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

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

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]

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.519.7804
F/212-549-258O
WWW.ACLU.ORG

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]

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

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]

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

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 ontent 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.

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

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]

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

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/212-549-258O
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.

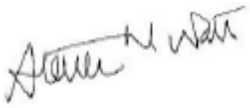
F. Additional Section 702 Reforms

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,



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/212-549-258O
WWW.ACLU.ORG