

July 25, 2019

Bruno Gencarelli
Head of Unit
European Commission
Directorate—General Justice and Consumers
Unit C.4: International Data Flows and Protection
Brussels, Belgium

**Re: The European Commission’s Annual Review of the E.U.–
U.S. Privacy Shield**



Washington Legislative
Office
915 15th Street, 6th FL
Washington DC 20005
T: 202-544-1681
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
*National Political
Director*

Dear Mr. Gencarelli,

We write in response to your invitation for the American Civil Liberties Union (“ACLU”) to provide input concerning the E.U.–U.S. Privacy Shield, recent developments in the U.S. legal framework, and potential U.S. privacy legislation.

Previously, the ACLU has expressed its view that reforms of Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) and Executive Order 12,333 are necessary to ensure that E.U. data transferred to the United States receives protections “essentially equivalent” to the protections required under the E.U. Charter.¹ It continues to be the ACLU’s position that U.S. surveillance laws and practices do not meet E.U. standards.

Recent Legal Developments

Since the ACLU’s last correspondence with the Commission, U.S. courts have issued several noteworthy rulings related to U.S. government secrecy and judicial redress for privacy violations:

- *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202 (9th Cir. 2019). In *Fazaga*, three plaintiffs alleged that the FBI paid a confidential informant to conduct a covert surveillance program that gathered information about Muslims based solely on their religious identity. *Id.* at 1210. The district court dismissed all but one of the plaintiffs’ claims on the basis of the

¹ See, e.g., Letter from ACLU to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission (Nov. 20, 2018) (attached as Exhibit A); Letter from ACLU to Bruno Gencarelli, Head of Unit, European Commission (Aug. 15, 2018), <https://www.aclu.org/letter/aclu-letter-european-commission-re-european-commissions-annual-review-eu-us-privacy-shield> (attaching prior letters) (attached as Exhibit B).

state secrets privilege—an evidentiary privilege that the government invokes to withhold evidence from litigation where disclosure would create what the government asserts is an unacceptable risk of harm to national security. *Id.* at 1215. Specifically, the district court held that because the government defendants would need to rely on privileged material to present their defenses, and because further litigation would impermissibly risk disclosure of privileged material, the majority of the plaintiffs’ claims could not proceed. *Id.* The Court of Appeals for the Ninth Circuit reversed the district court’s decision with respect to several claims. *Id.* at 1211. Two aspects of the Ninth Circuit’s holding are relevant here.

First, the Ninth Circuit held that FISA’s in camera, ex parte procedure for reviewing evidence, set forth at 50 U.S.C. § 1806(f), displaces the state secrets evidentiary privilege. *Id.* at 1226, 1230 & n.25. In other words, in cases involving purported state secrets and FISA claims, the government should not be permitted to withhold privileged evidence from the litigation altogether, and must instead submit that evidence to the court for in camera and ex parte review. *Id.* at 1211, 1226, 1230 & n.25. However, as discussed below, it remains to be seen how other courts will apply the Ninth Circuit’s holding. It also bears emphasis that the Ninth Circuit did not rule on whether FISA’s in camera, ex parte review procedure applies when the state secrets privilege is invoked as a complete bar to the justiciability of a case. *See id.* at 1230 & n.25.

Second, the Ninth Circuit held that the plaintiffs adequately alleged that FBI agents unlawfully planted recording devices in a home and an office in violation of 50 U.S.C. § 1810. *Id.* at 1225. The Commission has previously cited Section 1810 as one of the potential remedies theoretically available to E.U. persons whose privacy rights are violated by U.S. government surveillance. Critically, however, the Ninth Circuit’s opinion provides no basis for concluding that E.U. persons seeking to challenge Section 702 surveillance could obtain a remedy under Section 1810 because the U.S. will likely argue that a remedy is not available if that surveillance was authorized by the FISC. *See* 50 U.S.C. § 1810; *see also id.* § 1809(b) (“It is a defense . . . that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a . . . court order of a court of competent jurisdiction.”).

The government has petitioned the Ninth Circuit to rehear *Fazaga* en banc. It asserts that the Ninth Circuit panel erred in holding that FISA displaces the state secrets privilege.

- *Jewel v. National Security Agency*, No. 08-cv-04373-JSW (N.D. Cal. Apr. 25, 2019). In *Jewel*, the district court granted the government’s motion for summary judgment on claims concerning NSA surveillance, holding that the plaintiffs failed to establish standing as a factual matter. *Id.* at 18. The court further

concluded that even if the public evidence proffered by the plaintiffs were sufficient to establish standing, the issue could not be adjudicated without risking the disclosure of state secrets. *Id.* at 18, 25. Although the court recognized that, per the Ninth Circuit’s holding in *Fazaga*, FISA displaces the state secrets privilege, and although the court had applied FISA’s procedures to review secret evidence in camera, it nevertheless dismissed the case on state secrets grounds. *Id.* at 4, 6, 25. In other words, the government successfully invoked the standing doctrine and the state secrets privilege to prevent adjudication of the merits of the plaintiffs’ surveillance claims—notwithstanding the Ninth Circuit’s ruling in *Fazaga*. The district court’s opinion illustrates the ways in which the standing and state secrets doctrines continue to function as substantial obstacles to judicial redress.

The plaintiffs have appealed the district court’s ruling to the Ninth Circuit.

- *ACLU v. National Security Agency*, 925 F.3d 576 (2d Cir. 2019). In *ACLU*, the plaintiffs brought a Freedom of Information Act (“FOIA”) suit seeking documents concerning the U.S. government’s surveillance powers under Executive Order 12,333. Following extensive litigation in the district court, the plaintiffs appealed the district court’s decision to uphold the government’s claimed exemptions over seven key legal memoranda. *Id.* at 588, 600. The plaintiffs argued that because these memoranda contained the effective law and policy of the executive branch, they could not be withheld as “privileged” under FOIA. For example, as the plaintiffs argued, one memorandum at issue provided the legal basis for continued reauthorizations of President George W. Bush’s warrantless wiretapping program. *Id.* at 585. The Court of Appeals for the Second Circuit disagreed, holding that each of the memoranda could be withheld under various FOIA exemptions. *Id.* at 584. As the decision shows, FOIA is not a reliable means to obtain information about the effective law and policy governing U.S. surveillance—let alone information about whether U.S. surveillance has implicated the personal data of a particular individual.

Federal Legislative Developments

- *Commercial Privacy Legislation*: Congress is actively debating federal commercial privacy legislation, but has yet to pass comprehensive privacy laws. Thus, the U.S. lacks a comprehensive privacy framework that is analogous to the European Union’s General Data Protection Regulation (GDPR). The California Consumer Privacy Act (CCPA)², which is applicable only to certain entities that do business in California, is slated to go into effect in 2020. However, CCPA is only applicable to entities that do business in the state of California.

² Cal. Civ. Code § 1798.100 – 1798.199.

- *National Security Surveillance*: Provisions of the Patriot Act, including Section 215, which was used for a program that collected the call records of virtually everyone in the U.S., are set to expire at the end of 2020. Congress will either need to extend, modify, or let these provisions lapse. It is unclear whether the Patriot Act debate will impact other surveillance powers.

If you have questions, please feel free to contact Ashley Gorski (agorski@aclu.org) or Neema Singh Guliani (nguliani@aclu.org).

Sincerely,



Ronald Newman
National Political Director



Neema Singh Guliani
Senior Legislative Counsel



Ashley Gorski
Staff Attorney, National Security Project

Exhibit A

November 20, 2018

Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission

Dear Commissioner Jourová:

We have written to you previously regarding our concerns that Privacy Shield fails to ensure that E.U. data transferred to the United States receives protections “essentially equivalent” to those provided under the E.U. Charter.¹ We write to provide information regarding two recent developments that reinforce this concern:

- Insufficient Staffing of the Privacy and Civil Liberties Board: Congress has only confirmed three of the five nominees to the Privacy and Civil Liberties Board (“PCLOB”), leaving the board with an unbalanced quorum of three Republican nominated members to one Democratic nominated member. Moreover, the term of the Democratic nominee is set to expire early next year. As currently constituted, the board does not have balanced representation from both parties, which Congress intended to ensure that it operated in a fair and balanced manner.
- Inadequacy of Presidential Policy Directive (PPD)-28: The recent disclosure of the PCLOB’s PPD-28 report confirms that the directive’s protections for non-U.S. persons are extremely weak. In addition, it appears that the government has not taken sufficient steps to address deficiencies in PPD-28’s implementation.

PCLOB Staffing

The Privacy Shield arrangement rested in part on assertions by the U.S. government that the PCLOB provided strong oversight of U.S. surveillance practices. We have previously written to you raising concerns that the PCLOB is insufficient to ensure appropriate oversight of U.S. surveillance programs or ensure appropriate redress for E.U. residents. Recent actions further call into question whether the PCLOB can sufficiently and fairly perform oversight functions.

In October 2018, the Senate confirmed Adam Klein, Edward Felten, and Jane Nitze to the PCLOB. These members joined board member Elisebeth Collins.² The Senate has yet to take steps to have hearings or confirm the additional two nominees, one of whom is intended to replace Ms. Collins. This existing makeup of the board raises several concerns. First, the

¹ See Letter from ACLU to Bruno Gencarelli, Head of Unit, European Commission (August 15, 2018), https://www.aclu.org/sites/default/files/field_document/final_letter_pdf_with_attached_exhibits_a-d_2.pdf (attaching prior letters as Exhibits A–C).

² See PCLOB Press Release, *New PCLOB Board Members Release Joint Statement* (Oct. 18, 2008), <https://www.pclob.gov/newsroom/2018/10/18/Board-Members-Release.html>

current makeup leaves the board unbalanced with three Republican and only one Democratic nominee. This fails to reflect the intent of Congress, which was to ensure that the PCLOB had adequate representation of nominees from both parties. Second, the board's sole Democrat nominee's term is set to expire early next year. Thus, without additional action from Congress, the board could have a quorum without any Democratic nominees. Such a makeup would call into question the bipartisan legitimacy of oversight activities of the board, and make it vulnerable to partisan oversight.

PPD-28 Implementation

In October 2018, the U.S. government publicly released the PCLOB report on implementation of PPD-28 ("PCLOB Report").³ The report makes clear that PPD-28's protections are weak in practice and rife with exceptions. Moreover, it appears that the U.S. government has still not taken sufficient steps to implement the PCLOB's recommendations to address these concerns.

The PCLOB Report confirms just how modest the directive's privacy protections actually are. It states that in large part, PPD-28 simply prompted the intelligence community to memorialize its existing practices. For example, the PCLOB Report explains that, "[p]rior to the issuance of PPD-28, as a practical matter NSA's use of signals intelligence collected in bulk was *already limited* to the six . . . purposes" set forth in Section 2 of PPD-28.⁴ These purposes under PPD-28 include the problematic use of information collected in "bulk" for detecting and countering broad categories of activities, including cybersecurity threats and transnational crime.⁵ The report goes on to note that the "NSA's general querying standards have not changed as a result of PPD-28."⁶

The report also raises concerns that even the limited protections in the directive have not been applied consistently. The report states that "the lack of a common understanding as to the activities to which PPD-28 applies has led to inconsistent interpretation and could lead to compliance traps, especially as [intelligence community] elements engage in information sharing."⁷ One example is the FBI's approach to communications collected under the Foreign Intelligence Surveillance Act ("FISA"). The report raises questions about whether the FBI is fully complying with PPD-28, as well as whether it is seeking to carve out certain surveillance

³ Privacy & Civil Liberties Oversight Board, *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities* (December 2016), available at https://www.aclu.org/sites/default/files/field_document/ppd-28_report_for_foia_release.pdf ("PCLOB Report").

⁴ PCLOB Report at 6.

⁵ PPD-28 § 2, available at <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

⁶ *Id.* Notably, PPD-28's limitations on the use of information collected in "bulk" do not apply to data 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. See PPD-28 § 2 n.5 (defining "bulk" to exclude data that is "temporarily acquired to facilitate targeted collection").

⁷ PCLOB Report at 13.

activities from the directive’s modest requirements. It states that the “FBI applies PPD-28 to communications collected under Section 702 of FISA, but exempts communications collected under FISA Title I or Sections 702 and 705(b) of FISA. FBI’s rationale is that PPD-28 should not apply to the latter FISA activities because those surveillances require an individualized finding of probable cause.”⁸ However, this factor should have no bearing on the applicability of PPD-28.

To address these inconsistencies, the PCLOB recommended that the National Security Council and the Office of the Director of National Intelligence (“ODNI”) “issue criteria for determining which activities or types of data will be subject to PPD-28’s requirements.”⁹ It appears that, nearly two years later, ODNI still has not issued any such criteria.¹⁰

With respect to the storage and dissemination of communications, the PCLOB Report also highlights the ways in which the rules implementing PPD-28 do not extend the same protections to foreigners as to U.S. persons—contrary to the findings of the European Commission in its adequacy decision.¹¹ For example, the “NSA’s PPD-28 procedures state that the NSA may include [the personal information of non-U.S. persons] in reporting if it is ‘related to an authorized foreign intelligence requirement.’ This standard differs from the standard that governs dissemination of [U.S. person information]: [U.S. person information] may be disseminated if doing so is ‘necessary to understand the foreign intelligence information or assess its importance.’”¹² The PCLOB Report identified differing standards for the CIA’s dissemination of U.S. and non-U.S. person information as well.¹³

Finally, it remains unclear how PPD-28 will be applied to new forms of information sharing that have been authorized. Historically, the NSA had reviewed and redacted some types of sensitive personal information from the communications it intercepted before sharing selected intercepts and intelligence reports with other agencies. However, in 2016, the U.S. government implemented new rules that allowed the NSA to broadly share raw information, including with agencies that had no prior experience handling this kind of intelligence. The PCLOB explained that these agencies and components of agencies may need to take additional measures—including updating information systems, providing additional training, or adopting additional

⁸ PCLOB Report at 13.

⁹ PCLOB Report at 13–14.

¹⁰ See ODNI, Status of Implementation of PPD-28: Response to the PCLOB’s Report 4–5 (Oct. 2018) (“ODNI Response Report”), <https://bit.ly/2DepCEr> (stating that Section 702 is subject to the requirements of PPD-28, but omitting any reference to official criteria for determining what other activities are subject to the directive).

¹¹ 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* ¶ 85 (2016).

¹² PCLOB Report at 10–11.

¹³ See *id.*

guidance—to comply with the directive.¹⁴ Although the NSA has not yet relied on these new rules to grant other agencies access to raw signals intelligence,¹⁵ it is unclear whether the PCLOB’s concerns will be fully addressed before the raw information-sharing begins. Specifically, it is unknown whether agencies have appropriately updated their information technology systems, or whether agency personnel have received the training necessary to comply with PPD-28.

We urge you to consider these issues as you assess the adequacy of the Privacy Shield. If you have additional questions, please contact Neema Singh Guliani (nguliani@aclu.org) or Ashley Gorski (agorski@aclu.org).

Sincerely,



Neema Singh Guliani
Legislative Counsel
American Civil Liberties Union



Ashley Gorski
Staff Attorney, National Security Project
American Civil Liberties Union



Amie Stepanovich
U.S. Policy Manager, Global Policy Counsel
Access Now

cc:

Claude Moraes
Chairman, Committee on Civil Liberties, Justice and Home Affairs (LIBE)
European Parliament

¹⁴ PCLOB Report at 16–18.

¹⁵ See ODNI Response Report at 7.

Andrea Jelenik
Director
European Data Protection Board

Bruno Gencarelli
Head of Unit
European Commission

Exhibit B

August 15, 2018

Bruno Gencarelli
Head of Unit
European Commission
Directorate-General Justice and Consumers
Unit C.4: International Data Flows and Protection
Brussels, Belgium



Re: The European Commission’s Annual Review of the E.U.–U.S. Privacy Shield

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2644
Fax: (212) 549-2644
aclu.org

Susan N. Herman
President

Anthony D. Romero
Executive Director

Richard Zacks
Treasurer

Dear Mr. Gencarelli,

We write in response to your invitation for the American Civil Liberties Union (“ACLU”) to provide input concerning the E.U.–U.S. Privacy Shield, recent developments in the U.S. legal framework, and the functioning of the redress and review mechanisms discussed in the European Commission’s July 2016 Privacy Shield adequacy decision (“Adequacy Decision”).¹

Previously, the ACLU has expressed its view that reforms to Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12,333 are necessary to ensure that E.U. data transferred to the United States receives protections “essentially equivalent” to the protections required under the E.U. Charter.² Recent developments, including passage of legislation that could be relied on by the U.S. government to expand surveillance practices, further support the ACLU’s belief that U.S. surveillance laws and practices do not meet E.U. standards. Because the United States fails to provide an adequate level of

¹ 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* (2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

² See Letter from ACLU to Bruno Gencarelli, Head of Unit, European Commission (June 30, 2017), https://www.aclu.org/sites/default/files/field_document/european_commission_privacy_shield_response.pdf (attached as Exhibit A); Letter from ACLU & Human Rights Watch to Vera Jourová, Commissioner for Justice, Consumers & Gender Equality, European Commission (Feb. 28, 2017), https://www.aclu.org/sites/default/files/field_document/aclu_hrwh_letter_to_eu_re_privacy_shield_and_eu_us_umbrella_agreement_02-28-2017.pdf (attached as Exhibit B); Letter from ACLU to Isabelle Falque Pierrotin, Chairwoman of Working Party 29 (Jan. 5, 2016), https://www.aclu.org/sites/default/files/field_document/aclu_letter_to_isabelle_pierrotin.pdf (attached as Exhibit C).

protection for E.U.-person data, the Privacy Shield agreement should not stand.

In Part I, we briefly address four of the key errors in the Adequacy Decision—errors that were replicated in the Commission’s first annual review of the functioning of Privacy Shield. In Part II, we review recent developments that undermine the U.S. government assertions that formed the foundation of the Privacy Shield agreement. In Part III, we specifically address questions regarding safeguards to protect consumers from automated decision-making.

Summary of Key Errors in the Adequacy Decision

Below, we briefly address four of the key errors in the Commission’s Adequacy Decision, with cross-references to the expert report that we recently submitted in a pending legal challenge to Privacy Shield, *La Quadrature du Net contre Commission Européenne* (Affaire T-738/16). That report, referred to herein as the “ACLU Expert Report” and attached as Exhibit D to this letter, discuss these issues in greater detail.

A. U.S. foreign intelligence surveillance is limited to what is “strictly necessary” and does not involve access to data on a “generalised basis.” Adequacy Decision ¶ 90.

This erroneous conclusion rests on five main misunderstandings about U.S. surveillance law and practice.

First, the U.S. government has access on a generalized basis to communications and data under Executive Order (“EO”) 12333. Relying on the executive order, the government conducts a wide array of “bulk” or “mass” surveillance programs—including on fiber-optic cables carrying communications from the European Union to the United States. *See* ACLU Expert Report ¶¶ 51–62.

Second, the U.S. government has access on a generalized basis to communications under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”). Through “Upstream” surveillance under Section 702, the National Security Agency (“NSA”) indiscriminately copies and then searches through vast quantities of personal metadata and content as it transits the Internet. In addition, the legal threshold for targeting non-U.S. persons under Section 702 is very low, and the number of targets is high—more than 129,000—resulting in the mass collection of hundreds of millions of communications per year. *See* ACLU Expert Report ¶¶ 37–48.

Third, neither Section 702 nor EO 12333 surveillance is limited to what is strictly necessary. Both authorize the acquisition of “foreign intelligence,” a broad and elastic category. Under Section 702, “foreign intelligence” encompasses information related to the foreign affairs of the United States, which could include, for example, national health data or factors influencing the price of oil. Under EO 12333, “foreign intelligence” is

defined even more broadly and encompasses information related to the “capabilities, intentions, or activities” of foreign persons. *See* ACLU Expert Report ¶¶ 31, 53.

Fourth, the Adequacy Decision rests heavily on the assertion that the NSA touches only a fraction of communications on the Internet. But even if the NSA were intercepting and searching only 5% of global Internet communications, that would be an enormous volume in absolute terms, and it would still constitute “generalised” access to the portion of Internet communications that pass through the NSA’s surveillance devices. *See* ACLU Expert Report ¶¶ 39, 48, 55–56, 61–62.

Fifth, even so-called “targeted” surveillance involves the collection and retention of vast amounts of non-targets’ private information. *See* ACLU Expert Report ¶ 41.

B. Presidential Policy Directive 28 ensures that U.S. foreign intelligence surveillance is limited to purposes that are “specific, strictly restricted and capable of justifying the interference.” Adequacy Decision ¶¶ 89–90.

As a procedural matter, the U.S. Department of Justice (“DOJ”) has taken the position that executive directives such as Presidential Policy Directive 28 (“PPD-28”) can be modified or revoked at any time, even in secret. As a substantive matter, PPD-28 in no way limits the *collection* of data in bulk. Instead, its limitations apply only to the *use* of information collected in bulk, and it allows the use of this information for detecting and countering broad categories of activities, including cybersecurity threats and transnational crime.

In addition, PPD-28’s limitations on the retention and dissemination of personal information are extremely weak. The directive provides that the government may retain or disseminate the personal information of non-U.S. persons only if retention or dissemination of comparable information concerning U.S. persons is permitted under EO 12333. Critically, however, 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,” which is defined to encompass information relating to the activities of foreign persons and organizations. *See* ACLU Expert Report ¶¶ 63–74.

C. U.S. foreign intelligence surveillance is subject to sufficient oversight. Adequacy Decision ¶¶ 67, 92–110.

Existing oversight mechanisms are insufficient 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. Similarly, surveillance under Section 702 is not adequately supervised by the courts or by

Congress. Other oversight mechanisms, such as the Privacy and Civil Liberties Oversight Board and the Inspectors General, have only very limited authority and fail to compensate for the fundamental deficiencies in legislative and judicial oversight. *See* ACLU Expert Report ¶¶ 75–98.

D. E.U. persons will have legal recourse for the U.S. government’s processing of personal data in the course of foreign intelligence surveillance. Adequacy Decision ¶ 111.

Virtually none of the individuals subject to Section 702 or EO 12333 surveillance will ever receive notice of that fact. As a result, it is exceedingly difficult to establish what is known as “standing” to challenge the surveillance in any 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 remedy through the courts. To date, as a result of the government’s invocation and judicial application of the standing and “state secrets” 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. *See* ACLU Expert Report ¶¶ 99–112.³

³ The U.S. government’s recent representations about access to remedies in its reply to the United Nations Human Rights Committee notably fail to grapple with the effects of the standing and state secrets doctrines. *See* Int’l Covenant on Civil & Political Rights, H.R. Subcomm., *Concluding Observations on the Fourth Periodic Report of the U.S.A.: Information Received from the U.S.A. on Follow-Up to the Concluding Observations*, U.N. Doc. CCPR/C/USA/CO/4/Add.1 (Nov. 2017), https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4%2fAdd.1&Lang=en.

Both that submission and the European Commission’s first annual review of Privacy Shield emphasized that the ACLU had standing to challenge the U.S. government’s bulk collection of Americans’ call records under Section 215 of the USA Patriot Act. *See id.* ¶ 41 (citing *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015)); European Commission, *Commission Staff Working Document Accompanying the 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*, § 4.2.4, COM (2017) 611 final (Oct. 18, 2017) (same). However, *Clapper* was a highly unusual case: in the immediate aftermath of the Snowden revelations, the Director of National Intelligence officially acknowledged the authenticity of a court order directing Verizon Business Network Services, Inc. to produce to the National Security Agency all call detail records of its customers’ calls. *See* Press Release, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>. In light of this official acknowledgment, and the fact that the ACLU was a Verizon Business Network Services customer, it was indisputable that the ACLU’s call records were among those collected under the program. *See Clapper*, 785 F.3d at 801. With the exception of this unprecedented disclosure, parties who challenge U.S. government surveillance continue to encounter severe obstacles when seeking remedies in U.S. courts.

Recent Developments in the U.S. Legal Framework

Recent laws passed in the United States, including modifications to Section 702 of FISA and the Clarifying Overseas Use of Data Act (“CLOUD Act”), further raise concerns that E.U. data transferred to the United States will not receive an adequate level of protection.

A. *Section 702 of FISA*

In 2018, Congress reauthorized a modified version of Section 702 of FISA, which was broadly opposed by privacy and civil liberties groups. Instead of reforming the law, the modified version opened the door to more expansive surveillance practices that fail to comport with E.U. standards.

First, the new law contains language that could be used to argue that the government has codified “about” collection—expanding the scope of Section 702 beyond what the statute previously authorized. For years, the executive branch had wrongly argued that Section 702 can be used to collect information not just “to” or “from” a target, but also “about” a target. In 2017, following numerous instances in which the NSA failed to adhere to court-imposed restrictions for collection “about” targets, the NSA voluntarily halted this practice. Unfortunately, the modified version of Section 702 passed by Congress failed to explicitly prohibit “about” collection. Instead, it allowed the government to restart this practice if it obtains FISA court approval, and if Congress fails to pass legislation prohibiting the practice within a one-month time period. The government will likely argue that in passing this provision, Congress has codified “about” collection, although no court outside of the FISA court has assessed its legality. Thus, the modified version of Section 702 represents a step backward in the law and could be relied on to restart the types of “about” collection that have been halted.

Second, the new law contains ambiguous language that the government might rely on to argue that Congress further expanded the executive branch’s surveillance authority under Section 702. In the past, Section 702 “about” collection involved acquiring communications that contained a specific “selector” associated with a target, such as an email or phone number, and not merely an individual’s name or a characteristic. However, the new law suggests that collection of data that merely reference a target is permissible, which could be read by the government to allow “about” collection of communications in much broader circumstances.

B. *CLOUD Act*

Generally, foreign governments seeking content from U.S. providers are governed by Mutual Legal Assistance Treaties (“MLATs”). MLATs provide significant safeguards to ensure that individuals’ rights are not adversely impacted and that information obtained is not used to perpetrate human rights violations. MLATs generally require that any foreign government request be vetted by the DOJ and that a U.S. judge issue a warrant based on

probable cause before data can be handed over to a foreign government. As part of this process, the DOJ and a U.S. judge can consider human rights concerns and take steps to protect the privacy of third parties who may be impacted by any disclosure. Generally, MLATs are confined to stored communications.

However, in 2018, Congress passed the CLOUD Act, which permits the DOJ to enter into agreements with foreign countries that allow them to bypass the MLAT process and obtain data directly from U.S. providers. Of concern, these new agreements permit foreign countries to obtain stored communications without the safeguards provided under the MLAT process. They also permit access to real-time intercepts without compliance with the U.S. Wiretap Act or human rights treaty obligations. The United States is currently negotiating a CLOUD Act agreement with the United Kingdom.

There are significant concerns that future CLOUD Act agreements will fail to provide an adequate level of protection to E.U. data transferred to the United States. The CLOUD Act framework raises the following concerns with regards to E.U. data.

1. The CLOUD Act's limited protections for Americans do not apply to individuals in the European Union. For example, the CLOUD Act prohibits foreign governments from targeting Americans for surveillance, yet would allow foreign governments to target any other individual in the world (including individuals that do not reside in and are not citizens of the requesting country). In addition, it requires foreign governments that enter into CLOUD Act agreements to commit to minimizing U.S. persons' information. However, there is no corollary requirement for non-U.S. persons. In other words, a non-E.U. country that enters into a CLOUD Act agreement would be permitted to target E.U. citizens for surveillance under standards lower than those in the United States or European Union countries; retain information about non-Americans indefinitely; disseminate information to other countries; and use information to target E.U. residents for prosecution and arrest.

2. The CLOUD Act language fails to ensure that the United States does not enter into agreements with countries that commit human rights abuses, which can adversely impact individuals in the European Union. Under the act, the standards that countries must meet to be eligible for an agreement are vague, weak, and unclear. For example, among other concerns, the law does not explicitly prohibit agreements with countries that have a pattern or practice of engaging in human rights violations, nor does it require an assessment of whether a country has effective control and meaningful oversight of intelligence or law enforcement units that may engage in human rights violations. In addition, the statute states that countries must respect "universal international human rights"—which is not a recognized term in U.S. law—without definition or clarity regarding how to assess adherence. Moreover, it states that countries must protect freedom of expression, without explaining whether free expression is to be defined under

U.S. law, international law, or a country's own domestic law. Such ambiguity is particularly concerning given that the act eliminates any further vetting of requests by a U.S. government entity. Given this, there is a significant risk that future CLOUD Act agreements could permit foreign governments to obtain E.U.-person data and use that data to commit human rights abuses.

3. The standards that foreign governments must meet to be eligible for CLOUD Act agreements are vague and may result in data-sharing agreements that do not respect human rights or E.U. standards. For example, the CLOUD Act contains no requirement that foreign governments provide notice or the opportunity for meaningful redress to individuals impacted by surveillance. In addition, the act requires that foreign government requests for data be based on “articulable and credible facts, particularity, legality, and severity regarding the conduct under investigations”—a standard that is, at best, vague and subject to different interpretations, and is likely lower than the current probable cause standard applied to MLAT requests. Moreover, the statute fails to make clear that any request for information must be subject to *prior* judicial or independent oversight, as required under human rights law. As a result, the CLOUD Act opens the door to agreements that permit non-E.U. countries to obtain E.U.-person data under standards that do not provide the protections that would be required in the European Union or under human rights law.

Automated Decision-Making

In the area of automated decision-making, the United States lacks a comprehensive framework to provide safeguards when these mechanisms produce legal effects or significantly affect the rights or obligations of consumers. Specifically, there is no corollary in U.S. law to provisions of the General Data Protection Regulation that explicitly state, with certain narrow exceptions, that individuals have the ability to not be subject to decisions by data controllers based solely on automated processing which produces legal effects. In addition, there is not explicit law that makes clear that individuals are entitled to due process or human intervention in cases where automated decision-making by a data controller has been used to produce a legal effect. Thus, in many cases, consumers may be left without recourse where an automated process produces a discriminatory or simply erroneous result.

Existing laws in the United States prohibit discrimination in credit, housing, employment, and other contexts. However, there are significant difficulties in bringing legal challenges in cases where automated processing produces a discriminatory impact in these circumstances. First, individuals may lack the information or ability to obtain information to demonstrate that the automated process is producing a discriminatory effect. Second, not all data platforms acknowledge that they are bound by anti-discrimination laws. For example, it was only recently following litigation that Facebook acknowledged that it

was bound by laws that prohibit discriminatory advertising in the housing, employment, and credit context. Third, bringing legal challenges can be both time consuming and expensive, making it an infeasible avenue for many consumers who rightfully seek a remedy.

Conclusion

The ACLU continues to believe that the Privacy Shield fails to ensure that E.U. data transferred to the United States receives an adequate level of protection that is essentially equivalent to the protections afforded under the E.U. Charter. Recent legal developments in the United States further raise concerns that U.S. surveillance infringes Europeans' rights beyond what is strictly necessary and lacks sufficient oversight, and that U.S. law fails to provide meaningful avenues for redress. Moreover, unlike the E.U. General Data Protection Regulation, the United States lacks a comprehensive commercial privacy framework to ensure that consumers are not adversely impacted by automated processing and other data practices.

If you have additional questions, please feel free to contact Ashley Gorski (agorski@aclu.org) or Neema Singh Guliani (nguliani@aclu.org).

Sincerely,



Faiz Shakir
National Political Director



Neema Singh Guliani
Legislative Counsel



Ashley Gorski
Staff Attorney, National Security Project

Exhibit A



June 30, 2017

Bruno Gencarelli
Head of Unit
European Commission
Directorate-General Justice and Consumers
Data Protection Unit - C.3
B-1049 Brussels, Belgium

Re: The European Commission’s Annual Review of the EU–US Privacy Shield

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

Dear Mr. Gencarelli,

We write in response to your invitation for the American Civil Liberties Union (“ACLU”) to provide input concerning the EU–US Privacy Shield, recent developments in the US legal framework, and the functioning of redress and review mechanisms discussed in the European Commission’s July 2016 Privacy Shield adequacy decision.

Previously, the ACLU and other rights organizations have expressed our view¹ that reform to Section 702 of the Foreign Intelligence Surveillance Act is necessary to ensure that EU data transferred to the US receives protection that is “essentially equivalent” to the protections required under the EU Charter—calling into question the legality of the existing Privacy Shield agreement. Recent developments further support this view and raise concerns that US surveillance practices do not meet EU standards.

In Part I, we review recent developments that undermine the US government assertions that formed the foundation of the Privacy Shield agreement. In Part II, we discuss the inadequacy of redress mechanisms referred to in the Commission’s decision. Finally, in Part III of this submission, we highlight some of our prior concerns as they relate to conduct under Executive Order (“EO”) 12,333, which we urge you to consider as part of your review.

I. Recent Developments in the US Legal Framework

In a February 28, 2017 letter from the ACLU and Human Rights Watch to Commissioner Jourová, we described two significant recent developments in the United States that undermine the foundation of the Privacy Shield framework: the issuance of the executive order *Enhancing Public Safety in*

¹ Attachment A.

the Interior of the United States and the deterioration of the Privacy and Civil Liberties Oversight Board (“PCLOB”).²

In addition to these two changes to US policies, we wish to draw the Commission’s attention to several other developments since August 2016:

State of Section 702 reform legislation: In June, the Trump administration expressed its support not only for reauthorizing Section 702, but for making the authority permanent.³ The administration’s position is a troubling development given the massive breadth and intrusiveness of Section 702 surveillance, the statute’s extremely permissive targeting standard, and the government’s history of systemic compliance violations under the law.

The purpose of a sunset is to force the US government to assess whether surveillance programs are still necessary, or whether changed circumstances necessitate reform or termination. In this way, the sunset operates as an oversight tool, prompting regular review and examination of the authority by Congress and the intelligence agencies. Removal of the sunset would thus weaken the already deficient oversight structure surrounding Section 702. While many members of Congress do not support the administration’s position and are considering reform measures, there has been no reform bill introduced in Congress. At this juncture, engagement by the international community to press for surveillance reforms that ensure protection of fundamental rights is critical.

Lack of enforceability of Presidential Policy Directive 28 (“PPD-28”): A recently released court decision holds that PPD-28 does not create any enforceable rights—underscoring yet another way in which the directive does not adequately safeguard the rights of individuals in the EU.⁴ In June 2017, the US government released a partially redacted version of a 2014 Foreign Intelligence Surveillance Court (“FISC”) opinion addressing a US electronic communication service provider’s challenge to Section 702.⁵ The provider argued that the FISC should consider the interests of non-US persons abroad when evaluating the lawfulness of Section 702 surveillance—citing, among other sources, PPD-28.⁶ But the court deemed these interests irrelevant, in part because PPD-28, “by its terms, is not judicially enforceable.”⁷ Thus, under the court’s holding, even if the US government were to persistently and deliberately violate the terms of PPD-28, no EU or US person could enforce the directive in court. More generally, those who seek meaningful remedies for unlawful surveillance face significant obstacles to redress, as discussed in Part II, *infra*.

² Attachment B.

³ Thomas P. Bossert, *Congress Must Reauthorize Foreign Surveillance*, New York Times, June 7, 2017, <https://www.nytimes.com/2017/06/07/opinion/congress-reauthorize-foreign-surveillance.html>.

⁴ See *infra* note 44 (discussing shortcomings of PPD-28).

⁵ See Additional Release of FISA Section 702 Documents, IC on the Record, June 14, 2017, <https://icontherecord.tumblr.com/post/161824569523/additional-release-of-fisa-section-702-documents>. The 2014 FISC opinion is available at <https://www.dni.gov/files/documents/icotr/702/Bates%20510-548.pdf> (“2014 FISC Op.”).

⁶ See 2014 FISC Op. at 36.

⁷ *Id.*

Extensive violations of the procedures governing Section 702 surveillance: An April 26, 2017 FISC opinion, recently released with redactions, highlights an array of ongoing and significant violations of the court-ordered procedures governing Section 702 surveillance (“April 2017 FISC opinion”).⁸ These persistent violations confirm the inadequacy of existing oversight structures and call into question whether effective oversight of a program of this scale is even possible.

The violations noted by the FISC include:

- Failure by the NSA and CIA to complete required purges;
- Compliance and implementation problems regarding the NSA’s adherence to its targeting and minimization procedures;
- Improper querying of Section 702 data, such that “approximately eighty-five percent” of certain queries of FISA repositories using US person identifiers were “not compliant with the applicable minimization procedures”;
- Improper FBI disclosures of raw information to third parties;
- Failure to comply with requirements governing the handling of attorney-client communications; and
- Failure to provide prompt notification to the FISC when non-compliance is discovered, to ensure that appropriate remedial steps are taken.⁹

The NSA’s change to “about” collection: The government conducts at least two forms of surveillance under Section 702: “PRISM” (sometimes referred to as “downstream” surveillance) and “Upstream.” Through Upstream collection, the NSA copies and searches streams of internet traffic as that data flows across the internet “backbone”—the network of cables, switches, and routers that carry internet communications—inside the United States. In April 2017, the NSA announced that it would modify one aspect of “Upstream” surveillance under Section 702, known as “about” collection.¹⁰ Until this change, when the NSA conducted Upstream surveillance, it acquired international internet communications to, from, and *about* its tens of thousands of targets.

⁸ See 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>. The April 2017 FISC opinion is available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf (“April 2017 FISC Op.”).

⁹ April 2017 FISC Op. at 68–95.

¹⁰ See [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011); Privacy & Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 35–41 (2014), <https://www.pclob.gov/library/702-Report.pdf>; Charlie Savage, *N.S.A. Halts Collection of Americans’ Emails About Foreign Targets*, N.Y. Times, Apr. 28, 2017; 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>.

As a result of this change, the NSA will not “collect” or “acquire” for long-term retention and use communications that are merely “about” its targets—with some exceptions.¹¹ This change to “about” collection is notable for several reasons.

One, the NSA’s decision highlights that oversight—both internally at the NSA and by the FISC—is wholly lacking. The April 2017 FISC opinion describes privacy violations that were significant, persisted for months, and were not appropriately reported. According to the opinion, in October 2016, the government orally apprised the FISC of “significant non-compliance with the NSA’s minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers.”¹² Specifically, “with much greater frequency than had previously been disclosed to the Court,” NSA analysts had “used U.S.-person identifiers to query the result of Internet ‘upstream’ collection, even though NSA’s Section 702 minimization procedures prohibited such queries.”¹³ The FISC ascribed the government’s failure to timely disclose these violations to “an institutional ‘lack of candor’ on the NSA’s part and emphasized that ‘this is a very serious Fourth Amendment issue.’”¹⁴

Two, this policy change still permits “generalized access to the content of communications” of EU persons via Section 702 Upstream surveillance. Although the FISC opinion and new procedures state that the NSA will not “acquire” or “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 equipment *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.¹⁵ In other words, the NSA will continue to engage in Upstream surveillance under Section 702. Moreover, the NSA’s decision has no bearing on existing EO 12,333 surveillance activities.

Finally, the change illustrates the need for Congress to codify certain Section 702 policies. The government has candidly acknowledged that it may seek to restart “about” collection.¹⁶ If they do so, there is no guarantee that the public or even lawmakers would be informed. Without codification of this kind of policy shift, there is the risk that changes in leadership or circumstances will trigger even more intrusive and sweeping Section 702 surveillance practices.

¹¹ April 2017 FISC Op. at 23–25, 27.

¹² *Id.* at 4.

¹³ *Id.* at 15, 19.

¹⁴ *Id.* at 19 (quoting hearing transcript).

¹⁵ See April 2017 FISC Op. at 23, 25, 27. Notably, within government agencies, “acquisition” and “collection” are terms of art with very particular meanings. 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) expressly defines “collection” as excluding “[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, Aug. 8, 2016, <http://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887>.

¹⁶ *Hearing on the FISA Amendments Act, Panel 1 Before the S. Comm on Judiciary*, 115th Cong. (2015) (statement of Paul Morris, Dep. Gen. Counsel for Operations, N.S.A).

Expanded agency access to “raw” data under EO 12,333 and Section 702: The April 2017 FISC opinion also approves the expansion of the list of government agencies with access to unminimized Section 702 data, allowing the National Counterterrorism Center (“NCTC”) to now receive certain raw information acquired by the NSA and FBI.¹⁷ The NCTC’s retention rules permit the agency to retain non-responsive information for as long as 15 years.¹⁸ Information that has been reviewed as identified as responsive to one of several categories—including the broadly defined “foreign intelligence information”—may be retained indefinitely.

The FISC’s ruling is part of a broader trend of expanding the list of agencies with access to unminimized data. Last year, the US government adopted policies that would permit 16 additional federal agencies to access unminimized data collected by the NSA under EO 12,333, and to use such information for purposes that extend beyond protecting national security.¹⁹

II. Inadequacy of US Redress Mechanisms

The Privacy Shield adequacy determination incorrectly found that “[a] number of avenues are available under U.S. law to EU 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).²⁰ Below, we explain how these avenues have failed to provide meaningful vehicles for redress for persons concerned about the processing of their personal data. We also briefly address the inadequacy of the Privacy Shield Ombudsperson as a redress mechanism.

A. Obstacles to Challenging Surveillance in US Courts: Standing and State Secrets Doctrines

For the overwhelming majority of individuals whose rights are affected by US government surveillance under Section 702 and EO 12,333, 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 12,333 surveillance has ever produced a US court decision addressing the lawfulness of that surveillance. Nor has a plaintiff obtained a remedy of any kind for such surveillance, including under the statutory provisions cited by the Commission in its adequacy decision.

Because virtually none of the individuals who are subject to either Section 702 or EO 12,333 surveillance ever receive notice of that surveillance, it is exceedingly difficult to establish

¹⁷ April 2017 FISC Op. at 30.

¹⁸ *Id.* at 40.

¹⁹ Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency Under Sec. 2.3 of Executive Order 12,333 (Raw SIGINT Availability Procedures), <https://www.documentcloud.org/documents/3283349-Raw-12333-surveillance-sharing-guidelines.html>.

²⁰ Eur. Comm’n, Privacy Shield Implementing Decision ¶ 111.

standing to challenge the surveillance in US court.²¹ Without standing to sue, a plaintiff cannot litigate the merits of either constitutional or statutory claims.

Because Section 702 and EO 12,333 surveillance is conducted in secret, the US government routinely argues to courts that plaintiffs' claims of injury are mere "speculation" and insufficient to establish standing. In 2013, the US 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.²²

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 a civil challenge to Section 702 Upstream surveillance. In October 2015, a US district court dismissed the *Wikimedia* suit on the grounds that all nine plaintiffs lacked standing to sue. Among other things, the court held that Wikimedia had not plausibly alleged that any of its international communications—more than one trillion per year, with individuals in virtually every country on earth—were subject to Upstream surveillance.

In May 2017, the Fourth Circuit reversed the district court's opinion with respect to Wikimedia, but it affirmed the district court's dismissal of the claims of the eight other plaintiffs, who include Amnesty International USA, Human Rights Watch, and the National Association of Criminal Defense Lawyers.²³

It bears emphasis that the Fourth Circuit did not hold that Wikimedia has established standing as a matter of fact, nor did it consider whether Upstream surveillance is lawful. Those questions have yet to be litigated. Rather, the Fourth Circuit in *Wikimedia* was evaluating a "facial" challenge to the plaintiffs' complaint at a threshold stage of the litigation. Its analysis simply considered whether the plaintiffs' allegations of standing were plausible. A plaintiff that prevails on this threshold question must still present evidentiary material that establishes its standing as a matter of fact. Thus, even if the government does not appeal the Fourth Circuit's ruling as to the plausibility of Wikimedia's standing allegations, it will have another opportunity to challenge standing—this time as a factual matter. The government has repeatedly relied on such strategies

²¹ The US 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 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 12,333 surveillance). Notably, however, the government has refused to disclose its interpretation of what constitutes evidence "derived from" FISA. To date, only ten criminal defendants have received notice of Section 702 surveillance, despite the US government's collection of hundreds of millions of communications under that authority.

²² *See Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1148 (2013).

²³ *See Wikimedia Found. v. NSA*, No. 15-2560, 2017 WL 2240910 (4th Cir. May 23, 2017).

to block US courts from considering the lawfulness of surveillance conducted under Section 702.²⁴

Given the Fourth Circuit’s holding that eight of the nine plaintiffs lacked standing, its 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. Despite the breadth of Upstream surveillance, the Fourth Circuit rejected as implausible the standing claims of eight organizations that engage in substantial quantities of international communications as an essential part of their work, including sensitive communications with and about individuals likely targeted by the NSA for surveillance.

For EU human rights and legal organizations that routinely engage in sensitive EU–US communications in the course of their work—and for ordinary EU persons who communicate with friends or family in the US—the standing doctrine continues to be a significant obstacle to redress for rights violations resulting from Section 702 and EO 12,333 surveillance.

Standing doctrine is not the only obstacle to redress. In addition, 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.²⁵ 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.²⁶ Although courts have held that FISA preempts the application of the state secrets privilege for FISA-related claims,²⁷ the government has nevertheless raised the privilege in challenges to Section 702 surveillance.²⁸

B. Government Arguments About the Applicability of the US Constitution to Non-US Persons Abroad

The US government has taken the position that non-US persons located abroad have no right to challenge surveillance under the US Constitution. In particular, the US 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

²⁴ See, e.g., *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) (challenging the factual basis for plaintiffs’ standing); *Jewel v. NSA*, No. 08-04373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015) (challenging the factual basis for plaintiffs’ standing and invoking the state secrets privilege).

²⁵ See *United States v. Reynolds*, 345 U.S. 1 (1953).

²⁶ See, e.g., *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1093 (9th Cir. 2010) (dismissing challenge to US government’s extraordinary rendition and torture program on state secrets grounds).

²⁷ See, e.g., *Jewel v. National Security Agency*, 965 F. Supp. 2d 1090, 1105 (N.D. Cal. 2013).

²⁸ 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).

rights.”²⁹ The government bases this 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 US government search of physical property located in Mexico and belonging to a Mexican national.³⁰ Although the ACLU maintains that the government’s analysis is incorrect, when evaluating the availability of redress for non-US persons, it is significant that the US government regularly argues that non-US persons seeking to challenge warrantless surveillance programs are not entitled to constitutional protection.

C. Inadequacy of the Freedom of Information Act as a Form of Redress

The Freedom of Information Act was not designed to operate as a form of redress; rather, the US Congress enacted this law to provide transparency to the public about US government activities.³¹ Because the FOIA permits the government to withhold properly classified information from disclosure³² 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 US government’s surveillance of a particular individual’s communications or data.

The ACLU is 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 12,333. 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 US naval facility at Guantanamo Bay, Cuba, and who sought information concerning the surveillance of their communications by the NSA.³³

D. Inability of the Privacy Shield Ombudsperson To Provide Meaningful Redress

Last year, the negotiations between the European Union and the United States over the Privacy Shield agreement led to the US executive branch’s creation of the Privacy Shield Ombudsperson position. But the Ombudsperson’s legal authority and ability to provide meaningful redress are severely limited.

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,

²⁹ Supp. Br. of Plaintiff–Appellee at 12, *United States v. Mohamud*, No. 14-30217 (9th Cir. Oct. 3, 2016).

³⁰ *See id.* at 261–62, 273.

³¹ *See* Eur. Comm’n, Privacy Shield Implementing Decision ¶ 114; 5 U.S.C. § 552.

³² *See* 5 U.S.C. § 552(b)(1).

³³ *See Wilner v. NSA*, 592 F.3d 60 (2d Cir. 2009).

or, in the event of non-compliance, such non-compliance has been remedied.”³⁴ 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.

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 or international law, 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. Moreover, the Ombudsperson cannot respond to any general claims that the Privacy Shield agreement is inconsistent with EU data protection laws.

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.

III. Section 702 and EO 12,333 Surveillance Violate the Standards Set Forth in *Schrems v. Data Protection Commissioner*

In our January 5, 2016 letter to the Chairwoman of the Working Party 29, we discussed several reforms that must be made to Section 702 to satisfy the standards set forth by the Court of Justice of the European Union (“CJEU”) in *Schrems v. Data Protection Commissioner* (Attachment A). Among other things, we explained that the US relies on Section 702 to obtain “generalized” access to the content of EU–US communications, in violation of CJEU’s decision;³⁵ that Section 702’s broad authorizations to obtain “foreign intelligence information” from any foreigner do not satisfy the CJEU’s requirement that the government employ an “objective criterion” limiting surveillance to purposes that are “specific, strictly restricted and capable of justifying the interference,” and such broad authorizations infringe Europeans’ rights beyond what is “strictly necessary”;³⁶ and that, under Section 702, the government claims sweeping authority to retain and use the data it has collected.³⁷

These concerns apply with even greater force in the context of electronic surveillance conducted under EO 12,333. This surveillance, which largely takes place outside US soil, implicates EU-

³⁴ See EU–US Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence § 4(e), <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g>.

³⁵ Attachment A at 5.

³⁶ Attachment A at 5–6. Notably, “foreign intelligence information” is defined under the statute to encompass far more than information relevant to “national security.” Compare 50 U.S.C. § 1801(e), with Eur. Comm’n, Privacy Shield Implementing Decision ¶¶ 88–89 & n.98.

³⁷ Attachment A at 6.

person communications as they are in transit from the EU to the US.³⁸ EO 12,333 is the primary authority under which the NSA conducts foreign intelligence, and it encompasses numerous bulk collection programs that involve acquiring communications and data on a generalized basis, without discriminants.³⁹ These programs have included, for example, the NSA's recording of every single cell phone call into, out of, and within at least two countries;⁴⁰ its collection of hundreds of millions of contact lists and address books from email and messaging accounts;⁴¹ its collection of billions of cell phone location records each day;⁴² and its surreptitious interception of data from Google and Yahoo user accounts as that information travels between those companies' data centers located abroad.⁴³ Through PPD-28, the US acknowledged its EO 12,333 bulk collection practices—which involve generalized access to the contents of communications, in violation of the standards articulated in *Schrems*.⁴⁴

³⁸ See Eur. Comm'n, Privacy Shield Implementing Decision ¶ 75 (observing that the US may access the personal data of EU persons "outside the United States, including during their transit on the transatlantic cables from the Union to the United States"); see also 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/> (describing how the NSA taps directly into fiber-optic cables at "congestion points" overseas).

³⁹ See, e.g., Letter from ACLU to Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), <https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333>.

⁴⁰ 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/>.

⁴¹ Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-Mail Address Books Globally*, Wash. Post, Oct. 14, 2013, https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

⁴² 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.

⁴³ 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.

⁴⁴ See Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential Policy Directive/PPD-28 (Jan. 17, 2014), <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>. PPD-28 provides that when the US collects nonpublicly available signals intelligence in bulk, it shall use that data only for detecting and countering six types of activities. Taken together, these categories are very broad and open to interpretation. Moreover, PPD-28's limitations on the use of information collected in bulk do not extend to other problematic types of mass surveillance, including the "bulk searching" of internet communications, in which the US government searches the content of vast quantities of electronic communications for "selection terms."

The directive's most significant reforms—which can be modified or revoked by the US President at any time—are with respect to the retention and dissemination of communications containing "personal information" of non-US persons. Yet even these reforms impose few constraints on the US government. Under PPD-28, the US may retain or disseminate the personal information of non-US persons only if retention or dissemination of comparable information concerning US persons would be permitted under Section 2.3 of EO 12,333. Critically, however, Section 2.3 is extremely permissive: it authorizes the retention and dissemination of information concerning US persons when, for example, that information constitutes "foreign intelligence," broadly defined.

Even when the US government conducts “targeted” forms of surveillance under EO 12,333, the executive order and its accompanying regulations place few restrictions on the collection of non-US 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 permits surveillance of a vast array of non-US persons with no nexus to national security threats.⁴⁵ In other words, the US government does not employ an “objective criterion” limiting EO 12,333 surveillance to purposes that are “specific, strictly restricted and capable of justifying the interference,” and the infringement of Europeans’ rights goes beyond what is “strictly necessary.”⁴⁶

Despite its breadth, surveillance under EO 12,333 has not been subject to meaningful oversight. Surveillance programs operated under the executive order have never been reviewed by any court. Moreover, these programs are not governed by any statute, and, as the former Chairman of the Senate Intelligence Committee has conceded, they are not overseen in any meaningful way by Congress.⁴⁷ Moreover, efforts by the Privacy and Civil Liberties Oversight Board to study even a small subset of EO 12,333 programs have stalled, and relevant draft reports were never finalized or publicly released. We urge you to consider the adequacy of EO 12,333 protections and the other information cited above as part of your review of the adequacy of the Privacy Shield.

We would welcome the opportunity to discuss these issues with you in more detail. If you have questions, feel free to contact Neema Singh Guliani (nguliani@aclu.org or 202-675-2322) or Ashley Gorski (agorski@aclu.org or 212-284-7305).

Sincerely,



Faiz Shakir
Director



Ashley Gorski
Staff Attorney, National Security Project



Neema Singh Guliani
Legislative Counsel

⁴⁵ See EO 12,333 § 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”).

⁴⁶ See Case C-362/14, *Schrems v. Data Protection Comm’r*, 2000 EUR-Lex 520 (Oct. 6, 2015), available at <http://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C&parties=Schrems> ¶¶ 92–93.

⁴⁷ 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>.

Exhibit B



February 28, 2017

Attn:

Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission

CC:

Claude Moraes
Chairman, Committee on Civil Liberties, Justice and Home Affairs (LIBE)
European Parliament

Frans Timmermans
First Vice-President, Better Regulation, Interinstitutional Relations, the Rule of Law and the Charter of Fundamental Rights
European Commission

Andrus Ansip
Vice-President, Digital Single Market
European Commission

Isabelle Falque-Pierrotin
Chairwoman, Article 29 Working Party
European Commission

Dear Commissioner Jourová,

Recent developments in the United States call into question assurances by the US government that formed the foundation of both the Privacy Shield agreement and the US-EU umbrella agreement. We write to urge you to reexamine whether these agreements sufficiently protect the fundamental rights of people in the European Union in light of these changed circumstances.

In recent weeks, President Donald Trump has issued several executive orders that represent an attack on the rights of immigrants and foreigners—including specific provisions designed to strip these individuals of critical privacy protections that have been provided by previous Democratic and Republican administrations for decades. Concurrently, there has been a deterioration in existing oversight and accountability structures that impact whether, consistent with the ruling in the *Schrems*¹ and *Digital*

¹Case C-362/14, *Schrems v. Data Protection Comm’r*, 2000 EUR-Lex 520 (Oct. 6, 2015), <http://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C&parties=Schrems>.

Rights Ireland judgments², people in the EU are afforded appropriate privacy protections and redress in cases where their data is transferred to the US.

Previously, the ACLU and other rights organizations have written to you expressing our view that reform to US surveillance laws is necessary to ensure that EU data transferred to the US receives protection that is “essentially equivalent” to the protections required under the EU Charter—calling into question the legality of the existing Privacy Shield agreement (Attachment 1).³ We have also stressed the inadequacy of existing privacy oversight and redress mechanisms for both US residents and individuals around the world. The following recent changes to US policies only deepen our concerns that assurances underpinning both the Privacy Shield and US-EU umbrella agreement are not valid, requiring a reexamination of whether these agreements are consistent with the rights enshrined in the EU Charter of Fundamental Rights:

- Issuance of the executive order *Enhancing Public Safety in the Interior of the United States*: Issued on January 25, 2017, Section 14 of the executive order reverses policies of the Bush, Obama, and prior administrations by prohibiting federal agencies, consistent with applicable law, from providing Privacy Act protections to individuals who are not US citizens or lawful permanent residents.⁴ As a result of this change, people in the EU have diminished protections when it comes to limits on dissemination of their personal information, the right to access their private information held by the US government, and the right to request corrections to their information.
- Deterioration of the Privacy and Civil Liberties Oversight Board (PCLOB): The Privacy and Civil Liberties Oversight Board, while fulfilling a valuable public reporting role, is limited in its oversight function and was not designed to provide redress concerning US surveillance practices. Thus, the PCLOB has never provided remedies for rights violations or functioned as a sufficient mechanism to protect personal data. In recent months, the situation has worsened: the PCLOB currently lacks a quorum, which strips its ability to issue public reports and recommendations, make basic staffing decisions, assist the Ombudsman created by the Privacy Shield framework,

² Case C-293/12, *Digital Rights Ireland v. Minister for Comm.*, 2006 EUR-Lex 24 (Apr. 8, 2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=403885>.

³ In addition to the concerns outlined in that letter, we note that surveillance conducted under Executive Order (EO) 12,333, also violates the standards articulated by the Court of Justice in *Schrems*. This surveillance, which the US government largely conducts outside US soil, implicates EU citizen communications as they are in transit from the EU to the US. *See* Eur. Comm’n, Implementing Decision, Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, ¶ 75 (Dec. 7, 2016) *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf. Notably, EO 12,333 is the primary authority under which the NSA conducts foreign intelligence, and it encompasses numerous bulk collection programs that involve acquiring communications on a generalized basis, without discriminants. *See, e.g.*, Letter from ACLU to Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), <https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333>. In PPD-28, the US effectively acknowledged and ratified its bulk collection practices under this authority. *See* Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential Policy Directive/PPD-28 (Jan. 17, 2014), <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

⁴ Exec. Order No. 13,768, 82 Fed. Reg. 8,799 (Jan. 25, 2017), *available at* <https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf>.

and conduct other routine business as part of its oversight responsibilities.⁵ The current administration and Senate have yet to act to fill the vacancies on the PCLOB.⁶

1. Executive order: *Enhancing Public Safety in the Interior of the United States*:

As part of the *Schrems* judgment, the Grand Chamber of the Court of European Justice of the European Union emphasized that Article 7 and 8 of the EU Charter of Fundamental Rights requires:

“...clear and precise rules governing the scope and application of a measure and imposing minimum safeguards so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of their data.”⁷

In addition, they emphasized that any legislation:

“...not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protections, as enshrined in Article 47 of the Charter.”⁸

Consistent with this requirement, the Privacy Shield framework adequacy determination relied in part on US government assurances that there were appropriate mechanisms in place for individuals to seek redress in cases where their data was accessed by the US government.⁹ Similarly, the umbrella agreement requires the US to ensure that individuals are entitled to seek access and correction to their personal information, unless specified exceptions apply.¹⁰ The umbrella agreement also requires that the US provide the ability to seek administrative redress to individuals in the EU in cases where they are improperly denied the ability to access or correct their information.¹¹

However, provisions in the recent executive order issued by the Trump administration raise concerns regarding whether EU data transferred to the US meets the standards outlined in these documents. Specifically, Section 14 of the executive order states that federal agencies “shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” Prior to issuance of the executive order, consistent with a 1975 OMB recommendation, many federal agencies, as a matter of longstanding policy, provided certain Privacy Act protections to databases that contained the information of US persons (defined as US citizens and lawful permanent

⁵ 50 U.S.C. § 601 note; *See also* GARRETT HATCH, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS (Cong. Research Service, 2012), <https://fas.org/sgp/crs/misc/RL34385.pdf>.

⁶ Elisabeth Collins is the only sitting members of the PCLOB and is a member of the Republican party.

⁷ *Schrems*, *supra* note 1 at ¶ 91.

⁸ *Id.* at ¶ 95.

⁹ Commission Implementing Decision (EU) No. 2016/1250, 2016 O.J. (L. 207/1) ¶ 25, *available at* <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN>.

¹⁰ Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (draft 2016) at articles 16 and 17, *available at* http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

¹¹ *Id.* at article 18

residents) and non-US persons.¹² These protections included limits on dissemination without consent (subject to exceptions), the right to access your own agency records, the right to request corrections to your records, and remedies where an agency fails to comply with certain requirements. As a result of Section 14, however, these rights will no longer be fully provided to individuals residing within the EU.

While the Judicial Redress Act provides some additional privacy protections for EU citizens, it does not completely mitigate the impact of the executive order's provision for several reasons. First, the Judicial Redress Act only applies to citizens of EU countries.¹³ Thus, if an individual lawfully works or lives in the EU, but has not obtained full citizenship status, then he or she may not be entitled to protection under the Judicial Redress Act. Thus, the EO provision strips privacy protections from thousands of lawful EU immigrants.

Second, the Judicial Redress Act alone does not provide the full range of Privacy Act protections that were provided as a matter of policy, prior to issuance of the executive order.¹⁴ The Judicial Redress Act only extends the right to EU citizens to bring a case in civil court to challenge US government action if their records were “willfully and intentionally” disseminated without consent in violation of relevant provisions of the Privacy Act, or in cases where a “designated federal agency or component” fails to comply with a request for information or correction.¹⁵ Thus, even with the Judicial Redress Act, EU citizens may be left without appropriate recourse to address improper dissemination of their information that is accidental or inadvertent in nature. In addition, EU citizens may be unable to address failures to provide access or corrections in cases where their information is held by federal agencies that are not designated under the bill. For example, the Department of Health and Human Services (HHS) has several databases that contain personal information of refugees and immigrants to the US. However, HHS is not a designated agency under the Judicial Redress Act, and thus EU citizens may not be able to access or request corrections to information held by HHS.¹⁶ Moreover, only information shared with the US government by an entity in a EU country for law enforcement purposes is covered—personal information collected by US agencies themselves is not covered, nor is information collected for non-law enforcement purposes such as intelligence gathering.

Finally, the Judicial Redress Act requires that an individual file a civil claim to enforce their rights, and does not require that federal agencies create an administrative process to address privacy violations. As a practical matter, this means that enforcement of EU citizens' rights may not only be time consuming, but

¹² Memorandum from Hugo Teufel III, Chief Privacy Off., DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-US Persons (Jan. 7, 2009), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf; *See* Privacy Act of 1974; System of Records Notice, 81 Fed. Reg. 46682 (July 18, 2016), *available at* <https://www.gpo.gov/fdsys/pkg/FR-2016-07-18/pdf/2016-16812.pdf>.

¹³ Judicial Redress Act, Pub. L. No., 114-126, §2(f), 130 Stat. 282 (2016), *available at* <https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf>.

¹⁴ It is worth noting that the Privacy Act contains numerous exceptions for national security and law enforcement purposes. As a result, even for individuals in the United States, it does not provide adequate redress opportunities in cases where individuals believe their rights have been violated as a result of surveillance. However, the policy change would eliminate even this limited protection. 5 U.S.C. § 552a.

¹⁵ Judicial Redress Act, *supra* note 12 at § 2(a).

¹⁶ Judicial Redress Act of 2015; Attn'y Gen. Designations, 82 Fed. Reg. 7860 (Jan. 23, 2017), *available at* <https://www.federalregister.gov/documents/2017/01/23/2017-01381/judicial-redress-act-of-2015-attorney-general-designations>.

also costly. Thus, while the Judicial Redress Act provides some relief to EU citizens, it does not fully mitigate the impact of the executive order.

2. Privacy and Civil Liberties Oversight Board

The CJEU has emphasized that appropriate oversight is critical to ensuring that EU data receives appropriate privacy and other fundamental rights protections. Thus, as part of its adequacy determination for the Privacy Shield, the European Commission relied on assurances that the US intelligence community was subject to various oversight mechanisms, including the PCLOB. The adequacy determination notes that the PCLOB ensures appropriate oversight over US surveillance practices by examining relevant records, issuing recommendations, hearing testimony, and preparing reports (including an examination of PPD-28).¹⁷ Similarly, supporting documentation provided by the Director of National Intelligence asserted that the PCLOB is an independent oversight body that is part of “robust and multi-layered oversight”.¹⁸

Even with a fully-functioning PCLOB, we had serious concerns that there was not effective oversight of US surveillance activities, and we strongly disagreed with many of the US government’s assertions in this arena. However, notwithstanding these concerns, it is clear that the European Commission relied on the representations regarding the oversight role of the PCLOB as part of its adequacy determination. Unfortunately, however, the PCLOB is no longer a fully functional body. Currently four of the five board positions on the PCLOB are vacant.¹⁹ Without a quorum, the PCLOB cannot issue reports and recommendations, including its planned report on activities conducted under executive order 12333 and the implementation of PPD-28.²⁰ In addition, the Board is further limited in its ability to make staffing decisions necessary to fulfill its responsibilities.²¹ Moreover, 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, ensuring that a full Board contains representation from both political parties. The current membership, however, represents only one political party.

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. Indeed, the PCLOB remained largely dormant from 2007 to 2012 due in part to these hurdles. For the PCLOB to operate effectively, it is critical that the President appoint and the Senate confirm individuals with a demonstrated commitment to and background in privacy, civil liberties, and transparency.

Given these recent changes to US policies and oversight structures, we believe that the assurances that the European Commission relied on as part of the Privacy Shield and US-EU umbrella agreement are no longer valid. Thus, we urge you to examine whether these agreements are consistent with the protections enshrined in the EU Charter of Fundamental Rights.

¹⁷ Comm’n Implementing Decision, *supra* note 8 at ¶ 95.

¹⁸ *Id.* at Annex VI.

¹⁹ *Board Member Biographies*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (Accessed Feb. 21, 2017), <https://www.pcllob.gov/about-us/board.html>.

²⁰ *See also*, 6 C.F.R. § 1000.3 (2013), *available at* <https://www.pcllob.gov/library/FederalRegister-PCLOB-2013-0005-Delegation-Reg.pdf>.

²¹ *Id.*

Sincerely,



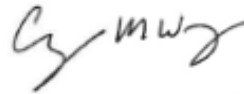
Faiz Shakir
Director
American Civil Liberties Union



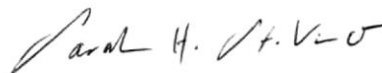
Lotte Leicht
European Union Director
Human Rights Watch



Neema Singh Guliani
Legislative Counsel
American Civil Liberties Union



Cynthia M. Wong
Senior Internet Researcher
Human Rights Watch



Sarah St. Vincent
Researcher, U.S. Division
Human Rights Watch

Exhibit C



Attention: Isabelle Falque Pierrotin, Chairwoman of the Working Party 29

Directorate C (Fundamental Rights and Union Citizenship) of the European Commission,
Directorate-General for Justice and Consumers
B-1049, Brussels, Belgium
Office No. MO-59 02/013

Re: U.S.–E.U. Safe Harbor and FISA Section 702 Reform

January 5, 2016

Dear Ms. Falque Pierrotin,

On behalf of the American Civil Liberties Union (“ACLU”),¹ we write to address the reforms that should be made to Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) to permit transatlantic data flows from the European Union to the United States under a new Safe Harbor agreement.

In recent years, the international flow of data has become an essential component of the global economy, facilitating both the growth of U.S. businesses and the exchange of ideas. However, as the *Schrems* decision recently issued by the Grand Chamber of the Court of Justice of the European Union (CJEU) makes clear,² the surveillance practices of the U.S. government have become an obstacle to the continued free flow of data from the European Union to the United States. In *Schrems*, the CJEU invalidated the legal framework for the E.U.–U.S. Safe Harbor agreement, which authorized U.S. companies to transmit personal data from the European Union to the United States in compliance with E.U. data protection and privacy laws. The CJEU did so because, among other reasons, it concluded that the body that had ratified the Safe Harbor agreement failed to account for the ways in which U.S. surveillance law and practice may violate fundamental rights and freedoms.

Below, we explain how Section 702 should be amended in response to the *Schrems* decision. The ACLU proposed some of these amendments before the *Schrems* decision was issued, but *Schrems* makes these amendments even more necessary. In brief,

¹ For nearly 100 years, the ACLU has been our nation’s guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual’s rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

² Case C-362/14, *Schrems v. Data Protection Comm’r*, 2000 EUR-Lex 520 (Sept. 23, 2015), available at <http://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C&parties=Schrems>.

Schrems makes clear that any new Safe Harbor agreement will not survive a judicial challenge before the CJEU unless the United States, preferably through legislation but at least through executive order, (1) ends the practice of “Upstream” collection; (2) narrows the scope of Section 702 surveillance in certain other respects; (3) limits the retention and use of data collected under Section 702; (4) creates new redress mechanisms; and (5) creates new transparency mechanisms.

I. The *Schrems* Judgment and Safe Harbor

A. Background

The Safe Harbor framework is designed to facilitate U.S. organizations’ compliance with E.U. data protection law. Pursuant to the 1995 E.U. Data Protection Directive (“1995 Directive”), data may be transferred from an E.U. member state to a country outside of the European Union only if the receiving country “ensures an adequate level of protection” for that data, judged in light of “all the circumstances surrounding [the] data transfer.”³ The 1995 Directive permits the European Commission—the executive branch of the European Union—to find, as a categorical matter, that a third country provides an adequate level of data protection through either domestic law or international commitments.⁴

In response to the 1995 Directive, E.U. and U.S. officials began developing a “Safe Harbor” framework—a set of requirements that U.S. companies would agree to abide by to conduct E.U.–U.S. data transfers. The European Commission ratified the Safe Harbor framework in 2000 by finding that it provided an adequate level of protection for personal data as required by the 1995 Directive (“2000 Decision”). Approximately 4,500 companies—including Microsoft and Google—rely on the 2000 Decision and the Safe Harbor framework to transfer data from the European Union to the United States.⁵ The vast majority of these companies lack an alternative mechanism that would permit transfer of data between the European Union and the United States.

In June 2013, Max Schrems, a Facebook user, brought a complaint to the Irish Data Protection Commissioner, challenging Facebook’s transfer of his data to U.S. servers on the grounds that U.S. law failed to adequately protect his personal data under the E.U. Charter of Fundamental Rights (the “Charter”).⁶ His complaint focused on the revelations

³ European Parliament and Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31–50; *see id.* at art. 26 (outlining certain exceptions to this principle, *e.g.*, where “the data subject has given his consent unambiguously to the proposed transfer”).

⁴ *Id.* at art. 25.

⁵ Natalia Drozdiak, *EU Court Says Data-Transfer Pact with U.S. Violates Privacy*, WALL STREET JOURNAL, Oct. 6, 2015, <http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361>.

⁶ The Charter recognizes the right to respect for private and family life, the right to protection of personal data, and the right to effective remedies for unlawful infringements of those rights. *See* Charter of Fundamental Rights of the European Union, arts. 7, 8, 47, Dec. 12, 2000, 2000/C 364/01.

by Edward Snowden concerning NSA surveillance, and in particular on the PRISM program implemented under Section 702.⁷

B. CJEU Judgment in *Schrems*

The CJEU’s ruling in *Schrems* makes clear that U.S. surveillance law and practice must be reformed before a valid Safe Harbor agreement can be renegotiated.

The *Schrems* judgment includes two principal holdings. First, the CJEU held that the 1995 Directive does not prevent a national-level supervisory authority from investigating complaints concerning data protection. Thus, even after a new Safe Harbor is negotiated, national data protection authorities are empowered to review complaints. European national data protection authorities have indicated that they will begin enforcing the *Schrems* decision and processing complaints beginning January 30, 2016—ensuring that the adequacy of a new Safe Harbor agreement will almost certainly make its way back to the CJEU.⁸

Second, the CJEU held the European Commission’s ratification of the Safe Harbor agreement in 2000 was invalid, as it focused solely on the Safe Harbor framework and not the broader context of U.S. surveillance law and practice. The 2000 Decision failed to make *any* findings regarding U.S. regulations designed to limit interference with fundamental rights, or the existence of effective oversight and redress mechanisms to protect against U.S. government surveillance.⁹ Because the 2000 Decision lacked sufficient findings “regarding the measures by which the United States ensures an adequate level of protection . . . by reason of its domestic law or its international commitments,” it failed to comply with the 1995 Directive.¹⁰

The CJEU observed that its analysis was borne out the Commission’s 2013 assessment of the implementation of the Safe Harbor. That assessment concluded that U.S. authorities were able to access the data of E.U. citizens in a way that was “incompatible . . . with the purposes for which it was transferred” and “beyond what was strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000].”¹¹ In addition, the Commission’s 2013 report underscored

⁷ Initially, the commissioner denied Schrems’s request, in part because the 2000 Decision found that the United States adequately protects Europeans’ privacy rights. However, ultimately, the Irish High Court asked the CJEU for a ruling on whether national data protection authorities are bound by the 2000 Decision—which found that the United States ensures an “adequate” level of data protection—or whether those authorities must conduct their own investigations into data protection complaints. *See Schrems* ¶ 36.

⁸ If a national-level authority concludes that a third country fails to ensure an adequate level of protection, it must have recourse to the national courts, which may in turn refer the issue to the CJEU. *Id.* ¶ 65. The Court observed that judicial review of the requirements of the 1995 Directive should be “strict,” given the “important role” of data protection in preserving the fundamental right to respect for private life. *Id.* ¶ 78.

⁹ *Id.* ¶¶ 88–90. The Court underscored that the Safe Harbor dispute resolution mechanisms were not a vehicle for challenging the legality of U.S. government interference with fundamental rights—a fact that the Commission itself had confirmed in a 2013 report. *See id.*

¹⁰ *Id.* ¶¶ 82, 83.

¹¹ *Id.* ¶¶ 22, 90.

the lack of administrative and judicial redress to challenge U.S. government access to personal data.¹²

In its judgment, the CJEU also elaborated on what constitutes an “adequate level of protection” under the 1995 Directive, providing guidance on the level of protection that must be afforded to E.U. data stored in the United States under any new Safe Harbor agreement. To be “adequate,” a third country must ensure “a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of [the 1995 Directive] read in light of the Charter.”¹³ Characterizing the level of protection within the European Union as “high,”¹⁴ the Court explained that legislation cannot interfere with the fundamental right to privacy unless it sets forth “clear and precise rules governing the scope and application of a measure and imposing minimum safeguards.”¹⁵ Furthermore, any derogations or limitations on the protection of personal data apply “only in so far as is strictly necessary.”¹⁶

While the CJEU did not discuss U.S. law in detail, its analysis made clear that Section 702 surveillance fails to satisfy these standards for at least three reasons. First, the Court explained that the “strictly necessary” standard is not satisfied where U.S. law lacks objective criteria to limit access and use of data to specific purposes that justify the interference.¹⁷ Second, the Court stated that legislation permitting generalized access to the content of electronic communications compromised the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.¹⁸ Third, the Court emphasized that the right to judicial protection enshrined in Article 47 of the Charter requires that an individual have legal remedies to access personal data relating to them, and the ability to seek correction or erasure of such data.¹⁹ Given the Court’s analysis, Section 702 must be reformed in order for any new Safe Harbor agreement to withstand judicial scrutiny.

II. The *Schrems* Judgment and Section 702

Since the 2008 enactment of Section 702, the ACLU has opposed the statute on the grounds that it authorizes the warrantless surveillance of Americans’ international communications. Over the past three years, the defects in the Section 702 surveillance scheme—lack of judicial oversight, inadequate targeting and minimization procedures, and absence of redress mechanisms, among others—have become even more apparent. To satisfy the standards set forth in *Schrems*, Congress must reform Section 702 to provide greater protections for personal data. At a minimum, such reforms must include:

¹² *Id.*

¹³ *Id.* ¶ 73.

¹⁴ *Id.*

¹⁵ *Id.* ¶ 91.

¹⁶ *Id.* ¶ 93.

¹⁷ *Id.*

¹⁸ *Id.* ¶ 94.

¹⁹ *Id.* ¶ 95.

A. Ending “Upstream” Surveillance

Upstream surveillance, which the government claims is authorized by Section 702, involves the mass copying and searching of virtually all Internet communications flowing into and out of the United States.²⁰ 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 Americans and others around the world.²¹ After copying nearly all of the cross-border text-based Internet traffic, the NSA searches the metadata and content for key terms, called “selectors,” that are associated with its foreign targets, who need not have any nexus to national security. Communications containing selectors—as well as those that happen to be bundled with them in transit—are retained on a longer-term basis for further analysis and dissemination, with few restrictions.²²

Thus, through Upstream surveillance, the NSA indiscriminately accesses, copies, and examines vast quantities of personal metadata and content. As *Schrems* makes clear, this “generalized” access to data content breaches the essence of the right to privacy and would be inherently unlawful under E.U. law—regardless of whether the government retains the data for long-term analysis. *Schrems* also makes clear that, for a new Safe Harbor agreement to survive judicial scrutiny, the United States must provide data privacy protections at a level “essentially equivalent” to that guaranteed in the European Union.²³ Accordingly, Upstream surveillance under Section 702 fails to satisfy the *Schrems* framework and must be discontinued to permit a valid Safe Harbor agreement.

B. Narrowing the Scope of Section 702 Surveillance in Certain Other Respects

Section 702 authorizes warrantless surveillance inside the United States for purposes that extend far beyond national security needs or counterterrorism. The statute allows the Attorney General and Director of National Intelligence to “authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the

²⁰ The ACLU currently represents nine plaintiffs challenging the lawfulness of Upstream surveillance on constitutional and statutory grounds. *See* Wikimedia Found. v. NSA/Central Sec. Serv., No. 15-cv-00662-TSE, 2015 U.S. Dist. LEXIS 144059 (D. Md. Oct. 23, 2015), *appeal docketed*, No. 15-2560 (4th Cir. 2015); *see also* First Amended Complaint, Wikimedia Found. v. NSA/Central Sec. Serv. ¶¶ 47–51, No. 15-cv-00662-TSE (D. Md. June 22, 2015), ECF No. 72, https://www.aclu.org/sites/default/files/field_document/72_first_amended_complaint_for_declaratory_and_injunctive_relief_6.22.15.pdf (describing Upstream surveillance in detail).

²¹ *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) 35–37 (“PCLOB SECTION 702 REPORT”), <https://www.pclob.gov/library/702-Report.pdf>. The government also likely conducts a similar form of backbone surveillance outside of the United States under Executive Order 12,333, the primary authority under which the NSA gathers foreign intelligence. *See* OVERVIEW OF SIGNALS INTELLIGENCE AUTHORITIES PRESENTATION 4 (Jan. 8, 2007), *available at* <https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf>. Executive Order 12,333 provides broad latitude for the government to conduct surveillance on U.S. and non-U.S. persons—without judicial review and other protections that would apply to surveillance conducted under statutory authorities. *See*, ACLU, SUBMISSION TO PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, SURVEILLANCE CONDUCTED PURSUANT TO EXECUTIVE ORDER 12,333 (forthcoming).

²² *See, e.g.*, PCLOB SECTION 702 REPORT at 35–41.

²³ *Schrems* ¶ 73.

United States to acquire foreign intelligence information.”²⁴ The role of the Foreign Intelligence Surveillance Court (FISC) within this scheme consists mainly of reviewing general targeting and minimization procedures; the FISC does not evaluate whether there is sufficient justification to conduct surveillance on specific targets, nor does it approve the terms that the NSA uses to surveil communications. As a result, the NSA is permitted to engage in surveillance with little judicial oversight.

Critically, Section 702 does not require the government to make *any* finding—let alone demonstrate probable cause to the FISC—that its surveillance targets are foreign agents, engaged in criminal activity, or even remotely associated with terrorism. Instead, the government is permitted to target any foreigner believed to have “foreign intelligence information”—a term defined broadly to cover a wide array of communications. For example, “foreign intelligence information” is defined to include information about foreign affairs, which could encompass communications between international organizations and government whistleblowers, or even between journalists and sources.²⁵

This surveillance scheme plainly contravenes the standards set forth in *Schrems*. Broad authorizations to obtain “foreign intelligence information” from any foreigner do not satisfy the *Schrems* requirement that the government employ an “objective criterion” limiting surveillance to purposes that are “specific, strictly restricted and capable of justifying the interference,” and such broad authorizations infringe Europeans’ rights beyond what is “strictly necessary.”²⁶ To remedy these deficiencies, Congress must narrow the scope of Section 702 surveillance by narrowing the definition of “foreign intelligence information.”

C. Placing Limits on the Retention and Use of Section 702 Data

The *Schrems* judgment recognizes that the United States lacks adequate rules to limit the interference with the fundamental rights of persons in the European Union whose data is transferred to the United States.²⁷ Under Section 702, the government has broad authority to retain and use the data it has collected. Indeed, it can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information.²⁸ Even for data that does not fall into either of these categories, the default retention period is two years for data acquired through Upstream collection, and five years for other Section 702-acquired information. In addition, data can be disseminated to other countries and used for a wide variety of purposes, including criminal prosecution. To address the concerns in *Schrems*, Congress must put in place more stringent restrictions on the access and use of data acquired under Section 702.

²⁴ 50 U.S.C. § 1881a(a).

²⁵ *See id.* §§ 1881a(a), 1801(e).

²⁶ *Schrems* ¶¶ 92–93.

²⁷ *Id.*

²⁸ *See* Sec. 6 OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (accessed Nov. 2, 2015), available at <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf>

D. Providing Effective Redress

The *Schrems* judgment affirms that individuals in the European Union must have access to judicial remedies in cases where they challenge the treatment of their data—remedies they lack under the current legal framework in the United States. Recently, the House passed H.R. 1428, the “Judicial Redress Act,” which sought to extend certain protections in the Privacy Act to citizens of countries designated by the Attorney General. However, the reforms in the Judicial Redress Act, which are exceedingly limited in scope, fail to provide adequate redress to E.U. citizens subject to improper surveillance under Section 702. First, the protections in H.R. 1428 apply only to citizens of countries designated by the Attorney General, and can be revoked at the discretion of the Executive Branch. Second, H.R. 1428 grants only an exceedingly limited set of rights to E.U. citizens under the Privacy Act.²⁹ Finally, even for U.S. citizens, the Privacy Act fails to provide an avenue to challenge national security surveillance programs. Thus, to address the concerns in *Schrems*, Congress will need to create a framework for individuals to receive notice and meaningfully challenge surveillance of their data.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.519.7804
F/212-549-2580
WWW.ACLU.ORG

E. Increasing Transparency

The *Schrems* decision makes clear that the CJEU is the ultimate arbiter of whether any new Safe Harbor agreement provides sufficient level of protection for E.U. individuals’ privacy. To ensure an adequate level of transparency, any new Safe Harbor agreement should be contingent on the United States’ disclosing the legal analysis of FISC opinions relating to the scope, access, and use of E.U. individuals’ data under Section 702; the number of Section 702 orders submitted to U.S. companies; and the number of E.U. accounts and individuals affected by Section 702 surveillance. The Executive Branch has previously supported legislation that included these transparency requirements.

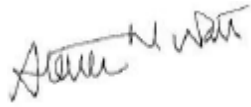
F. Additional Section 702 Reforms

In addition to the reforms noted above, the *Schrems* judgment offers the opportunity for Congress to examine other facets of Section 702 surveillance to address practices that violate the privacy and other human rights of U.S. and non-U.S. persons. Specifically, Congress should, at a minimum, require a warrant before acquiring, accessing, or using personal communications; close the “backdoor search loophole” permitting warrantless searching of Section 702 data for personal information; ensure standing for litigants to challenge Section 702 surveillance in Court; require notice when Section 702 information or evidence derived from it is introduced as evidence in a criminal, civil, or administrative proceeding; provide greater transparency and oversight; and reform the state secrets privilege, which acts as a barrier to judicial review of Section 702. Addressing these issues is necessary not only to protect the privacy and human rights of Americans and others around the world, but also to permit a new Safe Harbor agreement that will facilitate transatlantic data flows.

²⁹ See Letter from Electronic Privacy Information Center (EPIC) to Rep. Bob Goodlatte and Rep. John Conyers on H.R. 1428, the Judicial Redress Act of 2015 (Sept. 16, 2015), <https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf>.

If you have any questions, please contact Steven M. Watt, Senior Staff Attorney, at +1 212-519-7870 or swatt@aclu.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Steven M. Watt", written in a cursive style.

Steven Watt
Senior Staff Attorney, Human Rights Program
American Civil Liberties Union
swatt@aclu.org

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION**
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.519.7804
F/212-549-2580
WWW.ACLU.ORG

Exhibit D

Affaire T-738/16

LA QUADRATURE DU NET, FRENCH DATA NETWORK, FÉDÉRATION FDN

contre

COMMISSION EUROPÉENNE

**EXPERT REPORT OF ASHLEY GORSKI
ON BEHALF OF THE PLAINTIFFS**

TABLE OF CONTENTS

Qualifications and Duty of an Expert to The Court.....	ii
Introduction.....	1
I. Summary of Key Errors in the European Commission’s Privacy Shield Adequacy Decision	1
II. U.S. Surveillance Law and Practice	4
A. The U.S. Government Has Taken an Expansive and Unjustifiable View of the Surveillance Permitted by U.S. Law.....	6
B. The Foreign Intelligence Surveillance Act of 1978.....	9
C. Section 702 of the Foreign Intelligence Surveillance Act	11
D. How the U.S. Government Uses Section 702.....	14
E. Executive Order 12333	21
F. How the U.S. Government Uses Executive Order 12333.....	25
G. PPD-28.....	27
III. Inadequate Oversight	31
A. The Foreign Intelligence Surveillance Court.....	32
B. Congress.....	33
C. The Privacy and Civil Liberties Oversight Board.....	36
D. Inspectors General	38
IV. Obstacles to Redress	41
A. Notice, Standing, and the State Secrets Doctrine	41
B. U.S. Government Arguments Concerning the Applicability of the Fourth Amendment to Non-U.S. Persons Abroad.....	46
C. Other “Redress” Mechanisms Highlighted by the U.S. Government.....	47
1. Freedom of Information Act	47
2. Privacy Shield Ombudsperson.....	47
Conclusion	49

QUALIFICATIONS AND DUTY OF AN EXPERT TO THE COURT

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 1,600,000 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 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, a suit concerning Facebook's reliance on standard contractual clauses to transfer data from the E.U. to the United States.
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.

5. I was instructed by the Plaintiffs to provide an expert opinion on certain matters regarding the laws of the United States.
6. 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.
7. 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 Plaintiffs, other than any fees and expenses due in connection with my participation in the proceedings.

INTRODUCTION

8. I have been instructed by the Plaintiffs to opine on U.S. government surveillance law and practice, oversight mechanisms, and the barriers to achieving redress for rights violations resulting from U.S. foreign intelligence surveillance. In the first part of this report, I briefly summarize key errors in the European Commission’s Privacy Shield Adequacy Decision; in the second part, I discuss U.S. surveillance law and practice; in the third part, I describe the inadequacies of oversight mechanisms; and finally, in the fourth part, I discuss several of the barriers to redress.
9. 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, which I understand will be filed as exhibits with the Court.

I. SUMMARY OF KEY ERRORS IN THE EUROPEAN COMMISSION’S PRIVACY SHIELD ADEQUACY DECISION

10. Below, I briefly address four of the key errors in the Commission’s Adequacy Decision, with cross-references to the relevant sections of the report that discuss these issues in greater detail.¹

A. U.S. foreign intelligence surveillance is limited to what is “strictly necessary” and does not involve access to data on a “generalised basis.” Adequacy Decision ¶ 90.

This erroneous conclusion rests on five main misunderstandings about U.S. surveillance law and practice.

First, the U.S. government has access on a generalized basis to communications and data under Executive Order (“EO”) 12333 (**Ex. #2**). Relying on the executive order, the

¹ 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* (2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (“Adequacy Decision”) (**Ex. #1**).

government conducts a wide array of “bulk” or “mass” surveillance programs—including on fiber-optic cables carrying communications from the E.U. to the United States. *See infra* ¶¶ 51–62.

Second, the U.S. government has access on a generalized basis to communications under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) (**Ex. #3**). Through “Upstream” surveillance under Section 702, the National Security Agency (“NSA”) indiscriminately copies and then searches through vast quantities of personal metadata and content as it transits the Internet. In addition, the legal threshold for targeting non-U.S. persons under Section 702 is very low, and the number of targets is high—more than 100,000—resulting in the mass collection of hundreds of millions of communications per year. *See infra* ¶¶ 37–48.

Third, neither Section 702 nor EO 12333 surveillance is limited to what is strictly necessary. Both authorize the acquisition of “foreign intelligence,” a broad and elastic category. Under Section 702, “foreign intelligence” encompasses information related to the foreign affairs of the United States, which could include, for example, national health data or factors influencing the price of oil. Under EO 12333, “foreign intelligence” is defined even more broadly and encompasses information related to the “capabilities, intentions, or activities” of foreign persons. *See infra* ¶¶ 31, 53.

Fourth, the Adequacy Decision rests heavily on the assertion that the NSA touches only a fraction of communications on the Internet. But even if the NSA were intercepting and searching only 5% of global Internet communications, that would be an enormous volume in absolute terms, and it would still constitute “generalised” access to the portion of Internet communications that pass through the NSA’s surveillance devices. *See infra* ¶¶ 39, 48, 55–56, 61–62.

Fifth, even so-called “targeted” surveillance involves the collection and retention of vast amounts of non-targets’ private information. *See infra* ¶ 41.

B. *Presidential Policy Directive 28 ensures that U.S. foreign intelligence surveillance is limited to purposes that are “specific, strictly restricted, and capable of justifying the interference.” Adequacy Decision ¶¶ 89–90.*

As a procedural matter, the U.S. Department of Justice has taken the position that executive directives such as Presidential Policy Directive 28 (“PPD-28”) (**Ex. #4**) can be modified or revoked at any time, even in secret. As a substantive matter, PPD-28 in no way limits bulk collection; its limitations apply only to the *use* of information collected in bulk, and it allows the use of this information for detecting and countering broad categories of activities, including cybersecurity threats and transnational crime.

In addition, PPD-28’s limitations on the retention and dissemination of personal information are extremely weak. The directive provides that the government may retain or disseminate the personal information of non-U.S. persons only if retention or dissemination of comparable information concerning U.S. persons is permitted under EO 12333. Critically, however, 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,” which is defined to encompass information relating to the activities of foreign persons and organizations. *See infra* ¶¶ 63–74.

C. *U.S. foreign intelligence surveillance is subject to sufficient oversight. Adequacy Decision ¶¶ 67, 92–110.*

Existing oversight mechanisms are insufficient 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. Similarly, surveillance under Section 702 is not adequately supervised by the courts or by Congress. Other oversight mechanisms, such as the Privacy and Civil Liberties Oversight Board and Inspectors General, have only very limited authority and fail to compensate for the fundamental deficiencies in legislative and judicial oversight. *See infra* ¶¶ 75–98.

D. E.U. persons will have legal recourse for the U.S. government’s processing of personal data in the course of foreign intelligence surveillance. Adequacy Decision ¶ 111.

Virtually none of the individuals subject to Section 702 or EO 12333 surveillance will ever receive notice of that fact. As a result, 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. To date, as a result of the government’s invocation and judicial application of the standing and “state secrets” 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. *See infra* ¶¶ 99–112.

II. U.S. SURVEILLANCE LAW AND PRACTICE

11. The discussion in this section first sets forth the legal framework governing U.S. surveillance, to provide necessary context for the U.S. government’s claim that this surveillance is always conducted in accordance with the law and is “duly authorized.”² It then focuses on two of the most significant U.S. surveillance authorities: Section 702 of FISA, which authorizes warrantless surveillance that takes place on U.S. soil and targets foreigners; and EO 12333, which authorizes warrantless electronic surveillance that largely takes place abroad.³ After describing surveillance conducted under these two authorities, I discuss PPD-28, a directive issued by President Barack Obama in 2014 that has resulted in modest but insufficient reforms to surveillance law.

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) (“ODNI Letter”) (Ex. #5).

³ In the United States, a “warrant” is an order issued by a neutral and detached magistrate, based on probable cause, that authorizes a search or seizure. It must 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.

12. In describing the parameters of surveillance conducted under Section 702 and EO 12333, I do not intend to imply that these legal authorities—or the government’s 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. For the reasons I discuss in the fourth part of this report, there are significant barriers to challenging the lawfulness of this surveillance in civil litigation.
13. 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 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* ¶¶ 55–56, 61–62. 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* ¶¶ 31, 42, 53. In addition, in order to locate its targets’ communications, the government routinely searches the contents of countless communications in bulk.
14. As discussed below, under Section 702 and EO 12333, the U.S. obtains “generalised” access to the content of E.U.–U.S. communications, in violation of the Court of Justice’s decision in *Schrems v. Data Protection Commissioner* (C-362/14) (**Ex. #6**). In addition, Section 702’s and EO 12333’s broad authorizations to obtain “foreign intelligence information” from any foreigner do not satisfy the CJEU’s requirement that the government employ an “objective criterion” limiting surveillance to purposes that are “specific, strictly restricted and capable of justifying the interference,” and such broad authorizations infringe Europeans’ rights beyond what is “strictly necessary.”⁴

⁴ *See* Case C-362/14, *Schrems v. Data Protection Comm’r*, 2000 EUR-Lex 520 ¶¶ 93–94 (Oct. 6, 2015) (“*Schrems*”).

A. THE U.S. GOVERNMENT HAS TAKEN AN EXPANSIVE AND UNJUSTIFIABLE VIEW OF THE SURVEILLANCE PERMITTED BY U.S. LAW

15. In a letter annexed to the Privacy Shield agreement, the Office of the Director of National Intelligence (“ODNI”) explains that a “mosaic of laws and policies governs U.S. signals intelligence collection, and that this collection “must be undertaken in accordance with the Constitution and law.”⁵ However, as discussed below, the U.S. government has in the past taken an expansive view of the President’s authority to conduct foreign intelligence surveillance—even when that surveillance violates limitations imposed by other parts of the mosaic, including constitutional provisions and statutory law enacted by Congress.
16. 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.
17. The Fourth Amendment to the U.S. Constitution provides the baseline legal protection for privacy from government surveillance. Under the Fourth Amendment, searches and seizures must be “reasonable.” 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) (**Ex. #7**). 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) (**Ex. #8**); *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297, 316 (1972) (**Ex. #9**).

⁵ ODNI Letter at 3.

18. Yet the U.S. government contends, incorrectly, that the Fourth Amendment typically does not protect non-U.S. persons outside the United States. *See infra* ¶ 112. It also 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.⁶
19. 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 the Foreign Intelligence Surveillance Act of 1978, including Section 702 of that act, adopted in 2008.
20. However, 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 NSA to monitor and collect communications between foreigners and U.S. persons inside the United States without first obtaining judicial authorization, as required at the time by FISA. 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.”⁷ The Bush administration also claimed that when Congress passed the Authorization to Use Military Force (“AUMF”) following September 11th, 2001, it effectively authorized him to conduct whatever surveillance he deemed necessary in fighting international terrorism, regardless of the constraints of FISA or other statutory law.⁸ The AUMF is still in force today.⁹

⁶ *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 (**Ex. #10**).

⁷ 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.”) (**Ex. #11**).

⁸ *See* Ellen Nakashima, *Legal Memos Released on Bush-era justification for warrantless wiretapping*, Wash. Post, Sept. 6, 2014, <https://www.washingtonpost.com/world/national->

21. 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 was deeply controversial. Nonetheless, Congress largely allowed the practice of warrantless surveillance of international communications for foreign intelligence purposes to continue, and even expanded the government’s ability to conduct warrantless surveillance, while adding certain restrictions and limitations.¹⁰ Congress enshrined this surveillance scheme in Section 702.
22. 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.¹¹
23. 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.

security/legal-memos-released-on-bush-era-justification-for-warrantlesswiretapping/2014/09/05/91b86c52-356d-11e4-9e92-0899b306bbea_story.html (Ex. #12).

⁹ 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> (Ex. #13).

¹⁰ I use the term “international” to describe communications that either originate or terminate outside the United States, but not both.

¹¹ 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> (Ex. #14). 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) (Ex. #15).

B. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

24. 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 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) (**Ex. #16**). 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.¹²
25. 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) (**Exs. #19–21**).¹³ To obtain a 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) (**Ex. #22**).
26. 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

¹² 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 (**Ex. #17**). 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> (**Ex. #18**).

¹³ Some kinds of foreign intelligence surveillance were left unregulated by FISA and are conducted under the auspices of EO 12333. *See infra* ¶¶ 51–62.

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).

27. The basic framework established by FISA, which I refer to below as “traditional” 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 described below. These amendments include the provision known as Section 702 of FISA. *See* 50 U.S.C. § 1881a.
28. 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.¹⁴ 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.¹⁵

¹⁴ *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> (**Ex. #23**); 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> (**Ex. #24**); 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 (**Ex. #25**).

¹⁵ *See* ODNI Letter at 10 n.12 (discussing traditional FISA). The ODNI 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 2016, even “targeted” collection under FISA’s business record authority, 50 U.S.C. § 1861(b)(2)(C), resulted in the acquisition of more than 150,000,000 “call detail records.” ODNI, *Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016* at 20 (Apr. 2017), https://www.dni.gov/files/icotr/ic_transparency_report_cy2016_5_2_17.pdf (“ODNI Statistical Transparency Report”) (**Ex. #26**).

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

C. SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

30. 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.¹⁶ 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.
31. 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.¹⁷ 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.”¹⁸ The statute

¹⁶ In August 2007, Congress passed a predecessor statute, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (**Ex. #27**). Those authorities expired in February 2008.

¹⁷ See 50 U.S.C. § 1801(i) (defining “United States person”).

¹⁸ The U.S. government’s foreign intelligence surveillance is not limited to national security purposes. See ODNI 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 Adequacy Decision ¶¶ 76, 88 & n.97. It also characterizes the acquisition of foreign intelligence information as a “legitimate policy objective” within the meaning of *Schrems*,

defines “foreign intelligence information” broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e).

32. 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.¹⁹ Rather than individually review the executive branch’s targets or selectors, the FISC instead reviews, on an annual basis, government “certifications” that seek approval of broad categories for foreign intelligence surveillance. *See* 50 U.S.C. § 1881a(i). Although the ODNI Letter states that the government’s certifications identify “specific categories” of foreign intelligence,²⁰ documents show that these categories are in fact quite expansive, including topics such as counterterrorism, weapons of mass destruction, and foreign governments.²¹ According to a leaked version of the “foreign governments” certification, the FISC has permitted surveillance related to more than 190 different countries.²²
33. 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). By design, these “targeting” and “minimization” procedures give the government broad latitude to analyze and disseminate both U.S. and non-U.S. persons’ communications. *Id.* § 1881a(d)–(g). Targeting procedures must be reasonably designed to ensure that government agents are

see id. ¶ 89 & n.97, despite the fact that the *Schrems* opinion referred specifically to “national security” as a legitimate policy objective. *See Schrems* ¶ 88.

¹⁹ *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) (**Ex. #28**).

²⁰ ODNI Letter at 10.

²¹ *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 (**Ex. #29**).

²² 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> (**Ex. #30**). News reports indicate that the NSA has relied on the foreign governments certification to search for addresses and 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> (**Ex. #31**).

“targeting persons reasonably believed to be located outside the United States,” and are avoiding the “intentional acquisition” of purely domestic communications. *Id.* at § 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.* at §§ 1801(h) (emphasis added), 1881a(e). Although the ODNI Letter cites to these procedures as privacy safeguards, in practice, the procedures are weak and riddled with exceptions;²³ moreover, they are not designed to provide any safeguards for E.U. persons outside the United States, as discussed in greater detail *infra*.²⁴

34. 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,

²³ 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”) (Ex. #32); 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”) (Ex. #33).

²⁴ 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”) (Ex. #34). 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 Court ha[d] not requested additional tasking sheets or queries beyond what was provided in January and May 2015.” PCLOB, *Recommendations Assessment Report* 19 (Feb. 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf (Ex. #35).

Section 702 permits the government to target *any* non-U.S. person located outside the United States to obtain foreign intelligence information.

35. 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.²⁵
36. 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 or entity in the United States and a non-U.S. person abroad—to potential surveillance. The statute contains no express protections for the privacy of non-U.S. persons located abroad.

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

37. Official government disclosures show that the government uses Section 702 to conduct at least two types of surveillance: “Upstream” surveillance and “PRISM” surveillance.²⁶ Given the broad parameters of Section 702, the government may rely on the statute to conduct other still-secret surveillance programs as well.
38. 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.²⁷ The government identifies the user accounts it wishes to monitor, and

²⁵ 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”) (**Ex. #36**).

²⁶ 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”) (**Ex. #37**).

²⁷ See PCLOB Report 33–34; [Redacted], No. [Redacted], 2011 WL 10945618, at *9–10 & n.24 (FISC Oct. 3, 2011) (**Ex. #38**); *NSA Program Prism Slides*, Guardian, Nov. 1, 2013,

then orders the provider to disclose to it all communications to or from those accounts.²⁸ As of April 2013, the NSA was monitoring at least 117,675 targeted accounts via PRISM.²⁹

39. 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 U.S. persons and others around the world. When conducting this surveillance, the NSA searches the metadata and content of international Internet communications transiting the links that it monitors.³⁰ The agency searches for key terms, called “selectors,” that are associated with more than 100,000 foreign 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.³¹ Communications to and from selectors—as well as those that happen to be bundled with them in transit—are

<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) (**Ex. #39**).

²⁸ 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 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.”) (**Ex. #40**).

²⁹ *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/> (**Ex. #41**).

³⁰ *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> (**Ex. #42**); 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> (**Ex. #43**).

³¹ *See, e.g.*, Savage, *supra* note 22.

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 then searches the vast quantities of personal metadata and content passing through its surveillance devices.³²

40. 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.³³ Although the precise number of communications retained today under Section 702 is not public, the Privacy and Civil Liberties Oversight Board observed in 2014 that “[t]he current number is significantly higher.”³⁴ 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”,³⁵ by contrast, in 2016, the government targeted the communications of 106,469 individuals, groups, and organizations—most of whom are undoubtedly associated with multiple Internet accounts or “unique selectors.”³⁶ 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,

³² 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> (Ex. #44).

³³ See [Redacted], 2011 WL 10945618, at *9–10; PCLOB Report 111 n.476.

³⁴ PCLOB Report 116.

³⁵ 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) (Ex. #45).

³⁶ ODNI Statistical Transparency Report at 7 (disclosing that the government targeted 106,469 different individuals, groups, and organizations under Section 702 in 2016).

they are subject to interception and retention by communications providers acting at the direction of the U.S. government.³⁷

41. 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 intended surveillance targets but were caught in a net the agency had cast for somebody else."³⁸ 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."³⁹ 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.

³⁷ 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.

³⁸ 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 (Ex. #46).

³⁹ *Id.*

42. The U.S. government has recently published partially redacted versions of its Section 702 targeting procedures for the Federal Bureau of Investigation (“FBI”) and NSA.⁴⁰ As contemplated under 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).⁴¹ This is a very low threshold in light of the statute’s broad definition of “foreign intelligence information.” 50 U.S.C. § 1801(e).
43. 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.⁴² 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.⁴³ During that time, the communications may be reviewed and queried by analysts in both intelligence and criminal investigations.⁴⁴

⁴⁰ 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 (Ex. #47); NSA Section 702 Targeting Procedures.

⁴¹ NSA Section 702 Targeting Procedures at 4.

⁴² 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> (Ex. #48).

⁴³ 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.

⁴⁴ 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),

44. Under Section 702, the U.S. government claims it has 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 several years, the government engaged in this collection—known as “about” collection—as part of Upstream surveillance. As discussed below, although the government has halted “about” collection for the time being, there is no indication that the NSA now lacks generalized access to the content of communications via Upstream surveillance under Section 702.
45. Earlier this year, the U.S. government released a partially redacted version of an April 2017 FISC opinion addressing the government’s submissions seeking reauthorization to conduct surveillance under Section 702. The FISC’s opinion describes the NSA’s decision to modify “about” collection under the statute.⁴⁵ In October 2016, the government orally apprised the FISC of “significant non-compliance with the NSA’s minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers.”⁴⁶ Specifically, “with greater frequency than had previously been disclosed to the Court,” 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.”⁴⁷ 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.⁴⁸ Over the following months, the government filed several written submissions with the FISC concerning Upstream-related compliance violations. In light of these serial violations, the FISC twice extended the deadline for its consideration of the government’s annual Section 702 certifications, though it allowed the surveillance to continue in the interim, notwithstanding these systematic violations.⁴⁹

https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf (**Ex. #49**).

⁴⁵ 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 (**Ex. #50**).

⁴⁶ *Id.* at 4.

⁴⁷ *Id.* at 15, 19.

⁴⁸ *Id.* at 19 (quoting hearing transcript).

⁴⁹ *Id.* at 19–23.

46. In March 2017, the government informed the FISC that it had chosen a new course: rather than have the FISC rule on the validity of the targeting and minimization procedures that it had previously submitted for the FISC’s approval in September 2016, the government filed revised certifications, NSA targeting procedures, and NSA minimization procedures. These amendments changed how the NSA would conduct “about” collection.
47. Until this change, when the NSA conducted Upstream surveillance, it acquired international Internet communications to, from, *and about* its selectors. According to the FISC’s opinion, “the government will eliminate ‘abouts’ collection altogether.”⁵⁰ Similarly, the NSA’s revised targeting procedures state that Section 702 “[a]cquisitions . . . will be limited to communications to or from persons targeted.”⁵¹ Thus, as a result of the NSA’s change in its policy under Section 702, it can (for now) “collect” or “acquire” for the government’s long-term retention and use only those Internet communications that are to or from a target, and not those that are merely “about” a target—with some exceptions.⁵²
48. Notably, however, the FISC’s opinion and the NSA’s new procedures do not describe in any detail how the NSA will end its acquisition of “about” communications. Previously, in the course of Upstream surveillance, the NSA copied and searched the full contents of communications transiting the international Internet links monitored by the agency.⁵³ Although the opinion and new procedures state that the NSA will not “acquire” or “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

⁵⁰ *Id.* at 23.

⁵¹ *Id.* at 25.

⁵² *Id.* at 27. Within government agencies, “collect” and “acquire” are terms of art with very particular meanings. 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) expressly defines “collection” as excluding “[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> (**Ex. #51**).

⁵³ 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 30; Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, *supra* note 30.

equipment 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. 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.⁵⁴
50. Importantly, the NSA’s change in policy does not affect collection under EO 12333.

E. EXECUTIVE ORDER 12333

51. EO 12333 is the primary authority under which the NSA gathers foreign intelligence.⁵⁵ 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 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.⁵⁶ 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,

⁵⁴ See Press Release, NSA, *supra* note 26.

⁵⁵ EO 12333, as amended, *available at* <https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333>.

⁵⁶ 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 (Ex. #52). 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. 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 (Ex. #53); Charlie Savage, *Power Wars Document: Transit Authority and the 1990 Lawton Surveillance Memo* (Nov. 18, 2015), <http://www.charliesavage.com/?p=557> (Ex. #54).

including U.S. Signals Intelligence Directive 0018 (“USSID 18”) and other agency policies.⁵⁷ In addition, as discussed in greater detail below, PPD-28 and its associated agency policies further regulate EO 12333 activities.

52. 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, with particular emphasis on countering terrorism, espionage, and weapons of mass destruction.⁵⁸ EO 12333 authorizes surveillance for a broad range of purposes, 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.
53. 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”).
54. In addition, EO 12333 and its implementing regulations permit at least two forms of bulk surveillance.⁵⁹

⁵⁷ *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> (**Ex. #55**); *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) (**Ex. #56**).

⁵⁸ *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.”).

⁵⁹ *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”).

55. 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.⁶⁰ But there is no question that EO 12333 permits collection of electronic communications in bulk. Even if this collection filters out, for example, all video traffic, bulk collection is indiscriminate by definition, as it is “acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).”⁶¹ Thus, these policies plainly contemplate “access on a generalised basis to the content of electronic communications,” in violation of *Schrems v. Data Protection Commissioner*.⁶²
56. The 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.”⁶³ But the U.S. government’s foreign intelligence objectives are broadly defined, *see infra* ¶ 59, 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.”
57. 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

⁶⁰ 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”) (Ex. #57).

⁶¹ PPD-28 n.5.

⁶² *Schrems* ¶¶ 93–94.

⁶³ Adequacy Decision ¶ 73.

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.

58. 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.⁶⁴
59. Although the ODNI Letter emphasizes that intelligence analysts are constrained by the National Intelligence Priorities Framework (“NIPF”),⁶⁵ 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.⁶⁶ 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.⁶⁷ 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

⁶⁴ 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”).

⁶⁵ ODNI Letter at 6, 8; see also Adequacy Decision ¶ 70.

⁶⁶ *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-930205-2.html> (Ex. #58); 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”) (Ex. #59).

⁶⁷ 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> (Ex. #60).

technologies, highly developed conventional weapons and international trade, which all have priority ‘4.’”⁶⁸ With foreign intelligence priorities this broad, individual analysts have tremendous latitude in conducting surveillance.

60. 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;⁶⁹ (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 “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.⁷⁰

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

61. 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;⁷¹ its acquisition of 200 million text messages from around the world each day;⁷² its recording

⁶⁸ *Id.*

⁶⁹ 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).

⁷⁰ See *infra* ¶ 74.

⁷¹ 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 (**Ex. #61**).

⁷² James Ball, *NSA Collects Millions of Text Messages Daily in ‘Untargeted’ Global Sweep*, The Guardian, Jan. 16, 2014, <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep> (**Ex. #62**).

of every single cell phone call into, out of, and within at least two countries;⁷³ its collection of hundreds of millions of contact lists and address books from personal email and instant-messaging accounts;⁷⁴ and its surreptitious interception of data from Google and Yahoo user accounts as that information travelled between those companies' data centers located abroad.⁷⁵

62. 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.⁷⁶ 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.*”⁷⁷ In other words, as data is transferred from the E.U. to the United States, the U.S. government may access that data on a “generalised basis,” without an “objective criterion” limiting EO 12333 surveillance to purposes that are “specific, strictly restricted and capable of justifying the interference”—and the infringement of Europeans’ rights goes beyond what is “strictly necessary.”⁷⁸

⁷³ 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> (Ex. #63).

⁷⁴ 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 (Ex. #64).

⁷⁵ 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 (Ex. #65).

⁷⁶ 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> (Ex. #66).

⁷⁷ Adequacy Decision ¶ 75 (emphasis added).

⁷⁸ See Schrems ¶¶ 92–93.

G. PPD-28

63. 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.
64. 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. In addition, a recently released court decision holds that PPD-28 does not create any enforceable rights, underscoring yet another way in which the directive does not adequately safeguard the rights of individuals in the E.U.⁷⁹ In June 2017, the U.S. government released a partially redacted version of a 2014 FISC opinion addressing a U.S. electronic communication service provider’s challenge to Section 702.⁸⁰ The provider argued that the FISC should consider the interests of non-U.S. persons abroad when evaluating the lawfulness of Section 702 surveillance—citing, among other sources, PPD-28.⁸¹ But the court deemed these interests irrelevant, in part because PPD-28, “by its terms, is not judicially enforceable.”⁸² 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 IV, *infra*.

⁷⁹ See *infra* ¶¶ 65–74 (discussing shortcomings of PPD-28).

⁸⁰ See ODNI, *Additional Release of FISA Section 702 Documents*, IC on the Record (June 14, 2017), <https://icontherecord.tumblr.com/post/161824569523/additional-release-of-fisa-section-702-documents>. The 2014 FISC opinion is available at <https://www.dni.gov/files/documents/icotr/702/Bates%20510-548.pdf> (“2014 FISC Op.”) (Ex. #67).

⁸¹ See 2014 FISC Op. at 36.

⁸² *Id.*

1. PPD-28's Principles

65. 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.”⁸³
- “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.”⁸⁴
- “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.”⁸⁵
- “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.”⁸⁶

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

⁸³ PPD-28 § 1.

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.*

2. PPD-28 and Bulk Collection

67. 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.
68. Taken together, these categories are very broad and open to interpretation, and they effectively ratify the practice of bulk, indiscriminate surveillance.
69. 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 under EO 12333, Section 702, and traditional FISA, as described in paragraphs 28, 39, and 57 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.).”⁸⁷ This definition explicitly excludes data that is “temporarily acquired to facilitate targeted collection.”⁸⁸ 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.

⁸⁷ *Id.* § 2 n.5.

⁸⁸ *Id.*

3. PPD-28 and Retention, Dissemination, and Use

70. 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.
71. 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 12333.⁸⁹ 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 12333.⁹⁰
72. 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.⁹¹ 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).
73. Further, with respect to storage and dissemination, PPD-28 does not extend the same protections to foreigners as to U.S. persons, as the Adequacy Decision claims.⁹² 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

⁸⁹ *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."

⁹⁰ PPD-28 § 4(a)(i).

⁹¹ 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.).

⁹² *See* Adequacy Decision ¶ 85.

importance.”⁹³ 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.⁹⁴

74. 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.⁹⁵

III. INADEQUATE OVERSIGHT

75. The U.S. legal system provides three main avenues for intelligence oversight: internal oversight, legislative oversight by Congress, and judicial oversight by the courts. Oversight is a critical part of ensuring that intelligence activities comply with the law.
76. Despite the ODNI Letter’s characterization of foreign intelligence oversight as “rigorous,”⁹⁶ 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.⁹⁷ Similarly, surveillance under Section 702 is not adequately supervised by the courts or by Congress. Other oversight mechanisms, such as the Privacy and Civil Liberties Oversight Board and Inspectors General, have only very limited authority and fail to compensate for fundamental deficiencies in judicial and legislative oversight.

⁹³ USSID 18 § 7.2; *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”).

⁹⁴ NSA PPD-28 Section 4 Procedures § 7.2.

⁹⁵ NSA PPD-28 Section 4 Procedures §§ 6–7.

⁹⁶ ODNI Letter at 7.

⁹⁷ 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-nasas-data-collection-authorized.html> (**Ex. #68**).

A. THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

77. The FISC has not been effective at preventing even 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.
78. After the FISC first learned that the NSA had violated the rules governing various mass surveillance programs conducted over the past several years, 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.”⁹⁸ 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.”⁹⁹
79. 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.¹⁰⁰ 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.

⁹⁸ [Redacted], 2011 WL 10945618, at *5 & n.14.

⁹⁹ *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9150913, at *5 (FISC Mar. 2, 2009) (**Ex. #69**).

¹⁰⁰ 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.

80. 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 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.¹⁰¹ The 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."¹⁰²
81. Finally, because neither Section 702 nor its procedures afford any express protection to foreigners who are located abroad, the FISC's oversight does not give any consideration to the rights of those persons.¹⁰³

B. CONGRESS

82. 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. Senator Richard J. Durbin has explained that, even when legislators are briefed by intelligence officials, only the most senior leaders are kept abreast of intelligence activities. "You can count on two hands the number of people in Congress who really know," he told the *New York Times*.¹⁰⁴ These committees, in turn,

¹⁰¹ *Id.* at 68–95.

¹⁰² *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) (Ex. #70).

¹⁰³ 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.

¹⁰⁴ 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> (Ex. #71).

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.¹⁰⁵ More generally, members of Congress—including on the Senate Intelligence Committee—have been repeatedly thwarted when attempting to obtain information about NSA surveillance.¹⁰⁶ According to Senator Patrick Leahy, lawmakers often get more accurate information from newspapers.¹⁰⁷ Even when legislators obtain relevant classified information, they are 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.

83. 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

¹⁰⁵ 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 (Ex. #72); 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> (Ex. #73).

¹⁰⁶ 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> (Ex. #74); 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> (Ex. #75).

¹⁰⁷ 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-leahy-nsa_n_4030514.html (Ex. #76); 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> (Ex. #77); 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> (Ex. #78).

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 (**Ex. #79**).¹⁰⁸ 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.¹⁰⁹ This policy makes it extremely difficult for members of Congress, including Democrats sitting on relevant committees, to conduct meaningful oversight of foreign intelligence surveillance.

84. 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 community and the NSA to provide such an estimate.¹¹⁰ The Inspectors General initially dismissed the idea, contending that it would take too many resources and would itself violate Americans' privacy, because the NSA would have to closely examine the content of calls and emails to determine whether the participants were Americans. In October 2015, a bipartisan coalition of 32 organizations dedicated to preserving privacy and civil liberties wrote to the then-Director of National Intelligence, James Clapper, to make clear that the privacy community supported producing this estimate, and to suggest how the estimate could be obtained in a manner that would protect civil liberties.¹¹¹

¹⁰⁸ 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> (**Ex. #80**).

¹⁰⁹ 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> (**Ex. #81**).

¹¹⁰ 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 (**Ex. #82**).

¹¹¹ Letter from Privacy and Civil Liberties Coalition to the Hon. James R. Clapper, Director, ODNI (Oct. 29, 2015), https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf (**Ex. #83**).

85. After years of advocacy by these NGOs and continued requests from Congress, DNI Clapper committed to providing the estimate.¹¹² However, the Trump administration has now reneged on that commitment, despite the fact that Congress is considering whether to reauthorize Section 702, and this estimate would play an important role in the reauthorization debate by illuminating the breadth of the government’s surveillance under the statute.¹¹³

C. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

86. As part of its Adequacy Decision, the European Commission relied on assurances that the U.S. intelligence community was subject to various executive-branch oversight mechanisms, including the Privacy and Civil Liberties Oversight Board (“PCLOB”). The Adequacy Decision emphasizes that the PCLOB is an independent body that oversees U.S. surveillance practices by examining relevant records, issuing recommendations, hearing testimony, and preparing reports.¹¹⁴ However, at present, the PCLOB is not a fully functional body, and recent events undermine the Commission’s conclusion that it is an independent oversight mechanism.

87. Today, four of the five PCLOB board positions are vacant.¹¹⁵ Without a quorum, the PCLOB cannot issue reports and recommendations, including its planned report on activities conducted under EO 12333.¹¹⁶ In addition, the Board is further limited in its

¹¹² 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> (Ex. #84).

¹¹³ 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/e74f7f7be-4b88-11e7-a186-60c031eab644_story.html (Ex. #85); 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 (Ex. #86).

¹¹⁴ Adequacy Decision ¶¶ 95, 98.

¹¹⁵ *Board Members*, Privacy and Civil Liberties Oversight Board, <https://www.pclob.gov/board-members/> (accessed Dec. 19, 2017) (Ex. #87).

¹¹⁶ *See also* 6 C.F.R. § 1000.3 (2013), available at <https://www.pclob.gov/library/FederalRegister-PCLOB-2013-0005-Delegation-Reg.pdf> (Ex. #88).

ability to make staffing decisions necessary to fulfill its responsibilities.¹¹⁷ 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.¹¹⁸ The current membership, however, represents only one political party. 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. Indeed, the PCLOB remained largely dormant from 2007 to 2012 due in part to these hurdles.

88. 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.
89. Recent events also undermine the Adequacy Decision’s conclusion 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 declassified, it was also explained that this report cannot be released to the public, as it is currently subject to Presidential privilege.”¹¹⁹ If the President can assert privilege over the PCLOB’s reports to prevent those documents from being distributed—a proposition that seems legally dubious at best—it cuts off one of the PCLOB’s few powers: the ability to issue public reports.
90. Finally, the scope of the PCLOB’s mandate may be limited by Congress. Last year, Senators considered legislation that would bar the PCLOB from considering the privacy and civil liberties interests of non-U.S. persons.¹²⁰

¹¹⁷ *Id.*

¹¹⁸ *See* 42 U.S.C. § 2000ee(h)(2) (**Ex. #89**).

¹¹⁹ First Annual Review at 31.

¹²⁰ 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> (**Ex. #90**).

D. INSPECTORS GENERAL

91. The Adequacy Decision discusses the significance of Inspectors General (“IGs”) as a mechanism for overseeing foreign intelligence surveillance, notwithstanding their inability to issue binding recommendations.¹²¹ Although IGs have a critical role to play in the oversight ecosystem, the Adequacy Decision overstates the independence of IGs in three respects. It also fails to account for the scope of a typical IG investigation and for recent troubling news about the U.S. intelligence community’s Office of the Inspector General.
92. First, in support of its claim that IGs are independent, the Adequacy Decision states that IGs have “secure tenure.”¹²² However, IGs can be removed by the President without cause.¹²³ Congress must be notified in those circumstances, but this notification requirement does not provide Congress with legal authority to oppose or override the termination. Historically, IGs have been protected by political norms, including the norm that new Presidents do not dismiss existing IGs without cause. Yet the force of these norms is uncertain under President Trump’s administration. Indeed, members of Congress wrote to the White House following reports that the Trump administration transition team threatened to fire several IGs in advance of the inauguration.¹²⁴ Thus, it overstates the case considerably to say that IGs have “secure tenure.”
93. Second, the Adequacy Decision claims that IGs have great liberty to conduct investigations and obtain evidence, except where limits are “necessary to preserve important national (security) interests.”¹²⁵ In fact, however, the ability of IGs to gather evidence is limited in a number of significant ways.

¹²¹ Adequacy Decision ¶ 97.

¹²² *Id.* ¶ 97 n.110.

¹²³ 5 U.S.C. App. 3 Sec. 3 (**Ex. #91**).

¹²⁴ Letter from Rep. Elijah E. Cummings & Rep. Gerald E. Connolly to Donald F. McGahn, White House Counsel (Jan. 31, 2017), <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2017-01-31.EEC%20Connolly%20to%20white%20house%20counsel%20McGahn%20Re.Trump%20Transition%20Team%20threats%20to%20IGs.pdf> (**Ex. #92**).

¹²⁵ Adequacy Decision ¶ 97 n.110.

94. 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. In addition, media reports suggest that institutional cultures within the intelligence community discourage whistleblowing. According to the Project on Government Oversight, just last year, an intelligence community review panel concluded that NSA IG George Ellard had retaliated against an NSA whistleblower.¹²⁶ Despite that fact, Ellard kept his job—raising serious concerns about an anti-whistleblower culture within the Department of Defense.¹²⁷ Similarly, the acting head of the CIA’s Office of Inspector General reportedly has several outstanding whistleblower retaliation complaints against him.¹²⁸
95. 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.”¹²⁹ Although the Inspector General Empowerment Act of 2016 has improved IGs’ access to information, Horowitz emphasized that IGs still face difficulties obtaining the information they require.¹³⁰ Some agencies fail to timely supply access to critical records, and IGs lack

¹²⁶ 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> (**Ex. #93**).

¹²⁷ Patrick G. Eddington, *Why is Mattis Declaring War on Whistleblowers?*, American Conservative, Aug. 3, 2017, <http://www.theamericanconservative.com/articles/why-is-mattis-declaring-war-on-whistleblowers> (**Ex. #94**).

¹²⁸ 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> (**Ex. #95**).

¹²⁹ 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> (**Ex. #96**).

¹³⁰ *Id.* at 3, 6.

the authority to subpoena witnesses to testify.¹³¹ Horowitz also observed that Department of Justice (“DOJ”) attorneys—including those who interpret surveillance law and thereby grant internal approval to surveillance programs—are insulated from independent IG oversight. The Department of Justice IG oversees DOJ employees, but not DOJ lawyers, who are under the investigative authority of the DOJ’s Office of Professional Responsibility. As a result, “misconduct by DOJ [lawyers acting in a legal capacity] is investigated by a component head who is appointed by the Department’s leadership and who lacks statutory independence.”¹³²

96. Third, recent events highlight the obstacles that IGs may face in publishing reports documenting official wrongdoing. In November 2017, the Department of Homeland Security Inspector General informed Congress that the agency is blocking the release of his report concerning President Trump’s directive to suspend travel to the U.S. by citizens of seven majority-Muslim countries. The report found that Customs and Border Protection officials violated two court orders that had limited the implementation of the directive.¹³³
97. 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 not typically assess whether a particular surveillance program authorized by senior executive branch officials or the President is constitutional.¹³⁴
98. Finally, in addition to these structural limitations, the central Office of the Inspector General for the U.S. intelligence community is reportedly in disarray.¹³⁵ This IG’s office was created in 2010 to launch independent audits and investigations across intelligence

¹³¹ *Id.*

¹³² *Id.* at 6–7.

¹³³ Josh Gerstein et al., *Watchdog Says Homeland Security Bottling Up Travel Ban Report*, Politico, Nov. 20, 2017, <https://www.politico.com/story/2017/11/20/homeland-security-travel-ban-253902> (**Ex. #97**).

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) (**Ex. #98**).

¹³⁵ McLaughlin, *supra* note 128.

agencies. However, it is “in danger of crumbling thanks to mismanagement, bureaucratic battles, clashes among big personalities, and sidelining of whistleblower outreach and training efforts.”¹³⁶ As of October 2017, the head of whistleblower outreach within the office had been barred from communicating with whistleblowers, could no longer brief agencies or congressional committees on his work, could not conduct outreach, and had no deputy or staff.¹³⁷

IV. OBSTACLES TO REDRESS

99. The Adequacy Decision states that “[a] number of avenues are available under U.S. law to EU 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”).¹³⁸ 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

100. 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

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ Adequacy Decision ¶ 111.

provisions cited in the Adequacy Decision and ODNI Letter: 50 U.S.C. § 1810, 18 U.S.C. § 2712, 18 U.S.C. § 1030, and 12 U.S.C. § 3417 (**Exs. #99–102**).¹³⁹

101. 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.¹⁴⁰

102. 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. The sole exception is when the government intends to use information against an “aggrieved person” in a trial or proceeding where that information

¹³⁹ Adequacy Decision ¶ 115; ODNI Letter at 16–17.

¹⁴⁰ Other collection authorities raise similar issues. For example, National Security Letters, a type of secret administrative subpoena, allow the FBI to obtain certain information in credit reports, financial records, and electronic subscriber and transaction records from particular types of companies. Although recipient companies can seek to challenge these subpoenas in court, National Security Letters typically gag companies from informing customers that their data is being sought and from otherwise discussing the letters. *See* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u–1681v; 18 U.S.C. § 2709; 18 U.S.C. § 3511; 50 U.S.C. § 3162 (**Exs. #103–107**). In 2015, Congress required the FBI to periodically review the National Security Letters it has issued to ascertain whether prior gag orders are still necessary, but statistics concerning the outcome of these reviews are unavailable. As another example, the Stored Communications Act allows the government to obtain certain records and information from providers of electronic communications services or remote computing services related to their customers or subscribers. *See* 18 U.S.C. §§ 2701–2712 (**Ex. #108**). Under the statute, the government can obtain a protective order to prohibit providers from notifying their users about the receipt of legal process. *See* 18 U.S.C. § 2705(b). The Department of Justice has recently issued guidance to limit the routine use of these gag orders, but that guidance has not been codified into law, and state and local authorities are not bound by this guidance when making demands for information in consumer accounts. *See* Ali Cooper-Ponte, *Modernizing ECPA: We Need Congressional Action Despite DOJ’s New Gag Order Guidelines*, Just Security, Nov. 8, 2017, <https://www.justsecurity.org/46875/modernizing-ecpa-congressional-action-doj-gag-order-guidelines> (**Ex. #109**).

was obtained or derived from FISA.¹⁴¹ In those circumstances, the government is statutorily required to provide notice.¹⁴² However, for five years after the enactment of Section 702, the Department of Justice failed to provide notice to a single criminal defendant, based on a notice policy that the Department has never publicly disclosed.¹⁴³ Though the Department claims to have changed that policy after concluding that it could not be legally justified, the new policy remains secret, as 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.¹⁴⁴

103. 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.
104. 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

¹⁴¹ 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) (**Ex. #110**).

¹⁴² *See, e.g.*, 50 U.S.C. § 1806 (**Ex. #111**).

¹⁴³ Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 26, 2013, <http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html> (**Ex. #112**).

¹⁴⁴ 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.”) (**Ex. #113**).

likelihood that the injury will be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (**Ex. #114**). 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.

105. 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) (**Ex. #115**).
106. Following the ruling in *Clapper*, the ACLU brought suit on behalf of 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. NSA*, 143 F. Supp. 3d 344, 356 (D. Md. 2015) (**Ex. #116**). Among other things, the court held that Wikimedia had not plausibly alleged that any of its international communications—more than one trillion per year, with individuals in virtually every country on earth—were subject to Upstream surveillance.
107. In May 2017, the Court of Appeals for the Fourth Circuit reversed the district court’s opinion with respect to Wikimedia, but it affirmed the district court’s dismissal of the claims of the eight other plaintiffs, who include Amnesty International USA, Human Rights Watch, and the National Association of Criminal Defense Lawyers. *See Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017) (**Ex. #117**). Despite the breadth of Upstream surveillance, the Fourth Circuit rejected as implausible the standing claims of these other plaintiffs who engage in substantial quantities of international communications as an essential part of their work—including sensitive communications with and about individuals likely targeted by the NSA for surveillance.

108. Importantly, the Fourth Circuit did not hold that Wikimedia has established standing as a matter of fact, nor did it consider whether Upstream surveillance is lawful. Those questions have yet to be litigated. Rather, the Fourth Circuit in *Wikimedia* was evaluating, as a threshold matter, whether the plaintiffs’ complaint contained sufficient allegations for the case to go forward. Its analysis simply considered whether the plaintiffs’ allegations of standing were “plausible.” A plaintiff that prevails on this threshold question must still present evidentiary material that establishes its standing as a matter of fact. Thus, the government will have another opportunity to challenge Wikimedia’s standing—this time as a factual matter. The government’s routine insistence that civil plaintiffs lack standing to sue is one of the ways in which it has repeatedly blocked U.S. courts from considering the lawfulness of surveillance conducted under Section 702.¹⁴⁵
109. Given the Fourth Circuit’s holding in *Wikimedia v. NSA* that eight of the nine plaintiffs lacked standing, its 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. E.U. human rights and legal organizations that routinely engage in sensitive E.U.–U.S. communications in the course of their work—and ordinary E.U. persons who communicate with friends or family in the U.S.—will not receive notice from the U.S. government that they have been surveilled pursuant to Section 702 or EO 12333. Even where there are strong reasons to believe that one has been subject to this surveillance, the standing doctrine is a significant obstacle to redress.
110. Yet standing doctrine is not the only obstacle to redress. In addition, 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) (**Ex. #119**). In recent years, however, the government has successfully used the state

¹⁴⁵ *See, e.g., Clapper*, 568 U.S. 398 (challenging the factual basis for plaintiffs’ standing); *Jewel v. NSA*, No. 08-04373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015) (challenging the factual basis for plaintiffs’ standing and invoking the state secrets privilege) (**Ex. #118**).

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) (**Ex. #120**). 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) (**Ex. #121**), the government has nevertheless 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).

111. 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.

B. U.S. GOVERNMENT ARGUMENTS CONCERNING THE APPLICABILITY OF THE FOURTH AMENDMENT TO NON-U.S. PERSONS ABROAD

112. 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.”¹⁴⁶ 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) (**Ex. #123**). 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.

¹⁴⁶ Supp. Br. of Plaintiff–Appellee at 12, *United States v. Mohamud*, No. 14-30217 (9th Cir. Oct. 3, 2016), ECF No. 110-1 (**Ex. #122**).

persons seeking to challenge warrantless surveillance programs are not entitled to constitutional protection or redress.

C. OTHER “REDRESS” MECHANISMS HIGHLIGHTED BY THE U.S. GOVERNMENT

1. Freedom of Information Act

113. The Freedom of Information Act (“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.

114. 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) (**Ex. #124**).

2. Privacy Shield Ombudsperson

115. Last 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.¹⁴⁷ 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

¹⁴⁷ *See* E.U.–U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence, <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g> (**Ex. #125**).

to assess whether the procedures themselves are constitutional or to require the executive branch to implement a particular remedy.

116. 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.”¹⁴⁸
117. 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.
118. 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 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.¹⁴⁹ 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 Privacy and Civil Liberties Oversight Board, neither the Inspectors General nor the PCLOB can issue recommendations that are binding on the executive branch.¹⁵⁰ 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

¹⁴⁸ *See id.* § 4(e).

¹⁴⁹ First Annual Review at 35–36.

¹⁵⁰ *Id.*; Adequacy Decision ¶ 120.

the intelligence community, this position is not independent from the intelligence community.¹⁵¹

119. In short, under the existing rules, an individual who complains to the Ombudsperson will never 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. 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.

CONCLUSION

120. 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. Existing oversight mechanisms are inadequate, particularly given the breadth of the U.S. government's surveillance activities. Finally, for the overwhelming 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.

¹⁵¹ 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> (accessed Dec. 19, 2017) (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.") (Ex. #126).