THE HIGH COURT

Record No: 2016/4809 P

Between:

THE DATA PROTECTION COMMISSIONER

Plaintiff

-AND-

FACEBOOK IRELAND LIMITED

-AND-

MAXIMILLIAN SCHREMS

Defendants

EXPERT REPORT OF ASHLEY GORSKI
ON BEHALF OF THE SECOND NAMED DEFENDANT

CONTENTS

QUALIFICATIONS AND DUTY OF AN EXPERT TO THE COURT

1. I am a US-qualified attorney, currently employed by the National Security Project of the American Civil Liberties Union Foundation ("ACLU"), and I am admitted to practice law in the State of New York and in a number of United States Federal Courts. I have set out my qualifications, experience and expertise at Appendix 1 hereto.

2. I was instructed by Ahern Rudden Quigley, solicitors for Mr Schrems, the Second Named Defendant in proceedings before the Irish High Court – *The High Court Record No 2016 4809P Between The Data Protection Commissioner, Plaintiff, and Facebook (Ireland) Limited and Maximilian Schrems, Defendants* – (the **"Irish Proceedings"**) to provide an expert opinion on certain matters regarding the laws of the United States of America.

3. I understand that my duty as an expert is to assist the Court as to matters within my field of expertise and that this overrides any duty or obligation that I may owe to the party by whom I have been engaged or to any party liable to pay my fees.

4. I confirm that neither I nor the ACLU, nor any person connected with me, has any financial or economic interest in any business or economic activity of the Second Named Defendant, other than any fee and expenses due in connection with my participation in the proceedings.

INTRODUCTION

5. I have been instructed by Ahern Rudden Quigley to opine on the legal frameworks governing U.S. government surveillance, whether that surveillance implicates Facebook users' communications and data, and the barriers to achieving redress for rights violations resulting from that surveillance. In the first part of this report, I discuss U.S. surveillance law and practice; in the second part, I discuss the barriers to redress.

6. Throughout my opinion, I refer to and rely on a number of U.S. laws, Judgments, an Executive Order, policies, and other documents concerning U.S. surveillance law, which I understand will be collated and indexed for the Court.

U.S. SURVEILLANCE LAW AND PRACTICE

7. The discussion below focuses on two of the most significant U.S. government surveillance authorities: Section 702 of the Foreign Intelligence Surveillance Act ("FISA") **(Tab #1)**, which authorizes warrantless surveillance that takes place on U.S. soil; and Executive Order ("EO") 12333 **(Tab #2)**, which authorizes warrantless electronic surveillance that largely takes place abroad.[1] After describing surveillance conducted under these two authorities, I discuss Presidential Policy Directive 28 ("PPD-28") **(Tab #3)**, a directive issued by President Barack H. Obama in 2014 that has resulted in modest but insufficient reforms to surveillance law.

8. In describing the parameters of surveillance conducted under Section 702 and EO 12333, I do not intend to imply that these surveillance authorities—or the government's

[1] Warrantless searches are "per se unreasonable under the Fourth Amendment [to the U.S. Constitution]—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967). The Supreme Court has interpreted the warrant clause in the Fourth Amendment to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate; (2) that those seeking the warrant demonstrate to the magistrate "probable cause"; and (3) that any warrant particularly describe the things to be seized as well as the place to be searched. *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). The U.S. government contends, incorrectly, that the 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. *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 **(Tab #4)**.

interpretation of these authorities—comply with the U.S. Constitution or the United States' international commitments. Indeed, the constitutionality of Section 702 and EO 12333 is deeply contested; however, 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.

9. In sum, under Section 702 and EO 12333, the U.S. government claims extraordinary access to the private communications and data of U.S. and non-U.S. persons around the world.[2] Although there are guidelines governing the collection, retention, and use of this information, the U.S. government maintains that it is authorized to engage in what is known as "bulk collection" when it is operating abroad. *See infra* ¶ 31. 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 overseas are extraordinarily low. *See infra* ¶¶ 14, 30. In addition, in order to locate communications to, from, and about its targets, the government routinely searches the contents of countless communications in bulk. To understand just how permissive current U.S surveillance law is, it helps to understand the constraints and safeguards that were historically put in place by the U.S. Congress in 1978 in the Foreign Intelligence Surveillance Act. Today, however, with respect to surveillance directed at non-U.S. persons located abroad, those safeguards have been eliminated.

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

10. In 1978, largely in response to congressional investigations of wrongful surveillance by U.S. intelligence agencies, Congress enacted FISA to regulate surveillance conducted for foreign intelligence purposes. The statute created a secret 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) **(Tab #5)**.

11. As originally enacted, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. *See id.* §§ 1805, 1809(a)(1). To obtain a FISA order, the government was required to 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). The FISC could issue an order authorizing surveillance only if it found that, among other things, there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and "each of the facilities or places at which the

[2] Throughout this affidavit, I use the phrase "U.S. persons" to refer to United States citizens and residents. I use the term "international" to describe communications that either originate or terminate outside the United States, but not both.

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).

12. The basic framework established by FISA, which I refer to below as "traditional" FISA, remains in effect today, but it has been significantly weakened by 2008 amendments to the statute that permit the acquisition of international communications without probable cause or individualized suspicion, as described below.

Section 702 of the Foreign Intelligence Surveillance Act

13. 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.[3] *See* 50 U.S.C. § 1881a **(Tab #1)**. 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 traditionally conducted under FISA, and it is subject to only a very limited form of judicial oversight.

14. 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. 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 counterterrorism. The statute defines "foreign intelligence information" broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e).

15. 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, *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) **(Tab #7)**, and consists principally of reviewing the general procedures the government proposes to use

[3] In August 2007, Congress passed a predecessor statute, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007), whose authorities expired in February 2008 **(Tab #6)**.

in carrying out the surveillance of tens of thousands of targets, *see* 50 U.S.C. § 1881a(i).[4] Before obtaining a Section 702 order, the government must provide to the FISC a written certification attesting that the FISC has approved, or that the government has submitted to the FISC for approval, both "targeting procedures" and "minimization procedures." 50 U.S.C. § 1881a(d)–(g). These procedures dictate, at a high level of generality, who may be targeted for surveillance by the executive branch and how communications are to be handled once intercepted. The role that the FISC plays under Section 702 bears no resemblance to the role it has traditionally played under FISA.[5]

16. Third and relatedly, unlike traditional FISA, Section 702 authorizes surveillance that is not predicated on the probable cause standard. When the government submits a Section 702 application to the FISC, it need not demonstrate that its 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. Further, 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, the government may direct its 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.[6] Because Section 702 requires neither particularity nor probable cause, the government can rely on a single FISC order to intercept the communications of countless individuals for up to a year at a time.

17. The statute itself contains no protections for the privacy of non-U.S. persons located abroad. To the extent the statute provides safeguards, these safeguards take the form of "minimization procedures." 50 U.S.C. §§ 1881a(e), 1801(h)(1). The statute's minimization requirements are supposed to protect against the collection, retention, and dissemination of

[4] Office of the Director of National Intelligence ("ODNI"), 2015 Statistical Transparency Report at 5 (Apr. 30, 2016), https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf (disclosing that the government targeted 94,368 different individuals, groups, and organizations under Section 702 in 2015) **(Tab #8)**.

[5] *See, e.g.*, Hearing of the Privacy and Civil Liberties Oversight Board ("PCLOB") at 31:27–32:28 (July 9, 2013), http://cs.pn/177IpII (statement of former FISC Judge James Robertson).

[6] 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") **(Tab #9)**.

U.S.-person communications that may be intercepted "incidentally" or "inadvertently." Significantly, however, these provisions include an exception that allows the government to retain communications of both U.S. and non-U.S. persons if the government concludes that they contain any information broadly considered "foreign intelligence." *Id.* §§ 1801(h), 1801(e).

18. Because the legal threshold for targeting non-U.S. persons is so low, and because the minimization requirements are so permissive, Section 702 effectively exposes every international communication—that is, every communication between an individual in the United States and a non-U.S. person abroad—to potential surveillance.[7]

The Government's Implementation of Section 702

19. The government has interpreted and implemented Section 702 broadly, relying on the statute to intercept and retain huge volumes of communications. In 2011, Section 702 surveillance resulted in the retention of more than 250 million communications—a number that does not reflect the far larger quantity of communications whose contents the NSA searched before discarding them.[8] In 2015, the government targeted the communications of 94,368 individuals, groups, and organizations under a single FISC order.[9] 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, they are subject to interception and retention by communications providers acting at the direction of the U.S. government.

[7] Recent 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. Last year, Yahoo, in response to a classified FISC order, apparently scanned hundreds of millions of email accounts for a "set of characters" or digital "signature" of a communications method purportedly used by a state-sponsored terrorist organization. The search was reportedly performed on all messages as they arrived at Yahoo's servers. *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, N.Y. Times, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, Oct. 5, 2016, http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html **(Tab #10)**.

[8] *See* [*Redacted*], No. [Redacted], 2011 WL 10945618, at *9–10 (FISC Oct. 3, 2011); PCLOB Report 111 n.476 **(Tab #11)**.

[9] ODNI, 2015 Statistical Transparency Report at 5.

20. As required by Section 702, the government has proposed targeting and minimization procedures and the FISC has approved them. Although these procedures are ostensibly meant to protect the privacy of U.S. persons, the procedures are weak and riddled with exceptions. By design, they give the government broad latitude to analyze and disseminate both U.S. and non-U.S. persons' communications.

21. Although the government has not made public its Section 702 targeting procedures,[10] it has published partially redacted versions of its Section 702 minimization procedures for the NSA, FBI, CIA, and National Counterterrorism Center.[11] These procedures provide the government with broad authority to retain, analyze, and use the data it has collected. 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.[12] During that time, the communications may be reviewed and queried by analysts in both intelligence and criminal investigations.

22. Official government disclosures show that the government uses Section 702 to conduct at least two types of surveillance: "PRISM" and "Upstream" surveillance.[13] Given the broad parameters of Section 702, the government may rely on the statute to conduct other surveillance programs as well.

---

[10] *See* 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 (July 2014), https://www.dni.gov/files/documents/0928/NSA%20Section%20702%20Targeting%20Procedures.pdf (redacting the body of the text in its entirety) **(Tab #12)**.

[11] *See* ODNI, IC on the Record, *Release of 2015 Section 702 Minimization Procedures*, (Aug. 11, 2016), https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization **(Tab #13)**.

[12] The default retention period for PRISM collection is five years, and two years for Upstream collection. *See* 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 (July 2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf. These two distinct methods of Section 702 surveillance are discussed in greater detail below **(Tab #14)**.

[13] *See* PCLOB Report 33–41 **(Tab #15)**.

23. Government disclosures and media reports indicate that PRISM surveillance involves the acquisition of communications content and metadata directly from U.S. companies like Facebook, Google, and Microsoft.[14] The government identifies the user accounts it wishes to monitor, and then collects from the provider all communications to or from those accounts, including any and all communications with U.S. persons. As of April 2013, the NSA was monitoring at least 117,675 targeted accounts via PRISM.[15]

24. The disclosures by former NSA contractor Edward Snowden and related media reports indicate that Facebook is one of the internet service providers compelled to participate in PRISM. According to one publicly released NSA slide, Facebook began participating in PRISM on June 3, 2009.[16]

25. Government disclosures and media reports indicate that Upstream surveillance, which the government claims is authorized by Section 702, involves the mass copying and searching of Internet communications flowing into and out of the United States. With the help of 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 U.S. persons and others around the world. There, the NSA searches the metadata and content of international Internet communications for key terms, called "selectors," that are associated with its tens of thousands of foreign targets. (Selectors used in connection with this particular form of surveillance are identifiers such as email addresses or phone numbers.) Communications containing 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. Thus, through Upstream surveillance, the NSA has generalized access to the content of communications, as it indiscriminately copies and searches through vast quantities of personal metadata and content.[17]

---

[14] *See id.* 33–34; [*Redacted*], 2011 WL 10945618, at *9 & n.24; *NSA Program Prism Slides*, The Guardian, Nov. 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document **(Tab #16)**.

[15] *See NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post, July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ **(Tab #17)**.

[16] *See id.*

[17] *See, e.g.*, PCLOB Report 35–39, 41, 111 n.476; [*Redacted*], 2011 WL 10945618, at *10–11 (FISC Oct. 3, 2011).

26. Based on the public information concerning the scope of Upstream surveillance, I believe that there is a substantial likelihood that this surveillance results in the NSA's accessing, copying, and searching of data transmitted from Facebook Ireland to Facebook in the United States. While some or all of this data may be encrypted, that would not prevent the NSA from copying, examining, and seeking to decrypt the intercepted Facebook data. As noted in paragraph 21 above, 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.[18]

EXECUTIVE ORDER 12333

27. EO 12333 is the primary authority under which the NSA gathers foreign intelligence.[19] It provides broad latitude for the government to conduct surveillance on U.S. and non-U.S. persons alike—without any form of judicial review or the limitations that apply to surveillance conducted under Section 702. Electronic surveillance under EO 12333 is largely conducted outside the United States.[20] 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") **(Tab #19)** and other agency policies.[21] In addition, as discussed in greater detail below, PPD-28 and its associated agency policies further regulate EO 12333 activities.

28. 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,

---

[18] *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 **(Tab #18)**.

[19] EO 12333, as amended, *available at* https://www.dni.gov/index.php/about/organization/ic-legal-reference-book/ref-book-eo-12333.

[20] *See* John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, http://wapo.st/2bnOU39 **(Tab #20)**.

[21] *See* National Security Agency, USSID 18 (Jan. 25, 2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf; *see also* Office of the Director of National Intelligence, *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) **(Tab #21)**.

with particular emphasis on countering terrorism, espionage, and weapons of mass destruction.[22] EO 12333 is used to justify surveillance for a broad range of purposes, discussed below, resulting in the 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.

29. Despite its breadth, surveillance under EO 12333 has not been subject to meaningful oversight by either the U.S. Congress or U.S. courts. Surveillance programs operated under EO 12333 have never been reviewed by any court. Moreover, these programs are not governed by any statute, including FISA, and, as the former Chairman of the Senate Intelligence Committee has conceded, they are not overseen in any meaningful way by Congress.[23]

30. 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 abroad for the purpose of collecting "foreign intelligence"—a term defined so broadly that it appears to permit surveillance of any non-U.S. person, including surveillance of their communications with U.S. persons.[24]

31. In addition, the order and its implementing regulations permit at least two forms of bulk surveillance.[25] First, they permit the government to engage in what is sometimes termed "bulk collection"—that is, the indiscriminate collection of electronic communications or data. As explained further below, existing policies state that the U.S. government will *use* data collected in bulk for only certain broadly defined purposes.[26] But there is no question that these policies permit collection of electronic communications in bulk. Thus, these

[22] *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 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.").

[23] 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 **(Tab #22)**.

[24] *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").

[25] *See, e.g.*, USSID 18 § 4 **(Tab #23)**.

[26] National Security Agency, PPD-28 Section 4 Procedures § 5 (Jan. 12, 2015), *available at* https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf ("NSA PPD-28 Section 4 Procedures") **(Tab #24)**.

policies plainly contemplate "access on a generalized basis to the content of electronic communications." *Schrems v. Data Protection Commissioner* (C-362/14).

32. Second, the order and its implementing regulations allow what can be termed "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 looks 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. Indeed, unlike the selectors the government claims to use under Section 702's Upstream surveillance, EO 12333 procedures permit selectors that are not associated with particular targets (such as an email address or phone number). Thus, it appears that the government can use selectors likely to result in the collection of even larger amounts of information, such as the names of countries or political figures.

33. Indeed, even "targeted" forms of EO 12333 surveillance are extremely permissive, as the executive order authorizes the government to target non-U.S. persons abroad for virtually any "foreign intelligence" reason, broadly defined. *See* EO 12333 § 3.5(e).

34. EO 12333 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;[27] (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 may also retain data if it determines in writing that retention is in the broad "national security interest" of the United States. Information in categories (2), (3), and (4), including identifiers of a specific U.S. or non-U.S. person, may be disseminated for use throughout the government.

The Government's Implementation of EO 12333

35. 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

[27] The default five-year age-off is triggered when this data is in intelligible form. *See* NSA PPD-28 Section 4 Procedures § 6.1(a) **(Tab #25)**.

collection of billions of cell-phone location records each day;[28] its recording of every single cell phone call into, out of, and within at least two countries;[29] and its surreptitious interception of data from Google and Yahoo user accounts as that information travels between those companies' data centers located abroad.[30]

36. 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.[31] 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." [32]

37. In addition to the U.S. government's Section 702 collection of Facebook users' communications and data, media reports indicate that the NSA collects Facebook users' communications and data under EO 12333 as well. For example, under this authority, the NSA has collected hundreds of millions of contact lists and address books from personal email and instant-messaging accounts—including contact lists from Facebook accounts.[33]

---

[28] 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 **(Tab #26)**.

[29] Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, The Guardian, May 19, 2014, https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ **(Tab #27)**.

[30] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Do cuments 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 **(Tab #28)**.

[31] Ryan Gallagher, *How Secret Partners Expand NSA's Surveillance Dragnet*, The Intercept, June 18, 2014, https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ **(Tab #29)**.

[32] 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 ¶ 75, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf ("Commission Implementing Decision") **(Tab #30)**.

[33] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post, Oct. 14, 2013, http://www.washingtonpost.com/world/national-

Numerous other Snowden disclosures describe the collection or analysis of information from Facebook users.[34]

PPD-28

38. 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.

39. 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 next U.S. President.

---

security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html. The document describing the collection of data from Facebook is available at http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/ **(Tab #31)**.

[34] *See, e.g.*, Glenn Greenwald & Ryan Gallagher, *Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and its Supporters*, The Intercept, Feb. 18, 2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/. A document released in conjunction with this article states that "NSA may target via EO 12333 a DNI selector which is confirmed foreign. (Source #003) Okay to use [XKeyscore, a tool that allows analysts to examine data collected under Section 702 and EO 12333] micro-plugins (for example) that query against Facebook. GMail. Twitter, etc. IF screename/username is believed to be foreign." *Discovery SIGINT Targeting Scenarios and Compliance*, https://theintercept.com/document/2014/02/18/discovery-sigint-targeting-scenarios-compliance/. *See also* Morgan Marquis-Boire, Glenn Greenwald & Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications*, The Intercept, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/, and associated documents referencing Facebook, *available at* https://theintercept.com/document/2015/07/01/full-log-vs-http/; https://theintercept.com/document/2015/07/01/intro-xks-appids-fingerprints/; https://theintercept.com/document/2015/07/01/tracking-targets-online-social-networks/; Jacob Appelbaum, Marcel Rosenbach, Jörg Schindler, Holger Stark & Christian Stöcker, *NSA "Quantum Theory" Program: How the US Hacked Computers Worldwide*, Der Spiegel, Dec. 30, 2013, http://www.spiegel.de/netzwelt/netzpolitik/quantumtheory-wie-die-nsa-weltweit-rechner-hackt-a-941149.html, and an associated document referencing Facebook, *available at* http://www.spiegel.de/fotostrecke/nsa-dokumente-so-knackt-der-geheimdienst-internetkonten-fotostrecke-105326.html **(Tab #32)**.

PPD-28's Principles

40. The broad principles articulated in PPD-28 include the following:
    - The U.S. 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.[35]
    - The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the U.S. or its partners and allies.[36]
    - Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the U.S. shall consider the availability of other information, including from diplomatic and public sources.[37]
    - All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.[38]

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

Bulk Collection

42. PPD-28 provides that when the U.S. 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 U.S. and its interests;
    - threats to the U.S. and its interests from terrorism;
    - threats to the U.S. 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

[35] PPD-28 § 1(b).

[36] *Id.* § 1(c).

[37] *Id.* § 1(d).

[38] *Id.* § 4.

- transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes above.

43. Taken together, these categories are very broad and open to interpretation, and they effectively ratify the practice of bulk, indiscriminate surveillance.

44. 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 described in paragraph 32 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.)."[39] This definition explicitly excludes data that is "temporarily acquired to facilitate targeted collection."[40] In other words, these restrictions on use do not apply to data that is acquired in bulk and held for a short period of time, such as data copied and searched in bulk using Upstream surveillance under Section 702.

Retention, Dissemination, and Use

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

46. 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.[41] Similarly, the government may disseminate 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.[42]

47. 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

[39] *Id.* § 2 n.5.

[40] *Id.*

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

[42] PPD-28 § 4(a)(i).

information constitutes "foreign intelligence," or the information is obtained in the course of a lawful foreign intelligence investigation.[43]

48. 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.[44]

OBSTACLES TO REDRESS

49. Below, I discuss ways in which the U.S. government routinely seeks to prevent individuals from obtaining redress for Section 702 and EO 12333 surveillance through civil litigation in U.S. courts. I also briefly address two other purported redress mechanisms recently highlighted by the U.S. government in the Privacy Shield agreement.

GOVERNMENT DEFENSES: STANDING AND STATE SECRETS DOCTRINES

50. 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.

51. First, because virtually none of the individuals who are subject to either Section 702 or EO 12333 surveillance ever receive notice of that surveillance, it is exceedingly difficult to establish what is known as "standing" to challenge the surveillance in U.S. court.[45] Without

[43] 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.)

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

[45] The U.S. government's position is that it generally has no obligation to notify the targets of its foreign-intelligence surveillance, or the countless others whose communications and data have been seized, searched, retained, or used in the course of this surveillance. 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. 50 U.S.C. § 1801(k). In those circumstances, the government is statutorily required to provide notice. *See, e.g.*, 50 U.S.C. § 1806; *see also* Gov. Response in

standing to sue, a plaintiff cannot litigate the merits of either constitutional or statutory claims.

52. 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) **(Tab #33)**. 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)). A plaintiff must eventually establish these three elements of standing by a preponderance of the evidence. *See id.* at 2342.

53. Because Section 702 and EO 12333 surveillance is 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 International USA*, 133 S. Ct. 1138, 1148 (2013) **(Tab #34)**.

54. The ACLU is currently representing nine human rights, legal, media, and educational organizations—including Wikimedia, operator of one of the most-visited websites in the world—in another civil challenge to Section 702 surveillance. In October 2015, a U.S. district court dismissed this suit on the grounds that the plaintiffs lacked standing. *See Wikimedia Found. v. National Security Agency*, 143 F. Supp. 3d 344, 356 (D. Md. 2015) **(Tab #35)**. In particular, the court held that Wikimedia had not plausibly alleged that any of its international communications—more than one trillion per year—were in fact subject to Upstream surveillance. The ACLU has appealed the case, and we hope that the district court's opinion will be overturned. Nevertheless, the district court's opinion illustrates the

---

Opp. to Def's Mot. for Notice & Discovery of Surveillance, *United States v. Thomas*, No. 2:15-cr-00171-MMB (E.D. Pa. July 29, 2016), at 7–8 (arguing that a criminal defendant seeking information about government surveillance is not entitled to notice of EO 12333 surveillance). Notably, however, the government has refused to disclose its interpretation of what constitutes evidence "derived from" FISA. To date, only eight criminal defendants have received notice of Section 702 surveillance, despite the U.S. government's collection of hundreds of millions of communications under that authority.

difficulties that plaintiffs face in establishing standing, even at the outset of a case, when a plaintiff's allegations must merely be plausible.

55. Second, courts hearing civil suits have agreed with the government's invocation of the "state secrets privilege," preventing those 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 that disclosure of that specific information would cause harm to national security. *See United States v. Reynolds*, 345 U.S. 1 (1953) **(Tab #36)**. In recent years, however, the government has increasingly sought to use 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) **(Tab #37)**. Although courts have held that FISA preempts the application of the state secrets privilege for FISA-related claims, *see, e.g.*, *Jewel v. National Security Agency*, 965 F. Supp. 2d 1090, 1105 (N.D. Cal. 2013), the government has nevertheless raised the privilege in challenges to Section 702 surveillance, *see, e.g.*, *Jewel v. National Security Agency*, 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) **(Tab #38)**.[46]

56. 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.

GOVERNMENT DEFENSE: APPLICABILITY OF THE U.S. CONSTITUTION TO NON-U.S. PERSONS ABROAD

57. The U.S. government has taken the position that non-U.S. persons located abroad 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." Supp. Br. of Plaintiff–Appellee at 12, *United States v. Mohamud*, No. 14-30217 (9th Cir. Oct. 3, 2016). The government bases this

[46] Notably, the only individuals who have ever obtained a ruling on the merits in a challenge to Section 702 surveillance are three criminal defendants who received notice of that surveillance.

argument on *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), 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. *See id.* at 261–62, 273. 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.

OTHER "REDRESS" MECHANISMS HIGHLIGHTED BY THE GOVERNMENT

Freedom of Information Act

58. The Freedom of Information Act is not a form of redress per se; rather, the U.S. Congress enacted this law to provide transparency to the public about U.S. government activities. *See* 5 U.S.C. § 552 **(Tab #39)**. However, because the 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.

59. 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 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 Guantanamo 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) **(Tab #40)**.

Privacy Shield Ombudsperson

60. Earlier this year, 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.[47] But the Ombudsperson's legal authority and ability to provide meaningful redress are severely limited.

[47] *See* E.U.–U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g **(Tab #41)**.

61. 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, executive 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."[48] However, even where the Ombudsperson does find 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.

62. The Ombudsperson's authority is restricted in other ways as well. Most importantly, there is no indication that the Ombudsperson can in fact require an executive-branch agency to implement a particular remedy. Nor is there any indication that she 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 Privacy and Civil Liberties Oversight Board ("PCLOB"), *see* Commission Implementing Decision ¶ 120, neither the Inspectors General nor the PCLOB can issue recommendations that are binding on the executive branch.[49] Moreover, the Ombudsperson cannot respond to any general claims that the Privacy Shield agreement is inconsistent with E.U. data protection laws. Finally, because the Ombudsperson is part of the State Department, this position is not entirely independent from the intelligence community.[50]

63. In short, an individual who complains to the Ombudsperson is extremely unlikely to ever learn how his complaint was analyzed, or how any non-compliance was in fact remedied. He also lacks the ability to appeal or enforce the Ombudsperson's decision.

---

[48] *See id.* § 4(e).

[49] Each element of the Intelligence Community has an Office of the Inspector General with responsibility for oversight of various matters, including foreign intelligence activities. *See* Letter, Robert S. Litt, Office of the Director of National Intelligence, Office of General Counsel, to Justin S. Antonipillai, Counselor, U.S. Dep't of Commerce, and Mr. Ted Dean, Deputy Asst. Secretary, Int'l Trade Admin., at 7–8 (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F **(Tab #42)**.

[50] *See* Office of the Director of National Intelligence, *Intelligence Community*, https://www.dni.gov/index.php (listing 17 agencies and organizations, including the State Department, that comprise the intelligence community) **(Tab #43)**.

CONCLUSION

64. In summary, U.S. surveillance law is extremely permissive, as the government claims broad authority to acquire the communications and data of non-U.S. persons located abroad. For the vast majority of individuals subject to Section 702 and EO 12333 surveillance, there has to date been no viable avenue to obtain meaningful redress for the rights violations resulting from this surveillance.

APPENDIX 1

EXPERTISE OF THE EXPERT

1. I received my Bachelor of Arts degree from Yale University and my Juris Doctor degree 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. Upon completion of my clerkship with Judge Newman, I joined the ACLU's National Security Project, where I am currently an attorney.

2. The ACLU is a U.S. nationwide, non-profit, nonpartisan organization with more than 500,000 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.

3. As an attorney at the ACLU's National Security Project, I have developed significant expertise in U.S. surveillance law through litigation, advocacy, and public education efforts. My work largely involves litigating civil and criminal challenges to the lawfulness of government surveillance under Section 702 of the Foreign Intelligence Surveillance Act. I am also the lead attorney in a Freedom of Information Act lawsuit seeking key legal interpretations and regulations governing one of the U.S. government's primary surveillance authorities, Executive Order 12333. In addition to my litigation practice, I regularly discuss government surveillance in various media outlets and before public audiences. For example, in September 2016, I provided expert testimony on U.S. surveillance law and practice to the German Bundestag's First Committee of Inquiry, which is tasked with investigating NSA surveillance in the wake of the disclosures by Edward Snowden.

THE HIGH COURT

Record No: 2016/4809 P

Between:

THE DATA PROTECTION COMMISSIONER

Plaintiff

-AND-

FACEBOOK IRELAND LIMITED

-AND-

MAXIMILLIAN SCHREMS

Defendants

EXPERT REPORT OF ASHLEY GORSKI
ON BEHALF OF THE SECOND NAMED DEFENDANT
