WASHINGTON
LEGISLATIVE OFFICE

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

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 view[1] 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 SIGNT 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 disclosure[32] 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.