December 9, 2020

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science, and Transportation
U.S. Senate
Washington, D.C. 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
U.S. Senate
Washington, D.C. 20510

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

RE: The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows

Dear Chairman Wicker, Ranking Member Cantwell, 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 Senate Commerce Committee's hearing, "The Invalidation of the E.U.–U.S. Privacy Shield and the Future of Transatlantic Data Flows." We write to address the legal reforms that must be made to permit the free flow of data from the E.U. to the U.S., in the wake of the *Schrems II* decision by the Court of Justice of the European Union ("CJEU"), and subsequent guidance by the European Data Protection Board. These changes are essential to ensure that small and large businesses alike will not continue to suffer financial consequences through no fault of their own.

The reforms discussed below would also provide essential privacy protections for Americans, whose communications and data are swept up by the U.S. government's foreign intelligence surveillance in

[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 approximately two 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.

enormous quantities.[2] As technological advances permit ever-broader forms of surveillance—including bulk collection—there is an urgent need for stronger legal safeguards.

On July 16, the CJEU struck down the E.U.–U.S. Privacy Shield, used by over 5,300 companies, for failing to provide a sufficient level of protection for E.U. data.[3] 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 (SCCs), for data transfers from the E.U. to the U.S., given the scope of U.S. surveillance and obstacles to redress. Based on the CJEU's ruling, the European Data Protection Board recently issued draft guidance concerning SCCs that would make it virtually impossible to transfer personal data to "electronic communication service providers," 50 U.S.C. § 1881(b)(4), inside the U.S. for processing.[4] Indeed, the Irish Data Protection Commissioner has already issued a preliminary order to Facebook to halt its transfers to the U.S. about its E.U. users.[5]

The CJEU's ruling and the European Data Protection Board's guidance pose significant problems for U.S. companies in places as diverse as Boca Raton, Florida, San Francisco, California, and Cleveland, Ohio, who relied on Privacy Shield and currently rely on SCCs to

---

[2] *See, e.g.*, Barton Gellman *et al.*, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule that lets the NSA spy on Americans*, Wash. Post (July 18, 2014), https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

[3] C-311/18, *Data Protection Comm'r v. Facebook Ireland Ltd. & Maximilian Schrems* ("*Schrems II*") (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=15476758.

[4] *See* European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf; *see also, e.g.*, Omer Tene, Vice President at the International Association of Privacy Professionals, *Quick Reaction to EDPB Schrems II Guidance*, https://www.linkedin.com/pulse/quick-reaction-edpb-schrems-ii-guidance-omer-tene ("it's hard to see a clear path for data transfers to the US").

[5] Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, Wall St. J. (Sept. 9, 2020), https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980.

transfer data from the E.U. for processing and storage in the U.S. In many cases, companies rely on these data-transfer mechanisms for critical functions, such as providing services to customers overseas or human resources to a global workforce.

Below, we describe several reforms critical to ensuring future transatlantic data flows. Although we propose reforms to both Section 702 and EO 12333 surveillance, the Section 702 reforms are especially urgent. That is because the Section 702 collection of data "at rest" inside the United States is an insurmountable obstacle to the functioning of SCCs.

In particular, to address the CJEU's ruling, Congress must:

- Narrow the scope of Section 702 and EO 12333 surveillance;
- Expand the role of the Foreign Intelligence Surveillance Court in Supervising Section 702 and EO 12333 surveillance;
- Ensure that individuals affected by U.S. surveillance can challenge improper surveillance in court; and
- Limit retention and use of information under Section 702 and EO 12333.[6]

Separately, Congress must also work to pass comprehensive consumer privacy protections. That legislation must provide clear and strong data-usage rules and ensure that discrimination cannot take on new life in the 21st century. It must also allow states to enact stronger protections and provide people the opportunity to sue companies that violate their privacy. However, we note that these privacy protections, while essential, will not address the concerns of the CJEU, which focused on the U.S. government's overbroad surveillance authorities and obstacles to redress for government surveillance. To address the ruling in *Schrems II*, the path forward requires reforms to Section 702 and EO 12333.

Background

Under E.U. law, companies are generally forbidden from transferring personal data to non-E.U. countries on a repeated or systematic basis, unless the transfer is conducted pursuant to one of the following:

1. Special Transfer Mechanisms. Companies may, through contracts such as SCCs or similar mechanisms, establish certain rules for data transfers to safeguard privacy rights. In some contexts, these safeguards can compensate for deficiencies in a non-E.U. country's law—*e.g.*, if the non-E.U. country lacks protections for consumer privacy, companies may use an SCC to commit to extend basic rights to consumers vis-à-vis the companies.

In the U.S., however, no contract is capable of overcoming the fundamental problems with U.S. law identified by the CJEU: namely, the scope of U.S. foreign intelligence surveillance and obstacles to redress. No contract between two companies can narrow the sweep of government surveillance or ensure that targeted customers receive notice of classified surveillance.

2. Adequacy Decision. The European Commission may conclude, as a categorical matter, that a non-E.U. country provides an "adequate" level of protection through its domestic law

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

and international commitments—as it did through Safe Harbor and then Privacy Shield—but the Commission's adequacy decisions are subject to review by the CJEU. The CJEU has interpreted the "adequacy" standard to require that the non-E.U. country provide a level of protection of fundamental rights and freedoms that is "essentially equivalent" to those provided under E.U. law.[7]

Because the CJEU has identified fundamental defects in U.S. law, discussed in greater detail below, U.S. reforms should be a prerequisite to the negotiation of a new E.U.–U.S. data-transfer agreement. Indeed, European Commissioner Didier Reynders has stated publicly that "no quick fix" will adequately address the requirements of E.U. law.

But even if the European Commission were to agree to a quick fix, U.S. companies would still face substantial economic risks—including the risk that individual member-state Data Protection Authorities ("DPAs") would halt data flows. In analyzing transfers conducted pursuant to SCCs and similar mechanisms, DPAs are not bound by the European Commission's conclusions about whether a non-E.U. country's laws are adequate. Indeed, prior Commission adequacy decisions have acknowledged DPAs' authority to arrive at their own independent conclusions about whether to halt data transfers. And notably, in *Schrems II*, the CJEU held that DPAs are *required* to suspend data transfers if they conclude that such transfers are unlawful.

To ensure that any new E.U.–U.S. data-transfer agreement withstands CJEU scrutiny, and to ensure that U.S. companies do not pay the price for a failed "quick fix," Congress must enact the reforms below.

Reforms to U.S. Law

1. Narrow the Scope of Section 702 and EO 12333 Surveillance

For an adequacy decision to survive CJEU scrutiny, the non-E.U. country's laws may interfere with the protection of personal data "only in so far as is strictly necessary."[8] In *Schrems I*, the CJEU explained that, in conducting surveillance, the third country must employ an "objective criterion" limiting surveillance to purposes that are "specific, strictly restricted and capable of justifying the interference."[9] It also held that government access "on a generalised basis to the content of electronic communications" violates the "essence" of the right to private life.[10] In *Schrems II*, the CJEU elaborated on these concerns with respect to Section 702 and EO 12333 surveillance. It explained that Section 702 "does not indicate any limitations on the power it confers to implement surveillance programs," and it

---

[7] *Schrems II* ¶¶ 201, 203.

[8] C-362-14, *Schrems v. Data Protection Comm'r* ("*Schrems I*") ¶ 92 (Sept. 23, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10588011.

[9] *Schrems I* ¶ 93.

[10] *Schrems I* ¶ 94.

observed that the U.S. government collects communications in "bulk" under EO 12333[11]—*i.e.*, it accesses communications on a "generalised basis."

Congress should act immediately to narrow the scope of both Section 702 and EO 12333.

With respect to Section 702, Congress can begin to address this issue by requiring an executive branch finding of reasonable suspicion that surveillance targets are "foreign powers" or "agents of a foreign power" outside of the United States—a clear "objective criterion" to justify the interference with private communications.[12] In the alternative, Congress could narrow the definition of "foreign intelligence information" under 50 U.S.C. § 1801(e), though this reform may not be sufficient to address the CJEU's concerns about the breadth of Section 702 surveillance.

With respect to EO 12333, Congress should prohibit bulk collection and require that surveillance be directed at specified targets. Separately, Congress should narrow EO 12333's definition of "foreign intelligence," which currently allows the government to conduct surveillance to obtain any "information relating to the capabilities, intentions, or activities of . . . foreign persons."

2. Expand the Role of the Foreign Intelligence Surveillance Court in Supervising Section 702 and EO 12333 Surveillance

In invalidating Privacy Shield, the CJEU focused largely on 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 an annual review of general targeting and minimization procedures; the FISC does not evaluate whether there is sufficient justification to conduct surveillance on specific targets. Under EO 12333, the FISC has no role at all.

To address these concerns, and to ensure greater protection for Americans whose communications and data are swept up in this surveillance, Congress must enact significant changes to the FISC's role in supervising Section 702 and EO 12333 surveillance. At a minimum, the FISC or other independent entity should review targeting decisions on an individual ex post basis. Although this reform would likely require Congress to expand the number of FISC judges, it would enhance privacy protections for Americans swept up in this surveillance and, given the concerns of the CJEU, it is essential to ensuring the free flow of data between the E.U. and the U.S.

3. Ensure that Individuals Affected by U.S. Surveillance Can Challenge Improper Surveillance in Court

In *Schrems II*, the CJEU affirmed 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 a general matter,

---

[11] *Schrems II* ¶ 183.

[12] Notably, "foreign power" and "agent of a foreign power" are defined rather broadly under FISA to include international terrorists, political factions, and entities acting under a foreign government's effective control. *See* 50 U.S.C. § 1801(a)-(b).

individuals do not receive notice that their information has been collected for foreign intelligence purposes, even in cases where notice would not jeopardize an active investigation. The lack of notice makes it difficult—if not impossible—for people subjected to illegal surveillance to establish standing to challenge that surveillance in U.S. courts.

Congress should enact two key reforms to expand access to meaningful remedies.

First, a "standing fix": Congress can and should pass legislation to more clearly define what constitutes an "injury" in cases challenging government surveillance, as Senator Wyden and others proposed in a 2017 reform bill. While standing is a constitutional requirement, the Supreme Court has been clear that Congress has a role to play in defining what qualifies as an "injury" for the purposes of standing. Congress could, for example, explain that where a person takes objectively reasonable protective measures in response to a good-faith belief that she is subject to surveillance, those protective measures constitute an injury-in-fact. This reform would allow more individuals to begin to litigate claims of unlawful surveillance in the public courts.

Second, Congress should require the executive branch to provide delayed notice of foreign intelligence surveillance to targets of that surveillance, where such notice would not result in an imminent threat to safety or jeopardize an active investigation. In addition, FISA should be modified to define "derived," to ensure that the government fully complies with its existing statutory notice obligations.

4. Limit Retention and Use of Information Under Section 702 and EO 12333

In *Schrems II*, the CJEU found that U.S. surveillance law lacked sufficient safeguards, including with regard to the access and use of information.[13] 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. Even for data that does not fall into either of these categories, the default retention period is as long as five years. The retention limitations for communications and data collected under EO 12333 are similar.

Congress should enact additional restrictions on the use and retention of data collected under Section 702 and EO 12333. In particular, Congress should require that where an agency seeks to retain data beyond the default retention period, the agency must establish that the data falls within a narrow subset of critical "foreign intelligence." Congress should also limit the Section 702 and EO 12333 default retention period to three years.

[13] *Schrems II* ¶ 180.

Conclusion

For more information, please contact Senior Legislative Counsel Kate Ruane at kruane@aclu.org or (202) 675-2336, or Senior Staff Attorney Ashley Gorski at agorski@aclu.org or (212) 284-7305.

Sincerely,

Ronald Newman
National Political Director
National Political Advocacy Department

Kathleen Ruane
Senior Legislative Counsel
National Political Advocacy Department

Ashley Gorski
Senior Staff Attorney
National Security Project

cc: Members of the Senate Committee on Commerce, Science, and Transportation