July 21, 2020

U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Department of Commerce:

On behalf of the American Civil Liberties Union (ACLU),[1] we write to address the reforms that must be made to U.S. surveillance law and practices to permit the free flow of data between the United States (U.S.) and the European Union (E.U.), in light of the *Schrems II* decision issued by the Grand Chamber of the Court of Justice of the European Union (CJEU) last week. Such changes are critical to ensure that small and large businesses alike do not continue to suffer financial consequences through no fault of their own.

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political
Advocacy Department
915 15th St. NW, 6th FL
Washington, D.C. 20005
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political Director

On July 16, the CJEU struck down the E.U.–U.S. Privacy Shield, utilized by over 5,300 companies,[2] for failing to provide a sufficient level of protection for E.U. data. Specifically, the court found that U.S. surveillance authorities, including Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12333, permit large-scale surveillance that is not strictly necessary to the needs of the state. The court also found that the Privacy Shield failed to create adequate redress mechanisms for Europeans whose data is transferred to the U.S.—namely, the ability to be heard by an independent and impartial court.

In addition to invalidating Privacy Shield, the CJEU's ruling indicated serious problems with companies' reliance on a separate mechanism, Standard Contractual Clauses, for data transfers from the E.U. to the U.S., given the scope of U.S. surveillance and obstacles to redress. Some European Data Protection Authorities are now advising companies to stop large-scale data transfers to the U.S. altogether.[3]

This poses significant problems for U.S. companies in places as diverse as Boca Raton, Florida, San Francisco, California, and Cleveland, Ohio, who rely on these transatlantic data transfer agreements to lawfully transfer data from the E.U. for processing and storage in the U.S. In many cases, companies rely on these agreements to perform critical functions, such as providing services to customers overseas or human resources to a global workforce.

The Department of Commerce has stated that it is still examining the CJEU's decision. However, it is anticipated that the U.S. government and European Commission will engage in negotiations on a successor agreement to the Privacy Shield.

The *Schrems II* decision makes clear that the U.S. must reform its surveillance laws for any successor agreement to the Privacy Shield to withstand judicial scrutiny, and for companies to reasonably rely on Standard Contractual Clauses to transfer data to the U.S. Specifically, the U.S. must pass reform legislation that at a minimum:

(1) Narrows collection under Section 702 and EO 12333;

(2) Enhances the role of the FISA court in approving surveillance under Section 702 and EO 12333;

(3) Ensures that individuals are notified and able to challenge improper surveillance under Section 702 and EO 12333; and

(4) Limits retention and use of information under Section 702 and EO 12333.

Until Congress passes legislation making these reforms, the Executive Branch should implement these changes as a matter of policy and as an explicit condition of any successor agreement to the Privacy Shield.

Background

Pursuant to a 1995 European Parliament directive ("1995 Directive"), when data is transferred from an E.U. member state to a country outside of the European Union, the receiving country must "ensure[] an adequate level of protection" for that data, judged in light of "all the circumstances surrounding [the] data transfer."[4] 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.[5] Courts have interpreted this to require that the agreement provides a level of protection of fundamental rights and

[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] Dep't of Commerce, *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows* (July 16, 2020), *available at* https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

[3] *Berlin: Berlin Commissioner Issues Statement on Schrems II Case, Asks Controllers to Stop Data Transfers to the US*, Data Guidance, July 17, 2020, *available at* https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data.

[4] European Parliament and Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31–50; *see id.* at art. 26 (outlining certain narrow exceptions to this principle for transfers that are neither repeated nor systematic, *e.g.*, where the data subject has given his consent unambiguously to the proposed transfer).

[5] *Id.* at art. 25.

freedoms that is "essentially equivalent" to those provided within the E.U.[6] Although the 1995 Directive has since been replaced by the 2016 General Data Protection Regulation,[7] the legal framework described here remains in place.

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 without running afoul of E.U. privacy laws. The European Commission ratified the Safe Harbor framework in 2000 by finding that it provided an adequate level of protection for personal data. However, in 2015, the CJEU struck down the Safe Harbor agreement, based largely on concerns about the scope of U.S. government surveillance.[8]

Just a few months later, the U.S. and E.U. finalized negotiations on the Privacy Shield, the successor agreement to Safe Harbor. Prior to the new agreement, the U.S. did not undertake significant reforms to the scope of its surveillance practices, nor did it provide U.S. persons or non-U.S. persons meaningful avenues to challenge unlawful surveillance practices.

The *Schrems II* Decision

Almost immediately after the ink dried on Privacy Shield, the legal underpinnings of the agreement were once again the subject of an E.U. suit. In response to a complaint by Austrian privacy advocate Max Schrems, the Irish Data Protection Commissioner brought a case challenging the lawfulness of E.U.–U.S. data transfers. On July 16, 2020, the CJEU struck down the Privacy Shield, finding that the U.S. failed to provide an adequate level of protection for E.U. data, given the scope of U.S. surveillance and lack of meaningful remedies for unlawful surveillance. In addition, it directed Data Protection Authorities to prohibit the use of Standard Contractual Clauses, an alternative mechanism permitting transatlantic data transfers, if the clauses similarly failed to protect individual rights.

In its opinion, the court specifically held that Section 702 of FISA and EO 12333 electronic surveillance violate fundamental rights under E.U. law.

First, the court held that U.S. surveillance law did not meet the E.U. standards requiring that any interference with fundamental rights be strictly necessary and proportionate to the state's interest. In particular, the court observed that, under Section 702, the Foreign Intelligence Surveillance Court (FISC) does not approve the surveillance of particular targets; instead, it reviews broad surveillance programs on an annual basis, and confirms

---

[6] *See* C-311/18, *Schrems II v Data Protection Comm'r* ¶¶ 201, 203 (Dec. 19, 2019), *available at* http://curia.europa.eu/juris/document/document.jsf;jsessionid=EA6D17501EEC901F8137BC9AA3C03303?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=10396887.

[7] Regulation EU 2016/679, Gen. Data Prot. Regulation (Apr. 27, 2016), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=DE.

[8] *See* C-362/14, *Schrems v. Data Prot. Comm'r*, 2000 EUR-Lex 520 (Sept. 23, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10588011.

that a significant purpose of the surveillance is "foreign intelligence."[9] The court also observed that, under EO 12333, the U.S. government can access and collect personal data in bulk, without any judicial review whatsoever.[10] The court further explained that Presidential Policy Directive-28 (PPD-28) specifically allows the mass access to and collection of information without use of identifiers associated with specific targets, failing to "delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data."[11]

Second, the court found that U.S. law does not provide sufficient redress for surveillance abuses. Specifically, it pointed to paragraph 115 of the European Commission's Privacy Shield adequacy decision, which found that the "standing" doctrine is an obstacle to redress in U.S. courts.[12] Standing is an obstacle, in part, because the U.S government virtually never notifies individuals subject to foreign intelligence surveillance—not even after an investigation has concluded. Separately, the court also highlighted that neither PPD-28 nor EO 12333 confers "rights which are enforceable against the US authorities in the courts."[13] Finally, the court explained that the Ombudsperson created under the Privacy Shield could not ensure appropriate redress because there was no indication that the Ombudsperson "ha[d] the power to adopt decisions that are binding on those intelligence services"; the Ombudsperson was not sufficiently independent from the intelligence community; and there was no evidence of legal safeguards that would "accompany that political commitment on which data subjects could rely."[14]

As a result of the decision, the Privacy Shield may no longer be relied on as the legal basis to transfer data between the U.S. and the E.U. The decision has also undermined the legal basis for the use of Standard Contractual Clauses for data transfers to the U.S. Unlike the prior invalidation of the Safe Harbor agreement, no grace period for companies has been specified. It is expected that the U.S. and E.U. will promptly begin negotiations on a replacement to the Privacy Shield.

Reforms Needed

The ACLU has long raised concerns about surveillance conducted under Section 702 and EO 12333. Over the last several years, the defects in these surveillance regimes—mass collection, 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 II*, Congress must pass legislation or the President must issue a binding Executive Order that includes the following reforms:[15]

---

[9] *Schrems II* ¶¶ 179–80.

[10] *Schrems II* ¶ 183.

[11] *Id.*

[12] *Schrems II* ¶ 191.

[13] *Schrems II* ¶¶ 182–83.

[14] *Schrems II* ¶¶ 195–96.

[15] These reforms would not necessarily be sufficient to satisfy U.S. constitutional requirements.

A. Narrowing the Scope of EO 12333 and Section 702 Surveillance

Section 702 and EO 12333 authorize warrantless surveillance inside the U.S. for purposes that extend far beyond national security needs or counterterrorism. For example, 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" is defined to include information about foreign affairs, which could encompass communications between international organizations and government whistleblowers, or between journalists and sources.[16] EO 12333 is even broader in scope, similarly permitting targeting of individuals overseas for foreign intelligence purposes, broadly defined to include "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, [or] foreign persons."[17] The U.S. government relies on EO 12333 for the mass collection of personal data, including reportedly tapping of undersea cables and collection of all communications from certain countries.[18]

This surveillance scheme plainly contravenes the standards set forth by the CJEU. Broad authorizations to obtain "foreign intelligence information" from any foreigner do not satisfy the 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 authorizations infringe Europeans' rights beyond what is "strictly necessary."[19] To remedy these deficiencies, the scope of Section 702 and EO 12333 surveillance must be narrowed. Historically, the U.S. government has utilized the objective criterion of whether a target is a "foreign power" or an "agent of a foreign power" as a basis for FISA surveillance. Narrowing the definition of "foreign intelligence" to require that a target be a foreign power or agent of a foreign power would likely meet the standards set forth by the CJEU.

In addition to this reform, the U.S. must curtail large-scale collection under EO 12333 by requiring the use of selectors associated with a specific target. If Congress and the Executive Branch fail to end large-scale collection under EO 12333, they must—at a minimum—require a showing that the government has exhausted less intrusive means of surveillance, and implement more stringent minimization requirements.

---

[16] *See* 50 U.S.C. §§ 1881a(a), 1801(e).

[17] Exec. Order No. 12333, as amended, *available at* https://www.intelligence.senate.gov/laws/executive-order-12333-1981-amended-executive-orders-13284-2003-13355-2004-and-13470-2008 (EO 12333).

[18] *See* 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; *see also* Ryan Devereaux, Glenn Greenwald & Laura Poitras, *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.

[19] *Schrems I* ¶ 93.

B. Enhancing the Role of the FISC or Other Independent Entity

A central focus of the *Schrems II* opinion was the lack of independent approval of surveillance targets under Section 702 and EO 12333. Under Section 702, the role of the FISC 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. Under EO 12333, the FISC has no role at all. EO 12333 programs, procedures, and targets are determined solely by the Executive Branch; protections of non-US persons are governed by a presidential directive, not binding law; and changes to any existing procedures can be made without notice at the whim of any President.

In order to meet the standards set forth in *Schrems II*, Section 702 and EO 12333 should be modified to require the FISC or other independent authority to approve, or at a minimum, review, individual targeting decisions. In addition, the FISC should be required to annually review EO 12333 procedures to ensure that they comply with the limits of the Executive Order, PPD-28, and any other limits set forth in a successor agreement to the Privacy Shield.

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

The *Schrems II* judgment found that U.S. surveillance law lacked sufficient safeguards, including with regards to the access and use of information.[20] Under Section 702, the government has broad authority to retain and use the data it has collected. It can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information.[21] Even for data that does not fall into either of these categories, the default retention period is two years for Upstream and five years for information collected with the assistance of service providers. In addition, data can be disseminated to other countries, and used for a wide variety of purposes, including criminal prosecution. Under EO 12333 procedures, data can similarly be retained for five years or longer in certain circumstances, and used and disseminated for a wide array of purposes. The EO 12333 procedures are not legally binding, and do not explicitly grant individuals the rights to redress in cases where there is violation.

To address the concerns in *Schrems*, Congress must put in place additional legally enforceable restrictions on the access and use of data collected under Section 702 and EO 12333. EO 12333 restrictions involving the retention and use of information should be codified in law or other legally enforceable mechanism, just as limits on the retention of U.S. person information under EO 12333 were codified in the Intelligence Authorization Act for Fiscal Year 2015.[22] In addition, retention of information under EO 12333 and

[20] *Schrems II* ¶ 180.

[21] *See* Off. of the Dir. of Nat'l Intelligence, *Minimization Procedures Used By the NSA In Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* at Section 6 (accessed Nov. 2, 2015), *available at*, http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[22] H.R. 4681, Intelligence Authorization Act for FY 2015, 113th Cong., at Section 309 (2014).

Section 702 should be limited to three years, and access and use of such information should be narrowed to a subset of "foreign intelligence" purposes.

D. Providing Effective Redress

The *Schrems II* judgment affirms that individuals whose personal data is transferred from the E.U. must have access to judicial remedies to challenge the treatment of their data—remedies they lack under the current legal framework in the U.S. As the ACLU has explained,[23] one of the primary barriers to effective redress in U.S. courts is lack of notice. As a general matter, individuals do not receive notice that their information has been collected under Section 702 or EO 12333, even in cases where such notice would not jeopardize active investigations. The text of FISA only requires notification in cases where the government seeks to use information "obtained or derived" from Section 702 in civil, administrative, or criminal proceedings against an individual. However, the government has a history of failing to comply with Section 702's notice provision, and there are serious concerns it continues to define "derived" narrowly to skirt its obligation.[24] Under EO 12333, the government denies it has any obligation to provide notice at all, including in civil, criminal, or administrative proceedings. As a practical matter, the lack of notice makes it difficult—if not impossible—for litigants to establish standing to challenge unlawful surveillance in U.S. courts.

To address these deficiencies, there are several changes that must be made to Section 702 and EO 12333. One, the government should adopt a broader policy of requiring notice to individuals in cases where it would not result in an imminent threat to safety or jeopardize an active investigation. Two, FISA should be modified to define "derived," to ensure that the government fully complies with its statutory notice obligations. Three, EO 12333 should be modified to require notification to individuals in cases where information obtained or derived from electronic surveillance is used against an individual. Four, the authority of the existing Ombudsperson should be enhanced to make it entirely independent; permit the Ombudsperson to authorize specific notice and redress in cases where individuals bring claims regarding improper surveillance; and allow it to declassify information so that it can fully respond to complaints.

Conclusion

In addition to the reforms noted above, the *Schrems II* judgment offers the opportunity to examine other facets of Section 702 and EO 12333 surveillance that violate the privacy and civil liberties of Americans. Specifically, the government should, at a minimum, require a warrant before acquiring, accessing, or using Americans' communications; provide greater transparency and oversight; and reform the state secrets privilege, which acts as a barrier

[23] Ashley Gorski, *Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies, & Oversight*, ACLU (Aug. 30, 2018), *available at* https://www.aclu.org/sites/default/files/field_document/cjeu_schrems_report_final_august_30_2018.pdf.

[24] *See* Charlie Savage, *Warrantless Surveillance in Terror Cases Raises Constitutional Challenge*, N.Y. Times, Apr. 26, 2016, https://www.nytimes.com/2016/04/27/us/warrantless-surveillance-in-terror-case-raises-constitutional-challenge.html.

to judicial review of surveillance programs. 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 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,

Ronald Newman
National Political Director

Neema Singh Guliani
Senior Legislative Counsel

Ashley Gorski
Senior Staff Attorney, National Security Project