Statement for the Record of

Nuala O'Connor, President and CEO
Center for Democracy & Technology
and
Gregory T. Nojeim
Director, Freedom, Security & Technology Project
Center for Democracy & Technology

House Judiciary Committee
Subcommittee on Courts, Intellectual Property, and the Internet

Hearing on

International Data Flows: Promoting Digital Trade in the 21st Century
November 3, 2015

(Submitted November 13, 2015)

Chairman Issa, Vice-Chairman Collins, Ranking Member Nadler, and Members of the Subcommittee:

The Center for Democracy & Technology (CDT)[1] submits the following statement for the record summarizing the necessary reforms to U.S. surveillance and privacy laws that must be made in order to ensure the viability of any future Safe Harbor agreement between the U.S. and the E.U. In *Schrems v. Data Protection Commissioner*,[2] the Court of Justice of the European Union (CJEU) not only struck down the Safe Harbor agreement (an agreement vital to transatlantic trade on which over 4,000 U.S. companies had relied for fifteen years); it also found that national Data Protection Commissioners (DPCs) in the E.U. are obligated to investigate complaints that a country that receives E.U. users' data – such as the U.S. – does not provide adequate protection for data privacy rights.

As a result, the *Schrems* decision will have lasting and, without reforms to U.S. law, recurring consequences for international data flows and digital trade. CDT acknowledges the value of approving a short-term "Safe Harbor 2.0" agreement in order to provide temporary relief. In addition, the Judicial Redress Act and Presidential Policy Directive 28 (PPD-28), which provide limited privacy protections for Europeans located abroad,

---

[1] The Center for Democracy & Technology is a nonprofit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom.

[2] Case C-362/14, *Maximillian Schrems v. Data Protection Comm'r* (Oct. 6, 2015), *available at*: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

are small steps in the right direction. However, legislative action that directly addresses the concerns that were at the heart of the CJEU's judgment is required in order to establish a stable, long-term agreement that will not be subject to persistent challenges by European DPCs and courts.

This statement first examines the background of the *Schrems* judgment and the European privacy laws underlying it. The statement then outlines the privacy rights that the Court indicated must be guaranteed with respect to Europeans' data in order for the E.U. to allow companies to transfer such data to the U.S, and provides an overview of some of the reforms that must be made to U.S. law in order to adhere to those privacy rights. We focus on necessary surveillance reforms because concerns about surveillance are at the heart of the *Schrems* judgment, and because they are within the jurisdiction of the Judiciary Committee. We conclude by emphasizing that although the *Schrems* judgment necessitates changes in U.S. law surveillance law, surveillance reforms must ultimately be global in nature in order to provide effective data security and protections for human rights. In addition, the U.S. data protection regime must be strengthened by passage of an effective Consumer Bill of Rights.

I. Overview of the *Schrems* Case

A. Origins

In 1995, before the widespread use of the World Wide Web and email, the European Union had the prescience to create the Data Protection Directive,[3] which mandates that personal data may only be transferred from the E.U. to a non-EU country if the latter "ensures an adequate level of protection" of privacy and other individual rights. In 2000, the European Commission, the E.U.'s executive body, decided that the U.S. offered an "adequate level of protection" and that it was therefore lawful for companies to transfer data from the E.U. to the U.S.[4] This decision was the legal basis for the Safe Harbor arrangement. Under that arrangement, U.S. companies self-certify that they will take certain steps to protect personal information, but such steps are subsidiary to company obligations to disclose personal information governmental entities for law enforcement or national security reasons.

Following the Snowden revelations that began in June 2013, Facebook user Maximillian Schrems filed a complaint with the national Data Protection Commissioner (DPC) in Ireland, alleging that the U.S. did not provide an adequate level of privacy protections, and asked the Commissioner to investigate whether Facebook should be allowed to transfer E.U. users' data to the U.S. The High Court of Ireland decided to refer to the CJEU the question of whether national DPCs in the E.U. had the authority to carry out

[3] Directive 95/46/EC of the European Parliament of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[4] Decision 2000/520/EC (July 26, 2000), *available at*: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520.

such an investigation, since the European Commission had already found in its 2000 decision that U.S. data protections were "adequate."[5]

B. The CJEU's Judgment

The CJEU concluded that not only are national DPCs able to investigate complaints that a non-E.U. country's protection of Europeans' data privacy is inadequate, but that the DPCs are, in fact, obligated to conduct such investigations upon receiving a complaint.[6] The Court also went a step further and examined the issue of whether the European Commission's 2000 decision underlying the Safe Harbor agreement was valid, and concluded that it was not.[7]

The Court recalled that in order for such an agreement to be valid, the non-E.U. country – in this case, the United States – must ensure "an adequate level" of data protection in line with E.U. fundamental rights laws. The Court then indicated that in order to be "adequate," protections in the U.S. (or any other non-E.U. country) must be "essentially equivalent"[8] to those guaranteed in the E.U. under the Data Protection Directive and the Charter of Fundamental Rights of the European Union[9] (effectively, the E.U.'s "Bill of Rights," which contains explicit rights to privacy and the protection of personal data). Critically, the Court went on to elaborate on the specific types of privacy rights countries such as the U.S. must guarantee in order to receive data from the E.U. These privacy rights point directly to reforms of Section 702 of the Foreign Intelligence Surveillance Act of 2008 (FISA) as well as the establishment of baseline consumer privacy protections.

II. Recommendations

A. Reforms to Section 702 of FISA

The data protection requirements described in the CJEU's decision are standards that U.S. law does not currently meet, thanks in large part to Section 702 of FISA. Although Section 702 is not scheduled to sunset until 2017, achieving an adequate level of reform will take time, and a failure to begin addressing the CJEU's concerns as soon as possible will result in any new Safe Harbor agreement being subject to constant scrutiny and instability. CDT has determined that the *Schrems* decision necessitates the following reforms to Section 702. These are reforms that the Committee should embrace not just because they would facilitate commercial trade, but because they would advance the constitutional rights of Americans in the U.S., the human rights of people on a global basis, and at the same time, begin to strengthen the tenuous constitutional foundation on which this surveillance now rests:

---

[5] Schrems v. Data Protection Comm'r, [2014] I.E.H.C. 310 (H. Ct.) (Ir.), *available at*: http://www.bailii.org/ie/cases/IEHC/2014/H310.html.
[6] Case C-362/14 at ¶ 63.
[7] *Id.* at ¶ 67.
[8] *Id.* at ¶ 73.
[9] Charter of Fundamental Rights of the European Union art. 7-8, 2000/C 364/01, *available at*: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

- **The prohibition of "upstream" surveillance**: The CJEU found that laws allowing government authorities to "have access on a generalised basis to the content of electronic communications" violate "the essence of the fundamental right to respect for private life."[10] When the U.S. government engages in "upstream" surveillance based on section 702, it temporarily seizes virtually all Internet-based communications flowing into or out of the United States.[11] Officials then search those communications for all those that are "to," "from," or "about" a given selector (such as an email address), gather that data, and store it for later searching (via queries) by the NSA, CIA, and FBI.[12] *Because "upstream" surveillance involves seizing and searching communications content so comprehensively and on such a large scale, without strong legal restrictions designed to ensure that both the seizure and searching are strictly necessary and proportionate, the Court is unlikely to uphold any future E.U.-U.S. data transfer arrangement unless section 702 is amended to prohibit this type of activity*.

- **A strict limitation on the purposes for which the U.S. may conduct surveillance under section 702**: The CJEU indicated that E.U.-U.S. data transfers should not take place unless the U.S. government can only gain access to (and use) the data "for purposes which are specific, strictly restricted and capable of justifying" the privacy intrusion involved.[13] The current wording of section 702 broadly authorizes the collection of telephone calls, emails, instant messages, social network content, and other communications content of non-U.S. persons reasonably believed to be located abroad so long as a "significant purpose" of that collection is to acquire "foreign intelligence information."[14] Therefore, so long as acquiring foreign intelligence information is a "significant" purpose, the U.S. government can intercept such communications for a plethora of other reasons. *The broad, opaque language of the current section 702 should be revised to prevent the executive branch from conducting surveillance under the program unless it is seeking to investigate or prevent a limited set of specific dangers, such as terrorism. Moreover, the bodies that have the power to search or otherwise gain access to the data that has been collected, as well as the circumstances under which they may do so and their transparency obligations, should be clearly set out in law.*

- **Stronger, more transparent authorization and oversight processes**: The *Schrems* Court stated that limitations to E.U. citizens' privacy rights must be

[10] Case C-362/14 at ¶ 95.
[11] Charlie Savage, *N.S.A. Said to Search Content of Messages to and from the U.S.*, N.Y. TIMES (Aug. 8, 2013), *available at*: http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0.
[12] *See* Privacy and Civil Liberties Oversight Board (PCLOB), "Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 7 (July 2, 2014) [hereinafter "PCLOB Report"].
[13] Case C-362/14 at ¶ 93.
[14] 50 U.S.C. § 1881a(g)(2)(A)(v).

"strictly necessary,"[15] and emphasized the need for strong safeguards against abuse.[16] Under current law, the FISA Court (FISC) does not approve any particular acquisition or target.[17] It does not even authorize the terms and phrases that will be used when querying the collected information. Instead, it approves proposed guidelines for targeting that are meant to ensure that the surveillance is focused on non-U.S. persons reasonably believed to be located outside the United States.[18] The FISC also approves proposed minimization procedures meant to limit the acquisition, retention, use, and dissemination of non-public information about U.S. persons acquired through Section 702.[19] *Congress should strengthen the authorization and oversight process for Section 702 surveillance by requiring FISC or other independent approval of the specific terms the intelligence agencies may use to search captured data. In addition, reforms should be adopted to make Section 702 authorization and oversight processes more individualized and capable of imposing firm, clear, and consistent restraints.*

- **A genuine ability for individuals whose communications might be subject to secret surveillance to obtain redress for any abuses**: In addition to highlighting the need to provide "minimum safeguards" that effectively protect data subjects from risks of abuse, the Court also emphasized the need for individuals to have some type of access to judicial review of decisions pertaining to their personal data.[20] The Judicial Redress Act was a limited first step[21] to affording non-U.S. persons a small degree of judicial review under the Privacy Act, but the Privacy Act provides no meaningful redress for targets of intelligence agency surveillance under Section 702 because the agencies can exempt themselves from the Act's requirements on grounds of national security (and have indeed done so).[22] *Congress should provide an effective judicial redress mechanism for individuals whose communications might be subject to Section 702 surveillance. This can be achieved by providing a right to standing for people who can produce evidence that they may have been unlawfully monitored.*

B. Reforming the U.S. Data Protection Regime

In addition to U.S. surveillance practices under Section 702, the CJEU's concerns in the *Schrems* judgment appear to have stemmed from an overall lack of confidence in the level of protection and respect given to consumer data in the U.S. The United States is one of only two developed nations without privacy protections for all personal data

---

[15] Case C-362/14 at ¶ 92.
[16] *Id.* at ¶ 91.
[17] *See* PCLOB Report, *supra* n. 12, at 27.
[18] *Id.*
[19] *Id.*
[20] Case C-362/14 at ¶ 95.
[21] For CDT's analysis of the Judicial Redress Act, see https://cdt.org/blog/the-eu-us-umbrella-agreement-and-the-judicial-redress-act-small-steps-forward-for-eu-citizens-privacy-rights/; 32 CFR § 322.7(a).
[22] 5 U.S.C. § 552a(k).

(Turkey is the other).[23] Instead, only a handful of sector-specific laws apply to narrow categories of information, coupled with the Federal Trade Commission's (FTC) power to combat some privacy violations as "unfair and deceptive practices" under section 5 of the FTC Act.

U.S. law must be updated to conform to the needs of the digital age. With the advent of increasingly sophisticated technologies that collect detailed personal information, there is a pervasive sense that consumers have lost control of their data. Worse, this exponential increase in personal data that is collected, shared, and stored for indeterminate periods of time is coupled with a rise in the frequency and scope of data breaches.[24] *The U.S. data protection regime should be brought up to date by passing a strengthened Consumer Privacy Bill of Rights*[25] *with substantive protections that track the Fair Information Practice Principles (FIPPs)-transparency, individual control, respect for context, focused collection and responsible use, security, access and accuracy, and accountability. Such protections should be predicated on individual rights and not conditioned on an assessment of privacy risk. In addition, they must be protected by robust enforcement mechanisms.*

III. Conclusion

We appreciate the opportunity to present our views to the Subcommittee about the need for reforming U.S. privacy and surveillance practices in order to enable the long-term free flow of international data. Although this statement for the record focused on reforms to U.S. law, CDT acknowledges that a truly effective solution to the problem of protecting personal information will have to be global in nature. Some who have examined the CJEU's decision in *Schrems* have rightly pointed out that many European countries' surveillance programs would not live up to the privacy standards mandated by the CJEU, and that they of late are moving backward, not forward, in terms of the protections they afford. [26] These troubling laws do not change the United States' need to reform its surveillance practices in order to facilitate the free flow of information for commercial reasons in light of the CJEU's *Schrems* decision, or its obligation to change Section 702 to protect human rights and civil liberties.

We look forward to collaborating with you on these important issues. For more information, please contact CDT's Greg Nojeim, Director, Protect on Freedom, Security & Technology, gnojeim@cdt.org; (202) 407-8815.

---

[23] *See* NYMITY, Inc., "Sectoral and Omnibus Privacy and Data Protection Laws" (2015), *available at*: https://www.nymity.com/~/media/Nymity/Files/Privacy%20Maps/NYMITY_World_Map.ashx.
[24] *See* Verizon 2015 Data Breach Investigations Report (April 13, 2015), *available at*: http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/.
[25] For CDT's analysis of the Obama Administration's draft Consumer Privacy Bill of Rights Act, see https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/.
[26] Press Release, Center for Democracy & Technology, Draft UK Surveillance Bill Would Do More Harm than Good to Privacy (Nov. 4, 2015), *available at*: https://cdt.org/press/draft-uk-surveillance-bill-would-do-more-to-harm-than-good-to-privacy/.