WASHINGTON
LEGISLATIVE OFFICE

The Honorable Darrell Issa
Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jerrold Nadler
Ranking Member
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

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

KARIN JOHANSON
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

CC: Members of the Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet

RE: House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet hearing, "International Data Flows: Promoting Digital Trade in the 21st Century."

November 2, 2015

Dear Chairman Issa, Ranking Member Nadler, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"[1]), we submit this letter for the record in connection with the House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet hearing, "International Data Flows: Promoting Digital Trade in the 21st Century," to address the E.U.-U.S. 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 free flow of ideas. However, U.S. surveillance practices – which increasingly rely on dragnets that

[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.

collect and review the information of millions of Americans and others around the world – threaten the continued international flow of data.

The impact of U.S. surveillance practices on international data flows was evident in the recent *Schrems* judgment issued by the Grand Chamber of the Court of Justice of the European Union (CJEU)[2]. As part of the decision, the CJEU struck down the legal underpinnings of the E.U.- U.S. Safe Harbor Agreement, which permitted U.S. companies to transfer personal data from the E.U. to the U.S. The judgment was based, in part, on a finding that the legal basis for the arrangement failed to ensure an "adequate level of protection" for E.U. data in the U.S. In its decision, the court referenced the European Commission finding that U.S. authorities were able to access the data of E.U. citizens in the U.S. 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."[3]

Currently, U.S. and E.U. policy makers are reportedly negotiating a new Safe Harbor Agreement.[4] However, the *Schrems* judgment makes clear that U.S. surveillance practices must change to enable transatlantic data flow under the auspices of a new Safe Harbor Agreement. Specifically, we believe that before a new Safe Harbor—that can withstand subsequent judicial challenges—can be negotiated, the U.S. must, at a minimum, reform Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Schrems Judgment and Section 702

Since its inception, the ACLU has opposed Section 702 of the Foreign Intelligence Surveillance Act (FISA) – a surveillance law used by the government to search millions of communications of Americans and others around the world. To satisfy the standards set forth in *Schrems*, Congress must reform Section 702 to provide greater protections for data transferred from the E.U. At a minimum, such reforms must include:

- Eliminating Upstream Surveillance:[5]

As the CJEU made clear, surveillance must be necessary and proportionate to a country's national security needs.[6] Upstream surveillance conducted under Section 702 fails this test. Through upstream surveillance, the government taps directly into the Internet backbone inside the United States, which is made up of the cables and switches that carry the communications of hundreds of millions of Americans and others around the world.[7] The National Security Agency (NSA) seizes and copies all of these

[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.
[3] *Schrems*, ¶ 90.
[4] Mark Scott, *Data Transfer Pact Between U.S. and Europe is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html.
[5] The ACLU is currently engaging in litigation challenging Upstream surveillance as unconstitutional. Wikimedia Found. v. NSA/Central Sec. Serv., 2015 U.S. Dist. LEXIS 144059 (D. Md. Oct. 23, 2015)
[6] While the *Schrems* decision focused on largely on collection under the PRISM program, many of its concerns would similarly apply to the Upstream program. *Schrems*, ¶ 91.
[7] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) https://www.pclob.gov/library/702-Report.pdf.

communications, searching text-based communications for terms related to its "foreign targets" (as explained further below, these targets may not have any nexus to national security).

It is important to note that, as part of Section 702 surveillance, the Foreign Intelligence Surveillance Court (FISC) does not review whether there is sufficient cause to conduct surveillance on specific targets; nor does it approve the terms that the NSA uses to search text-based communications traversing the Internet. Thus, the NSA is permitted to engage in dragnet surveillance with little judicial oversight. Accordingly, current upstream surveillance fails to satisfy the framework put forward in *Schrems* and will need to be discontinued to permit a valid Safe Harbor Agreement.

- Narrowing the Scope of Section 702 Surveillance

Section 702 permits surveillance for purposes that extend far beyond national security needs or counterterrorism. Under Section 702, the government is not required to certify that surveillance targets are agents of a foreign power, 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" is defined to include information about foreign affairs, which could include communications between international organizations and government whistleblowers; diplomats; or even journalists and sources. Such surveillance, due to its very purpose, extends beyond what is necessary and proportionate to protect U.S. interests. As a result, Congress must narrow the purpose of Section 702 surveillance, including the definition of "foreign intelligence," to address the concerns highlighted in *Schrems*.

- Providing Effective Redress

The *Schrems* judgment notes that individuals in the E.U. must have access to judicial remedies in cases where they challenge the treatment of their data – something they lack under the current legal framework in the U.S. 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.[8] Finally, even for citizens of the U.S., 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 meaningfully challenge improper surveillance of individual's data stored in the U.S.

- Placing Limits on the Retention and Use of Section 702 Data

The *Schrems* judgment notes that the U.S. lacks rules to limit the interference with the fundamental rights of people in the E.U. whose data is transferred to the U.S. Under Section 702, the government has broad

---

[8] *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.

authority to retain and use the data of Americans and others around the world. Section 702 permits the retention of any data that constitutes "foreign intelligence," or is encrypted.[9] Even for data that does not fall into either of these categories, the default retention period is five years. 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 will need to place more stringent restrictions on the access and use of Section 702 data.

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 civil liberties of Americans. Specifically, Congress should, at a minimum, require a warrant before acquiring, accessing, or using Americans' communications; close the "backdoor search loophole" permitting warrantless searching of Section 702 data for information about Americans; 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 civil liberties of Americans and others around the world, but also to permit a new Safe Harbor Agreement that will facilitate transatlantic data flows.

If you have any questions, please feel free to contact Legislative Counsel, Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

Sincerely,

Karin Johanson
Director, Washington Legislative Office

Neema Singh Guliani
Legislative Counsel

[9] *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