounts affected by U.S. government surveillance is low. *See* First Annual Review at 28. In reality, however, the number of "accounts affected" is far higher for at least two reasons. First, surveillance targets correspond and interact with non-targets, whose private information is also swept up in surveillance. Second, these statistics do not account for the searching and collection of communications in transit under Section 702 Upstream surveillance; nor do they account for EO 12333 surveillance, which does not involve court orders or directives issued to electronic communication service providers.

[37] *See* Procedures Used by the Federal Bureau of Investigation for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (Sept. 21, 2016) (approved Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Targeting_Procedures_Sep_26_2017.pdf; NSA Section 702 Targeting Procedures.

[38] NSA Section 702 Targeting Procedures at 4.

intended surveillance targets but were caught in a net the agency had cast for somebody else."[39] Although many of the files were "described as useless by the analysts," they were nonetheless retained—including "medical records sent from one family member to another, resumes from job hunters and academic transcripts of schoolchildren. . . . Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risqué poses in shorts and bikini tops."[40] That these communications were acquired through the use of selectors demonstrates that even "targeted" surveillance involves the collection and retention of vast amounts of non-targets' private information. The *Washington Post*'s analysis also underscores the weakness of the U.S. government's minimization procedures, discussed below.

3. *Retention, Dissemination, and Use of Data Collected Under Section 702*

39. The U.S. government has also published partially redacted versions of its Section 702 minimization procedures for the NSA, FBI, CIA, and National Counterterrorism Center.[41] These procedures provide the government with broad authority to retain, analyze, and use the data it has collected. For example, it can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information. Even for data that does not fall into either of these categories, the government may retain the hundreds of millions of communications collected pursuant to Section 702 in its databases for years.[42] During

[39] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014, https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

[40] *Id.*

[41] *See* ODNI, *Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents*, IC on the Record (May 11, 2017), https://icontherecord.tumblr.com/post/160561655023/release-of-the-fisc-opinion-approving-the-2016.

[42] The default retention period for PRISM collection is five years, and two years for Upstream collection. *See* NSA Section 702 Minimization Procedures § 6(a)(1)(b). These two distinct methods of Section 702 surveillance are discussed in greater detail below.

that time, the communications may be reviewed and queried by analysts in both intelligence and criminal investigations.[43]

4. *Recent Modifications to One Subset of Upstream Collection*

40. Under Section 702, the U.S. government claims the authority to gather not only communications to and from the selectors associated with its foreign intelligence targets, but also the communications of any person *about* those selectors. For many years, the government engaged in this collection—known as "about" collection—as part of Upstream surveillance. Although the government has halted "about" collection for the time being, there is no indication that the NSA now lacks generalized access to the metadata or content of communications via Upstream surveillance under Section 702.

41. Last year, the NSA decided to modify one aspect of Upstream collection as a result of the agency's systemic failure to comply with court-imposed restrictions.[44] (The U.S. government's wide-ranging violations of the rules governing Section 702 surveillance are discussed in greater detail *infra* ¶¶ 93–96.) Specifically, NSA analysts had "used U.S.-person identifiers to query the results of Internet 'upstream' collection, even though NSA's Section 702 minimization procedures prohibited such queries."[45] The FISC ascribed the government's failure to timely disclose these violations to "an institutional 'lack of candor' on NSA's part" and emphasized that this was a "very serious" issue.[46]

42. In March 2017, the NSA informed the FISC that it would change how it conducts "about" collection under Section 702.[47] As a result of this change in its policy, the NSA will (for now) "collect" or "acquire" for the government's long-term retention and use only those

[43] *See, e.g.*, Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § III.D (Sept. 26, 2016), https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf.

[44] Mem. Op. & Order at 23–30, [*Redacted*] (FISC Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[45] *Id.* at 15.

[46] *Id.* at 19 (quoting hearing transcript).

[47] *Id.* at 23.

Internet communications that are to or from a target, and not those that are merely "about" a target.

43. Upstream surveillance has long involved the NSA copying and searching the full contents of communications transiting the international Internet links monitored by the agency.[48] Although a FISC opinion and new agency procedures state that the NSA will not "collect" communications that are merely about a target, they do not indicate that the NSA has stopped **copying and searching** communications as they pass through its surveillance devices prior to what the government calls "acquisition" or "collection"—*i.e.*, prior to the NSA's retention, for long-term use, of communications to or from its targets. In other words, there is no indication that the NSA now lacks generalized access to the content of communications via Upstream surveillance under Section 702.[49]

44. In addition, the U.S. government claims the legal authority to resume Section 702 "about" collection in the future, following FISC approval of revised targeting and minimization procedures.[50] Congress's 2018 modifications to Section 702 allow the NSA to restart the practice if it obtains FISC approval, and if Congress does not pass legislation prohibiting the practice within a one-month time period.[51]

45. Importantly, the NSA's change in policy does not affect collection under EO 12333.

---

[48] *See, e.g.*, [*Redacted*], 2011 WL 10945618, at *10, *15; PCLOB Report 35–41; Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, *supra* note 27; Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, *supra* note 27.

[49] Although one might consider the U.S. government's copying and searching of communications a "collection" or "acquisition" of them, the government does not. Within U.S. government agencies, "collect" and "acquire" are terms of art that refer to the longer-term retention of data. For example, although private communications can be searched as they pass through government computer systems, the Department of Defense (of which the NSA is a part) does not consider this "collection." Instead, the Department defines "collection" to exclude "[i]nformation that only momentarily passes through a computer system of the Component." DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* 45 (2016), http://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887.

[50] *See* Press Release, NSA, *supra* note 22.

[51] *See* 50 U.S.C. § 1881a(j)(1)(B).

E. EXECUTIVE ORDER 12333

46. EO 12333 is the primary authority under which the NSA gathers foreign intelligence.[52] It provides broad latitude for the government to conduct surveillance without any form of judicial review or the limitations that apply to surveillance conducted under traditional FISA or even Section 702. Electronic surveillance under EO 12333 is largely conducted outside the United States, though certain EO 12333 collection is conducted on U.S. soil.[53] Collection, retention, and dissemination of data under EO 12333 is governed by directives and regulations promulgated by federal intelligence agencies and approved by the Attorney General, including U.S. Signals Intelligence Directive 0018 ("USSID 18") and other agency policies.[54] In addition, as discussed in greater detail below, PPD-28 and its associated agency policies further regulate EO 12333 activities.

47. EO 12333's stated goal is to provide authority for the intelligence community to gather information bearing on the "foreign, defense, and economic policies" of the United States.[55] EO 12333 authorizes surveillance for a broad range of purposes, resulting in the

---

[52] EO 12333, as amended, *available at* https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.

[53] By surveillance "under EO 12333," I am referring to surveillance that is conducted pursuant to the executive order and is not conducted pursuant to FISA. *See* John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html. One form of EO 12333 surveillance that takes place inside the United States is "International Transit Switch Collection" under "Transit Authority," in which the U.S. government collects cable traffic that traverses U.S. territory but originates and terminates in foreign countries. *See, e.g.*, Signals Intelligence Directorate, *NSAW SID Intelligence Oversight Quarterly Report* 5 (May 3, 2012), *available at* https://www.aclu.org/sites/default/files/field_document/sid_oversight_and_compliance.pdf; Charlie Savage, *Power Wars Document: Transit Authority and the 1990 Lawton Surveillance Memo* (Nov. 18, 2015), http://www.charliesavage.com/?p=557.

[54] *See* NSA, USSID 18: Legal Compliance and U.S. Persons Minimization Procedures (Jan. 25, 2011), http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf ("USSID 18"); *see also* ODNI, Status of Attorney General Approved U.S. Person Procedures Under E.O. 12333 (July 14, 2016), https://www.dni.gov/files/documents/Table_of_EO12333_AG_Guidelines%20for%20PCLOB_%20Updated%20July_2016.pdf (listing other agencies' EO 12333 guidelines).

[55] *See* EO 12333 § 1.1 ("Special emphasis should be given to detecting and countering: (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) Threats to the United

collection, retention, and use of information from large numbers of U.S and non-U.S. persons who have no nexus to foreign security threats.

48. EO 12333 and its accompanying regulations place few restrictions on the collection of U.S. or non-U.S. person information. The order authorizes the government to conduct electronic surveillance for the purpose of collecting "foreign intelligence"—a term defined so broadly that it appears to permit surveillance of any non-U.S. person. *See* EO 12333 § 3.5(e) (defining "foreign intelligence" as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, **foreign persons**, or international terrorists" (emphasis added)). This definition is even broader than the definition of "foreign intelligence information" in FISA, discussed *supra* ¶ 26.

49. In addition, EO 12333 and its implementing regulations permit at least two forms of bulk surveillance.[56]

50. First, they permit the government to engage in "bulk collection"—that is, the indiscriminate collection of electronic communications or data. As explained further below, PPD-28 states that the U.S. government will *use* data collected in bulk for only certain broadly defined purposes.[57] But there is no question that EO 12333 permits collection of both content and metadata in bulk. Even if this collection filters out, for example, all video traffic, bulk collection is indiscriminate by definition, as data is "acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[58] Thus, these policies plainly contemplate access on a generalized basis to the content of electronic communications.

States and its interests from terrorism; and (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.").

[56] *See, e.g.*, USSID 18 § 4; White House, *Presidential Policy Directive 28—Signals Intelligence Activities* at n.5 (Jan. 14, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities ("PPD-28").

[57] *See* PPD-28; NSA, *PPD-28 Section 4 Procedures* § 5 (Jan. 12, 2015), https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf ("NSA PPD-28 Section 4 Procedures").

[58] PPD-28 n.5.

51. The European Commission's Privacy Shield Adequacy Decision asserts that bulk collection will always be "targeted in at least two ways" because it will relate to specific foreign intelligence objectives, and filters will focus the collection "as precisely as possible."[59] But the U.S. government's foreign intelligence objectives are broadly defined, *see infra* ¶ 54, and EO 12333's definition of "foreign intelligence" could encompass virtually any international communication. In addition, focusing bulk, indiscriminate collection as "precisely as possible" is not a meaningful safeguard against the U.S. government's generalized access to communications—particularly when the government has not explained how it determines what is "possible."

52. Second, the order and its implementing regulations allow "bulk searching," in which the government searches the content of vast quantities of electronic communications for "selection terms," as it does with Upstream surveillance under Section 702. In other words, the NSA subjects the data and communications content of the global population to real-time surveillance as the agency scans for specific information of interest. Under EO 12333, the selection terms the NSA uses to search communications in bulk may include a wide array of keywords. Unlike the selectors the government claims to use under Section 702's Upstream surveillance (such as email addresses or phone numbers), EO 12333 procedures permit selectors that are not associated with particular targets. Thus, it appears that the government can use selectors likely to result in the collection of significant volumes of information, such as the names of cities, political parties, or government officials.

53. Indeed, even when the U.S. government conducts "targeted" forms of surveillance under EO 12333, the executive order and its accompanying regulations are extremely permissive with respect to the collection of non-U.S. person information. EO 12333's broad definition of "foreign intelligence" permits surveillance of a vast array of non-U.S. persons with no nexus to national security threats.[60]

[59] Adequacy Decision ¶ 73.

[60] *See* EO 12333 § 3.5(e) (defining "foreign intelligence").

54. Although the ODNI Privacy Shield Letter emphasizes that intelligence analysts are constrained by the National Intelligence Priorities Framework ("NIPF"),[61] the framework's priorities are wide-ranging and elastic. News reports describe the framework as a "matrix of global surveillance," organized by country and theme, and color-coded according to priority.[62] According to an April 2013 version of the NIPF, the "intentions of the political leaders of foreign countries are given the highest priority," ranked as "tier 1" on a scale of one to five.[63] The NIPF also includes an array of other topics, several of which are expansive: for example, Germany "figures in the middle of this international intelligence score card . . . German foreign policy, along with financial and economic issues, are both rated with a '3.' Furthermore, the NSA is interested in Germany's arms control, new technologies, highly developed conventional weapons and international trade, which all have priority '4.'"[64] With foreign intelligence priorities this broad, individual analysts have tremendous latitude in conducting surveillance.

55. Once data has been collected under EO 12333, the executive order permits the retention and dissemination of both U.S. and non-U.S. person information. Under the relevant policies the U.S. government has promulgated, it can generally retain data for up to five years. In addition, it can retain data permanently in numerous circumstances, including data that is (1) encrypted or in unintelligible form;[65] (2) related to a foreign intelligence requirement; (3) indicative of a threat to the safety of a person or organization; or (4) related to a crime that has been, is being, or is about to be committed. The government

[61] ODNI Privacy Shield Letter at 6, 8; *see also* Adequacy Decision ¶ 70.

[62] *The NSA's Secret Spy Hub in Berlin*, Der Spiegel, Oct. 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html; *see also The Matrix is Here...Original NIPF Version, not 'Reloaded'*, Intercept, May 16, 2016, https://theintercept.com/snowden-sidtoday/2830028-the-matrix-is-here-original-nipf-version-not (featuring NSA's Signals Intelligence Directorate's internal newsletter, dated May 15, 2003, which describes the NIPF as "a prioritized list of intelligence topics that encompass the breadth of the Intelligence Community missions plotted against a global set of target countries and organizations").

[63] Ralf Neukirch et al., *Merkel's Pragmatic Approach to the NSA Scandal*, Der Spiegel, Nov. 4, 2013, http://www.spiegel.de/international/world/nsa-scandal-berlin-restricted-by-close-relationship-with-us-intelligence-a-931503-2.html.

[64] *Id.*

[65] The default five-year age-off is triggered when this data is rendered in an intelligible form. *See* NSA PPD-28 Section 4 Procedures § 6.1(a).

may also retain data if it determines in writing that retention is in the "national security interest" of the United States. Information in categories (2), (3), and (4), including information identifying specific individuals, may be disseminated for use throughout the government.[66]

F. HOW THE U.S. GOVERNMENT USES EXECUTIVE ORDER 12333 IN PRACTICE

56. Recent disclosures indicate that the U.S. government operates a host of large-scale programs under EO 12333, many of which appear to involve the collection of vast quantities of U.S. and non-U.S. person information. These programs have included, for example, the NSA's collection of billions of cell phone location records each day;[67] its acquisition of 200 million text messages from around the world each day;[68] its recording of every single cell phone call into, out of, and within at least two countries;[69] its collection of hundreds of millions of contact lists and address books from personal email and instant-messaging accounts;[70] and its surreptitious interception of data from Google and Yahoo user accounts as that information travelled between those companies' data centers located abroad.[71]

---

[66] *See infra* ¶¶ 66–70.

[67] Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, Wash. Post, Dec. 4, 2013, https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[68] James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, Guardian, Jan. 16, 2014, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

[69] Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, Intercept, May 19, 2014, https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas.

[70] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post, Oct. 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html.

[71] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post, Oct. 30, 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

57. According to media reports, under EO 12333, the NSA also taps directly into fiber-optic cables at "congestion points" overseas—junctions through which flow vast quantities of communications.[72] Indeed, as observed by the European Commission in its Privacy Shield Adequacy Decision, the U.S. government may access E.U. citizens' personal data "outside the United States, *including during their transit on the transatlantic cables from the Union to the United States*."[73] In other words, as data is transferred from the European Union to the United States, the U.S. government may access that data on a generalized basis.

G. PPD-28

58. In January 2014, President Barack Obama issued PPD-28, an executive branch directive that articulates broad principles to govern surveillance for intelligence purposes, and that imposes certain constraints on (i) the use of electronic communications collected in "bulk" under EO 12333; (ii) the retention of communications containing personal information of non-U.S. persons; and (iii) the dissemination of communications containing personal information of non-U.S. persons.

59. While PPD-28 recognizes the privacy interests of non-U.S. persons, the directive includes few meaningful reforms—and these reforms can easily be modified or revoked by the U.S. President.

1. *Enforceability of PPD-28*

60. A recently released court decision holds that PPD-28 does not create any enforceable rights, underscoring one of the ways in which the directive does not adequately safeguard the rights of individuals in the European Union.[74] In June 2017, the U.S. government released a partially redacted version of a 2014 FISC opinion, which held that PPD-28, "by

[72] Ryan Gallagher, *How Secret Partners Expand NSA's Surveillance Dragnet*, Intercept, June 18, 2014, https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a.

[73] Adequacy Decision ¶ 75 (emphasis added).

[74] *See infra* ¶¶ 63–70 (discussing shortcomings of PPD-28).

its terms, is not judicially enforceable."[75] Thus, under the court's holding, even if the U.S. government were to persistently and deliberately violate the terms of PPD-28, no E.U. or U.S. person could enforce the directive in court. More generally, those who seek remedies for unlawful surveillance face significant obstacles to redress, as discussed in Section II, *infra*.

2. *PPD-28's Principles*

61. PPD-28 articulates several broad principles to condition the collection of signals intelligence:

- "The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives."[76]
- "Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."[77]
- "The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially. . . . Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage."[78]

---

[75] Mem. Op. at 36, [*Redacted*] (FISC 2014), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/Bates%20510-548_OCR.pdf.

[76] PPD-28 § 1.

[77] *Id.*

[78] *Id.*

- "Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized."[79]

62. Despite these abstract commitments, as discussed below, PPD-28 includes few meaningful constraints on the government's surveillance practices.

3. *PPD-28's Authorization of the Use of Information "Collected in Bulk"*

63. PPD-28 provides that when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering six types of activities:
    - espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
    - threats to the United States and its interests from terrorism;
    - threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
    - cybersecurity threats;
    - threats to U.S. or allied Armed Forces or other U.S. or allied personnel; and
    - transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes above.[80]

64. In sum, this provision effectively ratifies the practice of bulk, indiscriminate collection, and it permits the use of information collected in bulk for several broad, open-ended purposes.

4. *PPD-28's Definition of "Collected in Bulk"*

65. Moreover, PPD-28's limitations on "bulk collection" do not extend to other problematic types of mass surveillance—including the "bulk searching" of Internet communications

[79] *Id.*

[80] *Id.* § 2.

under EO 12333, Section 702, and traditional FISA, as described in paragraphs 23, 35, and 52 above. PPD-28 defines bulk collection to include only: "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[81] This definition explicitly excludes data that is "temporarily acquired to facilitate targeted collection."[82] In other words, PPD-28's restrictions on use do not apply to data that is acquired in bulk and held for only a short period of time. For example, through Upstream surveillance, the U.S. government copies and searches international Internet communications *en masse* to locate communications associated with its targets. PPD-28's definition of "bulk" collection specifically excludes this form of bulk searching as well as similar techniques used under EO 12333.

5. *PPD-28 and Retention, Dissemination, and Use*

66. PPD-28's most significant provisions relate to the retention and dissemination of communications containing "personal information" of non-U.S. persons. However, even these provisions impose few constraints on the government.

67. By default, under the NSA's procedures implementing PPD-28, the government can generally retain data for up to five years, and it can retain data permanently if, for example, the data is encrypted or related to a foreign intelligence requirement. The government may also retain data if it determines in writing that retention is in the "national security interest" of the United States.[83]

68. Under the directive, the government may retain the personal information of non-U.S. persons only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333.[84] Similarly, the government may disseminate

[81] *Id.* § 2 n.5.

[82] *Id.*

[83] NSA PPD-28 Section 4 Procedures §§ 6–7.

[84] PPD-28 § 4(a)(i). PPD-28 requires that departments and agencies apply the term "'personal information' in a manner that is consistent for U.S. persons and non-U.S. persons," and states that "'personal information' shall cover the same types of information covered by 'information concerning U.S. persons' under section 2.3 of Executive Order

the personal information of non-U.S. persons only if the dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333.[85]

69. Critically, however, Section 2.3 of EO 12333 is extremely permissive: it authorizes the retention and dissemination of information concerning U.S. persons when, for example, that information constitutes "foreign intelligence," or the information is obtained in the course of a lawful foreign intelligence investigation.[86] Again, under the executive order, "foreign intelligence" includes "information relating to the capabilities, intentions, or activities" of foreign governments, organizations, **and persons**. *See* EO 12333 § 3.5(e).

70. Further, with respect to retention and dissemination, PPD-28 has not resulted in policies granting the same protections to foreigners as to U.S. persons, as the Adequacy Decision claims.[87] For example, under USSID 18, the NSA's reports may identify a U.S. person where the identity is "*necessary* to understand the foreign intelligence information or assess its importance."[88] In contrast, under the NSA's PPD-28 Section 4 procedures, the NSA may disseminate the personal information of non-U.S. persons if it is merely "related to" a foreign intelligence requirement—a less exacting standard.[89]

12333." *Id.* § 4 n.7. Notably, however, EO 12333 does not define "information concerning U.S. persons."

[85] *Id.* § 4(a)(i).

[86] EO 12333 § 2.3 ("Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of [the relevant agency or element] . . . . Those procedures shall permit collection, retention, and dissemination" of several types of information, including the categories noted above.).

[87] *See* Adequacy Decision ¶ 85.

[88] USSID 18 § 7.2 (emphasis added); *see also* NSA Section 702 Minimization Procedures § 6(b) (authorizing dissemination of a U.S. person's identity where it is "necessary to understand foreign intelligence information or assess its importance").

[89] NSA PPD-28 Section 4 Procedures § 7.2.

II. OBSTACLES TO REDRESS

71. The Privacy Shield Adequacy Decision states that "[a] number of avenues are available under U.S. law to E.U. data subjects if they have concerns whether their personal data have been processed (collected, accessed, etc.) by U.S. Intelligence Community elements," including bringing a civil suit challenging the legality of surveillance, or utilizing the Freedom of Information Act ("FOIA").[90] Below, I explain how these avenues have failed to provide meaningful vehicles for redress for persons concerned about the processing of their personal data. I also briefly address the inadequacy of the Privacy Shield Ombudsperson as a redress mechanism.

A. NOTICE, STANDING, AND THE STATE SECRETS DOCTRINE

1. *No Civil Lawsuit Challenging Section 702 or EO 12333 Surveillance Has Resulted in Any Kind of Remedy*

72. For the overwhelming majority of individuals whose rights are affected by U.S. government surveillance under Section 702 and EO 12333, the government's invocation and interpretation of the "standing" and "state secrets" doctrines have thus far proven to be barriers to adjudication of the lawfulness of its surveillance. To date, as a result of the government's invocation and judicial application of these doctrines, no civil lawsuit challenging Section 702 or EO 12333 surveillance has ever produced a U.S. court decision addressing the lawfulness of that surveillance. Nor has any person ever obtained a remedy of any kind for Section 702 or EO 12333 surveillance, including under the statutory provisions cited in the Adequacy Decision and ODNI Privacy Shield Letter: 50 U.S.C. § 1810, 18 U.S.C. § 2712, 18 U.S.C. § 1030, and 12 U.S.C. § 3417.[91]

[90] Adequacy Decision ¶ 111.

[91] Adequacy Decision ¶ 115; ODNI Privacy Shield Letter at 16–17.

2. *The U.S. Government Maintains That It Generally Has No Obligation to Notify the Targets of Surveillance Under Section 702 or EO 12333*

73. The U.S. government collects extraordinary volumes of communications under Section 702 and EO 12333 each year, and it copies and searches through an even greater quantity. However, because the government has classified its implementation of this surveillance, and because the surveillance is conducted entirely in secret, virtually none of the individuals who are subject to either Section 702 or EO 12333 surveillance ever receive notice of that fact.

74. The U.S. government's position is that it generally has no obligation to notify the targets of its foreign intelligence surveillance under Section 702 or EO 12333, or the countless others whose communications and data have been seized, searched, retained, or used in the course of this surveillance. Thus, even when the U.S. government acquires personal information, stores it for long-term purposes, and uses it—for example, by sharing it with E.U. states—it does not notify those subject to its surveillance.

75. The sole exception is when the government intends to use information against an "aggrieved person" in a trial or proceeding where that information was obtained or derived from FISA.[92] In those circumstances, the government is statutorily required to provide notice.[93] Notably, however, the government refuses to disclose its interpretation of what constitutes evidence "derived from" FISA. To date, I am aware of only ten criminal defendants who have received notice of Section 702 surveillance, despite the U.S. government's collection of billions of communications under that authority.[94]

---

[92] 50 U.S.C. § 1801(k); *see* Gov't Response in Opp. to Def's Mot. for Notice & Discovery of Surveillance at 7–8, *United States v. Thomas*, No. 2:15-cr-00171-MMB (E.D. Pa. July 29, 2016), ECF No. 74 (arguing that a criminal defendant seeking information about government surveillance is not entitled to notice of EO 12333 surveillance).

[93] *See, e.g.*, 50 U.S.C. § 1806.

[94] Even when the government uses Section 702 surveillance in connection with an investigation, individuals do not necessarily receive notice of that surveillance. *See* Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, Intercept, Nov. 30, 2017, https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702 ("The government is obligated to disclose to criminal defendants when information against them originates from Section 702 reporting, but federal prosecutors did not do so in Kurbanov's case.").

3. *The Standing Doctrine Is a Substantial Obstacle to Redress*

76. Because almost no one subject to Section 702 and EO 12333 surveillance receives notice, it is exceedingly difficult to establish what is known as "standing" to challenge the surveillance in U.S. court. Without standing to sue, a plaintiff cannot litigate the merits of either constitutional or statutory claims—and, by extension, cannot obtain any form of relief through the courts.

77. To establish a U.S. federal court's jurisdiction over a claim in the first instance, a plaintiff's complaint must include factual allegations that, accepted as true, plausibly allege the three elements of standing under U.S. doctrine: (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). The asserted injury must be "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 2341 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

78. At the initial stage of a case, a plaintiff's allegations of standing must merely be "plausible." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). But in order for a court to reach the merits of a challenge, a plaintiff must eventually establish these three elements of standing by a preponderance of the evidence. *See Susan B. Anthony List*, 134 S. Ct. at 2342.

79. Because Section 702 and EO 12333 surveillance are conducted in secret, the U.S. government routinely argues to courts that plaintiffs' claims of injury are mere "speculation" and insufficient to establish standing. In 2013, the U.S. Supreme Court accepted such an argument, holding that Amnesty International USA and nine other plaintiffs lacked standing to challenge Section 702 because they could not show with sufficient certainty that their communications were intercepted under the law. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410–11 (2013).

80. Even after the 2013 disclosures by Edward Snowden, no civil plaintiff challenging Section 702 or EO 12333 has established standing by a preponderance of the evidence. Indeed,

many plaintiffs have failed to surpass the initial threshold at the outset of litigation, where a plaintiff's allegations in support of standing must simply be "plausible."[95]

4. *The State Secrets Doctrine Is a Substantial Obstacle to Redress*

81. Standing doctrine is not the only significant obstacle to redress. The U.S. government has also repeatedly invoked the "state secrets privilege" in civil suits, preventing courts from addressing the lawfulness of government surveillance. When properly invoked, this privilege allows the government to block the disclosure of particular information in a lawsuit where the disclosure of that information would cause harm to national security. *See United States v. Reynolds*, 345 U.S. 1 (1953). In recent years, however, the government has successfully used the state secrets privilege not merely to shield particular information from disclosure, but to keep entire cases out of court based on their subject matter. *See, e.g., Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1093 (9th Cir. 2010) (dismissing challenge to U.S. government's extraordinary rendition and torture program on state secrets grounds). Although courts have held that FISA preempts the application of the state secrets privilege for FISA-related claims, *see, e.g., Jewel v. NSA*, 965 F. Supp. 2d 1090, 1105 (N.D. Cal. 2013), the government has nevertheless successfully raised the privilege in challenges to Section 702 surveillance, *see, e.g., Jewel v. NSA*, No. 08-04373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015) (dismissing a Fourth Amendment challenge to Upstream surveillance under Section 702 on standing and state secrets grounds).

82. To date, as a result of the government's invocation and the courts' acceptance of the standing and state secrets objections described above, no civil lawsuit challenging Section 702 or EO 12333 surveillance has ever produced a U.S. court decision addressing the lawfulness of that surveillance.

[95] *See, e.g., Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017). In *Wikimedia*, nine plaintiffs—including Amnesty International USA, Human Rights Watch, and Wikimedia—which engages in more than a trillion communications each year—challenged Upstream surveillance under Section 702. The Fourth Circuit rejected as implausible the standing of the eight plaintiffs other than Wikimedia, which was allowed to proceed to the next phase of the litigation. The opinion illustrates the difficulties that plaintiffs face in establishing standing, even at the outset of a case, when a plaintiff's allegations must merely be plausible. Standing remains a significant obstacle for individuals and organizations that do not engage in the volume and scope of communications of Wikimedia.

B. U.S. Government Arguments Concerning the Applicability of the Fourth Amendment to Non-U.S. Persons Abroad

83. The U.S. government has taken the position that non-U.S. persons located abroad generally have no right to challenge surveillance under the U.S. Constitution. In particular, the U.S. government has stated in court filings that "[b]ecause the Fourth Amendment generally does not protect non-U.S. persons outside the United States," the "foreign targets of Section 702 collection lack Fourth Amendment rights."[96] The government bases this argument on *United States v. Verdugo-Urquidez*, in which the Supreme Court declined to apply the Fourth Amendment's warrant requirement to a U.S. government search of physical property located in Mexico and belonging to a Mexican national. 494 U.S. 259, 261–62, 273 (1990). Although the ACLU maintains that the government's analysis is incorrect, when evaluating the availability of redress for non-U.S. persons, it is significant that the U.S. government regularly argues that non-U.S. persons seeking to challenge warrantless surveillance programs are not entitled to constitutional protection or redress.

C. Other "Redress" Mechanisms

1. *Freedom of Information Act*

84. FOIA is not a form of redress. Rather, this law provides transparency to the public about U.S. government activities. *See* 5 U.S.C. § 552. However, because FOIA permits the government to withhold properly classified information from disclosure, *see id.* § 552(b)(1), and because data gathered pursuant to foreign intelligence authorities is invariably classified, FOIA has not been an effective mechanism to obtain information related to the U.S. government's surveillance of a particular individual's communications or data.

85. I am not aware of any instance in which an individual has succeeded in obtaining information through FOIA that would establish the surveillance of his or her

[96] Supp. Br. of Plaintiff–Appellee at 12, *United States v. Mohamud*, No. 14-30217 (9th Cir. Oct. 3, 2016), ECF No. 110-1.

communications under either Section 702 or EO 12333. In fact, the government prevailed in blocking the disclosure of similar information in response to a FOIA request brought by attorneys who represented detainees held at the U.S. naval facility at Guantánamo Bay, Cuba, and who sought information concerning the surveillance of their communications by the NSA. *See Wilner v. NSA*, 592 F.3d 60 (2d Cir. 2009).

2. *Privacy Shield Ombudsperson*

86. In 2016, the negotiations between the European Union and the United States over the Privacy Shield agreement led to the U.S. executive branch's creation of the Privacy Shield Ombudsperson position.[97] But the Ombudsperson's legal authority and ability to provide meaningful redress are severely limited. As a general matter, the Ombudsperson assesses compliance with surveillance procedures, but there is no indication that she is empowered to assess whether the procedures themselves are constitutional, or to require the executive branch to implement a particular remedy.

87. When the Ombudsperson receives a proper complaint, she will investigate and then provide the complainant with a response "confirming (i) that the complaint has been properly investigated, and (ii) that U.S. law, statutes, executives [*sic*] orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI Letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied."[98]

88. Complainants receive no meaningful information through this scheme, nor are they able to assess the scope of any remedy. Even when the Ombudsperson finds that data was handled improperly, she can neither confirm nor deny that the complainant was subject to surveillance, nor can she inform the individual of the specific remedial action taken.

89. The Ombudsperson's authority is restricted in other ways as well. Most importantly, the Ombudsperson apparently lacks the power to require an executive branch agency to

[97] *See* E.U.–U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.

[98] *See id.* § 4(e).

implement a particular remedy. Although the Commission's annual review states that "the Ombudsperson will make use of the existing oversight structure to ensure that the violation is remedied," there is no indication that the Ombudsperson has any legal authority to require the "existing oversight structure" to implement a particular remedy.[99] Nor is there any indication that the Ombudsperson is empowered to conduct a complete and independent legal and factual analysis of the complaint—*e.g.*, to assess whether surveillance violated the Fourth Amendment, as opposed to simply examining whether surveillance complied with the relevant regulations. Although the Ombudsperson may cooperate with intelligence agencies' Inspectors General and may refer matters to the PCLOB, neither the Inspectors General nor the PCLOB can issue recommendations that are binding on the executive branch.[100] Moreover, the Ombudsperson cannot respond to any claims that the Privacy Shield agreement is inconsistent with E.U. data protection laws. Finally, because the Ombudsperson is part of the State Department, and the State Department is itself part of the intelligence community, this position is not independent from the intelligence community.[101]

90. In short, under the existing rules, an individual who complains to the Ombudsperson will never learn how his complaint was investigated, or how any non-compliance was in fact remedied. He also lacks the ability to appeal or enforce the Ombudsperson's decision. For those seeking redress, the Ombudsperson process provides nothing in the way of a transparent or enforceable remedial scheme. Instead, it is essentially a black box.

---

[99] First Annual Review at 35–36.

[100] *Id.*; Adequacy Decision ¶ 120.

[101] According to the Commission's First Annual Review, "the Ombudsperson will report any attempts of improper influence—from inside or outside the State Department—directly to the Secretary of State." First Annual Review at 34. Notably, however, the Secretary of State is not independent from the intelligence community. *See* ODNI, *Members of the IC*, https://www.dni.gov/index.php/what-we-do/members-of-the-ic#dos (explaining that the State Department is part of the intelligence community and that the State Department's "Bureau of Intelligence and Research provides the Secretary of State with timely, objective analysis of global developments as well as real-time insights from all-source intelligence. It serves as the focal point within the Department of State for all policy issues and activities involving the Intelligence Community.").

III. INADEQUATE OVERSIGHT

91. U.S. government oversight mechanisms provide no substitute for the lack of meaningful redress available to challenge the U.S. government's foreign intelligence surveillance. Despite the ODNI Privacy Shield Letter's characterization of foreign intelligence oversight as "rigorous,"[102] existing oversight mechanisms are inadequate given the breadth of the U.S. government's surveillance activities. Surveillance programs operated under EO 12333 have never been reviewed by any court, and the former Chairman of the Senate Intelligence Committee has conceded that they are not sufficiently overseen by Congress.[103] Similarly, surveillance under Section 702 is not adequately supervised by the courts or by Congress. Other oversight mechanisms, such as the PCLOB and Inspectors General, have only very limited authority and fail to compensate for fundamental deficiencies in judicial and legislative oversight.

A. THE FISC

92. Because neither Section 702 nor its procedures afford any express protection to E.U. persons who are located abroad, the FISC's oversight does not give any consideration to the rights of those persons.[104]

93. Even with respect to U.S. persons' rights, the FISC has not been effective at preventing systemic violations of statutory law or judicial orders. Rather, FISC judges rely on intelligence community self-reporting to learn of violations, sometimes years after the problems first began. Even when compliance violations are eventually disclosed to the FISC, the underlying problems may nevertheless persist for extended periods of time.

---

[102] ODNI Privacy Shield Letter at 7.

[103] Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, McClatchy, Nov. 21, 2013, http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html.

[104] Although PPD-28 should still apply, its protections are both weak and unenforceable, as discussed above. In addition, the government maintains that Section 702 collection is not "bulk" collection within the meaning of PPD-28.

94. After the FISC first learned that the NSA had violated the rules governing various mass surveillance programs conducted over the past decade, FISC judges allowed the programs to continue. For example, in 2011, the government disclosed to the FISC for the first time that the scope of Section 702 Upstream surveillance was broader than previously represented to the court. The FISC stated that it was "troubled that the government's revelations . . . 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."[105] In connection with another one of these programs, the court concluded that the rules had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."[106]

95. Similarly, the FISC's April 2017 opinion identified significant compliance problems with U.S.-person queries of Upstream data, which came to light through the NSA's belated self-reporting. In addition to identifying those problems, the opinion also discussed an array of additional ongoing or recent violations of the court-ordered procedures governing Section 702 surveillance.[107] It bears emphasis that, from the U.S. government's perspective, these court-ordered procedures are what make Section 702 surveillance lawful—and yet several agencies have systematically violated those rules, calling into question the legality of this surveillance writ large.

96. These violations include: NSA failures to complete required purges; compliance and implementation issues regarding the NSA's adherence to its targeting and minimization procedures; the NSA's improper querying of Section 702 data repositories (in addition to the Upstream querying issue discussed at paragraphs 40–45 above), such that "approximately eighty-five percent" of certain queries using U.S. person identifiers were "not compliant with the applicable minimization procedures"; improper FBI disclosures of raw information; FBI failures to comply with requirements governing the handling of attorney-client communications; and CIA problems completing its required purges.[108] The

[105] [*Redacted*], 2011 WL 10945618, at *5 & n.14.

[106] *In re Production of Tangible Things from* [*Redacted*], No. BR 08-13, 2009 WL 9150913, at *5 (FISC Mar. 2, 2009).

[107] Mem. Op. & Order at 68–95, [*Redacted*] (FISC Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[108] *Id.* at 68–95.

FISC also observed that, "[t]oo often . . . the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered."[109]

B. CONGRESS

97. Lawmakers are severely constrained in their efforts to oversee foreign intelligence surveillance programs. As an initial matter, because most of the details about U.S. government surveillance are classified, the executive branch typically limits dissemination of information about this surveillance to only a small subset of legislators on intelligence and judiciary committees.[110] These committees, in turn, have withheld information from the broader Congress. As just one example, the House Intelligence Committee withheld a letter drafted by the Obama administration to inform Congress about the NSA's mass collection of Americans' phone records—despite the fact that the administration specifically instructed the Intelligence Committee to share the letter prior to a key vote.[111] More generally, members of Congress—including on the Senate Intelligence Committee—have been repeatedly thwarted when attempting to obtain information about NSA surveillance.[112] Even when legislators obtain relevant classified information, they are

[109] *Id.* at 67–68 & n.57; *see also* Open Technology Institute, A History of FISA Section 702 Compliance Violations https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations (describing hundreds of Section 702 compliance violations since the enactment of the law).

[110] Jonathan Weisman & David E. Sanger, *White House Plays Down Data Program*, N.Y. Times, June 8, 2013, http://www.nytimes.com/2013/06/09/us/politics/officials-say-congress-was-fully-briefed-on-surveillance.html.

[111] *See* Peter Wallsten, *House Panel Withheld Document on NSA Surveillance Program from Members*, Wash. Post, Aug. 16, 2013, https://www.washingtonpost.com/politics/house-panel-withheld-document-on-nsa-surveillance-program-from-members/2013/08/16/944e728e-0672-11e3-9259-e2aafe5a5f84_story.html; *see also* Ailsa Chang, *What Did Congress Really Know About NSA Tracking*, National Public Radio, June 11, 2013, https://www.npr.org/sections/itsallpolitics/2013/06/11/190742087/what-did-congress-really-know-about-nsa-tracking.

[112] *See, e.g.*, Glenn Greenwald, *Members of Congress Denied Access to Basic Information About NSA*, Guardian, Aug. 4, 2013, https://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access; Press Release, Sen. Ron Wyden, *Wyden Suggests Ways to Estimate Americans Swept Up Under Foreign Surveillance Program*, Aug. 3, 2017, https://www.wyden.senate.gov/news/press-releases/wyden-suggests-ways-to-estimate-americans-swept-up-under-foreign-surveillance-program**;** *Patrick Leahy at NSA Hearing: 'We Get More in the Newspapers than in Classified Briefings*, Huffington Post, Oct. 2, 2013, www.huffingtonpost.com/2013/10/02/patrick-

unable to discuss those issues with other members of Congress outside of a secured facility. Legislators are also unable to rely on staffers for relevant research assistance unless those staffers obtain security clearances, and most legislators lack their own cleared staffer.

98. In addition, the executive branch has adopted policies that are deliberately designed to stymie congressional oversight. For example, a recent authoritative OLC opinion states that the intelligence community need respond only to requests for information from legislative committees or subcommittees vested with oversight authority, or the House or Senate as a whole. According to the opinion, agencies need not respond at all to requests from individual members of Congress; and, if agencies do respond, they should follow a general policy of providing only documents and information that are already public or would be made public under the Freedom of Information Act, 5 U.S.C. § 552.[113] Because the House and Senate are currently under the control of Republicans, this means that the intelligence agencies and the White House are not responding to oversight requests from individual Democrats.[114] This policy makes it extremely difficult for members of Congress, including Democrats sitting on relevant committees, to conduct meaningful oversight of foreign intelligence surveillance.

99. The executive branch has also refused to provide legislators with even basic information critical to Congress' oversight role. Among the most notable examples, the executive branch has refused to provide Congress with an estimate of the number of Americans' communications subject to Section 702 surveillance. In 2011, Senators serving on the Senate Intelligence Committee asked the Inspectors General of the intelligence

---

leahy-nsa_n_4030514.html; Garance Franke-Ruta, *The Hidden Classified Briefing Most of Congress Missed*, Atlantic, Sept. 20, 2013, https://www.theatlantic.com/politics/archive/2013/09/the-hidden-classified-briefing-most-of-congress-missed/279857; Ezra Klein, *The Intelligence Committee Can't Tell You What They're Not Telling You*, Wash. Post, June 7, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/07/the-intelligence-committee-cant-tell-you-what-theyre-not-telling-you.

[113] *See* Curtis E. Gannon, Acting Assistant Attorney General, Office of Legal Counsel, *Authority of Individual Members of Congress to Conduct Oversight of the Executive Branch*, May 1, 2017, https://www.justice.gov/olc/file/966326/download.

[114] Gabrielle Levy, *White House Blocks Democrats' Oversight Efforts*, U.S. News, June 2, 2017, https://www.usnews.com/news/politics/articles/2017-06-02/trump-administration-tells-agencies-to-ignore-democrats-oversight-requests.

community and the NSA to provide such an estimate.[115] After years of advocacy by NGOs and continued requests from Congress, DNI Clapper eventually committed to providing the estimate.[116] However, the Trump administration reneged on that commitment, despite the fact that this estimate would have played an important role in the debate over the reauthorization of Section 702 by illuminating the breadth of the government's surveillance under the statute.[117]

C. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

100. The U.S. government has represented that its intelligence community is subject to various executive-branch oversight mechanisms, including the PCLOB. However, at present, the PCLOB is not a fully functional body, and recent events undermine the U.S. government's assertions that it is an independent oversight mechanism.

101. Since February 2017, four of the five PCLOB board positions have been vacant.[118] Without a quorum, the PCLOB cannot issue reports and recommendations, including its planned report on activities conducted under EO 12333.[119] In addition, the Board is further limited in its ability to make staffing decisions necessary to fulfil its responsibilities.[120]

---

[115] Letter from Rep. John Conyers et al. to the Hon. James R. Clapper, Director, ODNI (Apr. 22, 2016), https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

[116] Dustin Volz, *U.S. To Disclose Estimate of Number of Americans Under Surveillance*, Reuters, Dec. 16, 2016, https://www.reuters.com/article/us-usa-cyber-surveillance/u-s-to-disclose-estimate-of-number-of-americans-under-surveillance-idUSKBN1452FX.

[117] Ellen Nakashima & Karoun Demirjian, *Intelligence Officials Rogers and Coats Said They Won't Discuss Specifics of Private Conversations with Trump*, Wash. Post, June 7, 2017, https://www.washingtonpost.com/world/national-security/nsa-director-rogers-and-intelligence-director-coats-said-they-wont-discuss-specifics-of-private-conversations-with-trump/2017/06/07/e74f7fbe-4b88-11e7-a186-60c031eab644_story.html; Letter from Rep. Bob Goodlatte & Rep. John Conyers to the Hon. Daniel Coats, Director of National Intelligence, June 27, 2017, https://judiciary.house.gov/wp-content/uploads/2017/06/062717_Letter-to-DNI-Coats.pdf.

[118] *Board Members*, Privacy and Civil Liberties Oversight Board, https://www.pclob.gov/board-members (accessed Aug. 30, 2018).

[119] *See also* 6 C.F.R. § 1000.3 (2013), *available at* https://www.pclob.gov/library/FederalRegister-PCLOB-2013-0005-Delegation-Reg.pdf.

[120] *Id.*

The vacancies also impact the extent to which the Board's membership represents diverse political viewpoints. Under statute, no more than three of the Board members may come from the same political party, which ensures that a full Board contains representation from both political parties.[121] The current membership, however, represents only one political party.

102. The process of filling the vacancies on the Board is not an easy one. It requires nomination by the President and confirmation by the Senate—a process that can be lengthy, arduous, and easily derailed. As of this writing, President Trump has nominated five individuals to serve on the Board, and hearings have been held on the first three nominees. Still, none of these individuals have been confirmed by the Senate.[122]

103. Furthermore, even if the PCLOB were fully functioning, it is not designed to provide redress concerning U.S. surveillance practices. It has never provided remedies for rights violations or functioned as a sufficient mechanism to protect personal data. It also lacks the authority to issue binding recommendations to the executive branch. In addition, the PCLOB's mandate is limited to balancing civil liberties and "terrorism prevention."[123] As a result, the board is not positioned to assess U.S. government surveillance and the use of data for broader foreign intelligence purposes beyond terrorism prevention.

104. Recent events also undermine the U.S. government's assertion that the PCLOB is an independent body. According to the European Commission's first annual review of Privacy Shield, the PCLOB's "report on the implementation of PPD-28 has been adopted and sent to the President. Although it was confirmed at the Annual Joint Review that the report has been checked from a national security point of view and certain parts are de-classified, it was also explained that this report cannot be released to the public, as it is currently subject to Presidential privilege."[124] Similarly, in its resolution calling for the suspension of Privacy Shield, the European Parliament expressed concern over President

[121] *See* 42 U.S.C. § 2000ee(h)(2).

[122] Jake Laperruque, *A Proposed Agenda for a New PCLOB*, Lawfare (Aug. 28, 2018), https://www.lawfareblog.com/proposed-agenda-new-pclob.

[123] *History and Mission*, Privacy & Civil Liberties Oversight Board, https://www.pclob.gov/about (accessed Aug. 30, 2018); *see also* 42 U.S.C. § 2000ee(c).

[124] First Annual Review at 31.

Trump's claim of "Presidential privilege" over the report.[125] If the President asserts privilege over the PCLOB's reports to prevent those documents from being distributed, it eliminates one of the PCLOB's few powers: the ability to issue public reports.

105. Finally, the scope of the PCLOB's mandate may be limited by Congress. In 2016, Senators considered legislation that would bar the PCLOB from considering the privacy and civil liberties interests of non-U.S. persons.[126]

D. INSPECTORS GENERAL

106. The European Commission's Adequacy Decision discusses the significance of Inspectors General ("IGs") as a mechanism for overseeing foreign intelligence surveillance, notwithstanding their inability to issue binding recommendations.[127] Although IGs have a critical role to play in the oversight ecosystem, the Adequacy Decision overstates the independence of IGs and fails to account for the scope of a typical IG investigation.

107. In support of its claim that IGs are independent, the Adequacy Decision states that IGs have "secure tenure."[128] However, IGs can be removed by the President without cause.[129] Congress must be notified in those circumstances, but this notification requirement does not provide Congress with legal authority to oppose or override the termination.

108. In addition, the Adequacy Decision claims that IGs have great liberty to conduct investigations and obtain evidence, except where limits are "necessary to preserve

[125] European Parliament, *Resolution on the Adequacy of the Protection Afforded by the EU–US Privacy Shield*, Eur. Parl. Doc. B8-0305 (2018), http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN.

[126] Coalition Letter Opposing Provision of Intelligence Authorization Act on PCLOB (June 24, 2016), https://cdt.org/insight/coalition-letter-opposing-provision-of-intelligence-authorization-act-on-pclob.

[127] Adequacy Decision ¶ 97.

[128] *Id.* ¶ 97 n.110.

[129] 5 U.S.C. App. 3 Sec. 3.

important national (security) interests."[130] In fact, however, the ability of IGs to gather evidence is limited in a number of significant ways.

109. Because contractors and other potential whistleblowers within the intelligence community lack adequate protection when reporting to IGs on illegal activity or policy violations, IGs are almost certainly deprived of information about abuses. Moreover, media reports suggest that institutional cultures within the intelligence community discourage whistleblowing.[131]

110. IGs face other obstacles to obtaining access to information, as discussed in recent congressional testimony by Department of Justice Inspector General Michael Horowitz. According to Horowitz, a 2015 OLC opinion threatened the ability of IGs "to conduct independent and thorough audits, investigations, and reviews by allowing agencies to limit IGs' access to records that were necessary to perform our oversight work."[132] Horowitz also emphasized that some agencies fail to timely supply access to critical records, and IGs lack the authority to subpoena witnesses to testify.[133]

111. Finally, not only are IGs limited in how they can investigate, but they are also limited—at least in practice—in terms of what they investigate in the first place. For example, IGs do

[130] Adequacy Decision ¶ 97 n.110.

[131] Adam Zagorin, *Top NSA Watchdog Who Insisted Snowden Should Have Come to Him Receives Termination Notice for Retaliating Against a Whistleblower*, Project on Government Oversight, Dec. 15, 2016, http://www.pogo.org/blog/2016/12/intelligence-community-landmark.html; Patrick G. Eddington, *Why is Mattis Declaring War on Whistleblowers?*, American Conservative, Aug. 3, 2017, http://www.theamerican conservative.com/articles/why-is-mattis-declaring-war-on-whistleblowers; Jenna McLaughlin, *A Turf War is Tearing Apart the Intel Community's Watchdog Office*, Foreign Policy, Oct. 18, 2017, http://foreignpolicy.com/2017/10/18/turf-war-intelligence-community-watchdog-falling-apart.

[132] Statement of Michael E. Horowitz, Chair, Council of the Inspectors General on Integrity and Efficiency, Inspector General, U.S. Dep't of Justice before the U.S. House of Representatives Committee on Oversight & Government Reform concerning "Recommendations and Reforms from the Inspectors General," Nov. 15, 2017, at 3, https://oversight.house.gov/wp-content/uploads/2017/11/Horowitz-CIGIE-Chair-DOJ-IG-Statement-11-15.pdf.

[133] *Id.* at 3, 6.

not typically assess whether a particular surveillance program authorized by senior executive branch officials or the President is constitutional.[134]

CONCLUSION

112. In summary, the U.S. government claims broad authority to acquire the communications and data of non-U.S. persons located abroad. At bottom, U.S. surveillance law is not designed to protect the privacy of non-U.S. persons, as illustrated by the government's arguments about the reach of the Fourth Amendment. Even in the narrow circumstances in which PPD-28 extends certain protections to non-U.S. persons, the protections are substantively weak and can be modified or revoked at any time. Redress and oversight mechanisms are also inadequate, particularly given the breadth of the U.S. government's surveillance activities.

[134] *See, e.g.*, Offices of Inspectors General of the Dep't of Defense, Dep't of Justice, CIA, NSA, and ODNI, *Unclassified Report on the President's Surveillance Program* 30 (July 10, 2009), https://oig.justice.gov/special/s0907.pdf (concluding that the legal analysis undergirding the Bush administration's warrantless surveillance program was "factually flawed," but omitting any independent constitutional analysis of the program).