Congressional Research Service
Informing the legislative debate since 1914

EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding *Schrems II* and Its Impact on the EU-U.S. Privacy Shield

March 17, 2021

Congressional Research Service
https://crsreports.congress.gov
R46724

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46724

March 17, 2021

Chris D. Linebaugh
Legislative Attorney

Edward C. Liu
Legislative Attorney

EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding *Schrems II* and Its Impact on the EU-U.S. Privacy Shield

On July 16, 2020, in a decision referred to as *Schrems II*, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield (Privacy Shield). Privacy Shield is a framework developed by the European Union (EU) and the United States to facilitate cross-border transfers of personal data for commercial purposes. Privacy Shield requires companies and organizations that participate in the program to abide by various data protection requirements and, in return, assures the participants that the transfer is compliant with EU law. The CJEU, however, found Privacy Shield inadequate in part because it does not restrain U.S. intelligence authorities' data collection activities. According to the CJEU, U.S. law allows intelligence agencies to collect and use the personal data transferred under the Privacy Shield framework in a manner that is inconsistent with rights guaranteed under EU law. The CJEU focused on Section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333, and Presidential Policy Directive 28, which govern how the U.S. government may conduct surveillance of non-U.S. persons located outside of the United States.

The CJEU's *Schrems II* ruling has significant implications for personal data transfers between the EU and the United States. While the decision does not shut the door on all transfers between these jurisdictions, it does considerably narrow the manner in which they may take place. For instance, companies may still use Standard Contractual Clauses (SCCs)—contractual clauses approved by the EU that bind the companies to certain data protection standards—as an alternative to the Privacy Shield framework. But *Schrems II* held that exporters using SCCs must evaluate the legal landscape of the recipient jurisdiction and take any "supplementary measures" necessary to ensure that data is protected at the level required under EU law.

This report examines the impact of *Schrems II* in further detail. It provides an overview of EU law governing international data transfers, including the *Schrems II* decision, and it reviews the U.S. surveillance laws relevant to that decision. It concludes by discussing some considerations for Congress.

Contents

EU Law and Data Transfers 1
European Commission's Privacy Shield Decision and SCCs 3
Schrems II 5
Overview 5
Transfers after *Schrems II* 6
A Closer Look at U.S. Intelligence Law Discussed in *Schrems II* 8
FISA Section 702 8
Executive Order 12333 10
Presidential Policy Directive 28 11
Considerations for Congress 12

Contacts

Author Information 14

On July 16, 2020, in *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximillian Schrems* (*Schrems II*), the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield (Privacy Shield), a program developed by the European Union (EU) and the United States to facilitate cross-border transfers of personal data for commercial purposes.[1] The CJEU determined that U.S. surveillance for foreign intelligence purposes does not provide protections necessary under EU law for the transfer of personal data from the EU to the United States. The CJEU focused on Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA), Executive Order (E.O.) 12333, and Presidential Policy Directive 28 (PPD-28). Generally, FISA 702 and E.O. 12333 authorize surveillance of non-U.S. persons located outside of the United States, and PPD-28 prohibits certain bulk collections and limits how long agencies can retain information on non-U.S. persons.[2] The CJEU reasoned that FISA 702 and E.O. 12333, even as limited by PPD-28, allow U.S. intelligence agencies to collect more information than is strictly necessary to fulfill their missions and do not provide EU citizens with sufficient avenues for judicial redress of alleged infringements of privacy.[3]

While the CJEU struck down Privacy Shield on the grounds that U.S. surveillance law is overly permissive, the court did not close the door altogether on data transfers from the EU to the United States. Rather, *Schrems II* preserved the validity of Standard Contractual Clauses (SCCs)—a separate mechanism under EU law for international data transfers—provided that data exporters take "supplementary measures" where necessary to ensure compliance with the level of protection required under EU law.[4]

This Report gives an overview of EU law governing international transfers of personal data, including the *Schrems II* decision, and how it interacts with U.S. surveillance laws. The Report starts by laying out the requirements for international transfers under the EU's principal data protection law, the General Data Protection Regulation (GDPR). It then discusses how the European Commission—the EU's "executive arm"—has sought to enforce these requirements with respect to personal data transferred to the United States through the Privacy Shield framework and various SCCs. The Report next reviews the CJEU's *Schrems II* decision and its impact on data transfers. After taking a closer look at the U.S. surveillance laws at issue in *Schrems II*—including Section 702 of FISA, E.O. 12333, and PPD-28—the Report closes by briefly discussing some considerations for Congress.

EU Law and Data Transfers

The EU considers privacy and protection of personal data to be fundamental rights. Articles 7 and 8 of the Charter of Fundamental Rights of the EU (the Charter) provide that "everyone has the right" to the "protection of personal data concerning him or her" and that data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[5] Article 52 of the Charter states that any limitations on these rights must be "[s]ubject to the principle of proportionality" and must be "necessary and

[1] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020); *Privacy Shield Overview*, PRIVACYSHIELD.GOV, https://www.privacyshield.gov/Program-Overview (last visited Feb. 9, 2021).

[2] See the section "A Closer Look at U.S. Intelligence Law Discussed in *Schrems II*" for an overview of these laws.

[3] See the section "*Schrems II*" for a further discussion of the court's reasoning.

[4] See the section "*Schrems II*" for a further analysis of the court's discussion of SCCs, and see the section "Transfers after *Schrems II*" for a discussion of supplemental measures.

[5] Charter of Fundamental Rights of the European Union, arts. 7–8, Dec. 18, 2000, 2000 O.J. C 364/1.

genuinely meet objectives of general interest of the Union or the need to protect the rights and freedom of others."[6] Lastly, Article 47 of the Charter entitles anyone who has had these rights violated to a "fair public hearing within a reasonable time by an independent and impartial tribunal previously established by law."[7]

Along with the fundamental rights provided in the Charter, the EU has enacted the GDPR, a comprehensive, EU-wide privacy law.[8] It took effect on May 25, 2018, replacing an earlier 1995 data protection directive.[9] The GDPR generally regulates how personal data is *processed*, a broad term encompassing any operation or set of operations performed on personal data.[10] The regulation applies to "controllers" (a person or entity who determines the "purposes and means" of processing personal data) and "processors" (a person or entity who processes the data on behalf of a controller) who are (1) established in the EU, (2) offer goods or services to individuals in the EU, or (3) monitor individuals' behavior in the EU.[11]

Most relevantly, the GDPR regulates the circumstances under which controllers and processors ("exporters") may transfer personal data from the EU to foreign countries. Under Chapter V of the GDPR, an exporter generally may initiate foreign transfers only in the following situations:

1. **Adequate level of protection.** Under Article 45, the exporter may send the data to a third country that the European Commission has, after examining the country's laws and practices, determined ensures an "adequate level of protection."[12]
2. **Appropriate safeguards and SCCs.** Under Article 46, the exporter may rely on one of the "appropriate safeguards" laid out in that provision. For instance, if the exporter is a multinational organization making international transfers within its organization, it may adopt binding corporate rules that comply with certain GDPR requirements. Alternatively, if the exporter is transferring data to an unaffiliated entity, it may insert SCCs—which are specific contractual terms approved by the European Commission—into its contract with the entity.[13]
3. **Derogations.** Under Article 49, the exporter may initiate transfers falling under one of several "derogations for specific situations"; for example, these derogations apply when the data subject gave informed consent to the transfer or

[6] *Id.* art. 52.

[7] *Id.* art. 47.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR]. The GDPR is discussed in more detail in CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh, and CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[9] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 1995 O.J. 95 (L281) [hereinafter Data Protection Directive].

[10] *Id.* art. 4(2) ("'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction").

[11] *Id.* art. 4(7–8).

[12] *Id.* art. 45.

[13] *Id.* art. 46.

> where the transfer is "necessary for the performance of a contract" that is either "between the data subject and the controller" or was concluded "in the interest of the data subject."[14]

European Commission's Privacy Shield Decision and SCCs

In accordance with the GDPR's framework for international transfers, the European Commission (EC) has issued a number of decisions recognizing countries that provide an "adequate level of protection" under Article 45.[15] For purposes of this Report, the most relevant Commission adequacy determination is the 2016 Privacy Shield decision that allowed the transfer of personal data to certain U.S. companies and organizations for commercial purposes and facilitated U.S.-EU trade of digitally-enabled services.[16]

In this decision, the EC determined that transfers to the United States pursuant to the Privacy Shield framework provide an adequate level of protection to EU data subjects.[17] The EU and the United States developed Privacy Shield after the CJEU invalidated an earlier framework, the U.S.-EU Safe Harbor framework, in 2015.[18] Under Privacy Shield, organizations self-certify to the International Trade Administration (ITA) in the Department of Commerce that they comply with certain principles for protecting personal data, and the ITA conducts compliance reviews on an ongoing basis to ensure participants abide by the program's requirements.[19] Privacy Shield provides several recourse mechanisms for individuals affected by a participant's non-compliance, including a right to invoke binding arbitration.[20] Privacy Shield participants who violate the program's requirements are also subject to enforcement by the Federal Trade Commission (FTC),[21] which may challenge participants' violations as "deceptive" conduct under the Federal Trade Commission Act and may seek an administrative cease-and-desist order or a court order.[22]

---

[14] *Id.* art. 49.

[15] *See Adequacy Decisions*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Dec. 15, 2020).

[16] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Jan. 1, 2016, O.J. L. 207, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN [hereinafter *EC Privacy Shield Decision*]. For a discussion of Privacy Shield and its impact on U.S.-EU trade, see CRS In Focus IF11613, *U.S.-EU Privacy Shield*, by Rachel F. Fefer and Kristin Archick.

[17] *Id.*

[18] *See U.S.-EU Safe Harbor Framework*, FTC.GOV, HTTPS://WWW.FTC.GOV/TIPS-ADVICE/BUSINESS-CENTER/PRIVACY-AND-SECURITY/U.S.-EU-SAFE-HARBOR-FRAMEWORK (last visited Jan. 12, 2021) ("On October 6, 2015, the European Court of Justice issued a judgment declaring invalid the European Commission's July 26, 2000 decision on the legal adequacy of the U.S.-EU Safe Harbor Framework. On July 12, 2016, the European Commission issued an adequacy decision on the EU-U.S. Privacy Shield Framework. This new Framework, which replaces the Safe Harbor program, provides a legal mechanism for companies to transfer personal data from the EU to the United States.").

[19] *Privacy Shield Framework*, PRIVACYSHIELD.GOV, https://www.privacyshield.gov/EU-US-Framework (last visited Dec. 5, 2020).

[20] *Recourse, Enforcement and Liability*, PRIVACYSHIELD.GOV, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY (last visited Dec. 5, 2020).

[21] *Enforcement of Privacy Shield*, PRIVACYSHIELD.GOV, https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield (last visited Dec. 5, 2020).

[22] *Id. See also* 5 U.S.C. § 45 (FTC cease-and-desist authority). For a further discussion of the FTC's enforcement authority over "deceptive" practices, see CRS Legal Sidebar LSB10388, *Will the FTC Need to Rethink Its Enforcement Playbook (Part II)? Circuit Split Casts Doubt on the FTC's Ability to Seek Restitution in Section 13(b) Suits*, by Chris

The EC determined that these principles and recourse mechanisms ensured that Privacy Shield participants provided an adequate level of protection to data subjects.[23]

However, the EC's decision did not only analyze the obligations imposed on Privacy Shield participants. The EC also assessed the access and use of personal data by U.S. public authorities, particularly in the intelligence context.[24] The EC looked at both (1) ex-ante limitations on intelligence collection (i.e., restrictions that apply *before* the collection occurs, such as laws prohibiting certain types of collection or requiring advanced judicial approval before collection), and (2) ex-post recourse available to individuals whose data has been collected (i.e., the ability to sue or bring some legal action for relief *after* the collection occurs).[25] On the first issue, it determined that U.S. intelligence gathering from European subjects was adequately limited, particularly because PPD-28, among other things, limited bulk collection of signals intelligence to situations in which targeted collection is not possible for technical or operational reasons.[26] It also relied on various assurances from the U.S. government, such as assurances that the United States would not disseminate personal information it collects "solely because the individual concerned is a non-U.S. person."[27] As for ex-post recourse, the EC acknowledged the limited options available to non-U.S. persons, specifically noting that "standing" requirements often restrict access to ordinary courts.[28] However, the EC concluded that the United States had provided sufficient redress by creating a "new Ombudsperson Mechanism," under which a Privacy Shield Ombudsperson within the U.S. Department of State would receive complaints and work with the Intelligence Community to ensure those complaints are investigated and resolved.[29] In light of these limitations and protections, the EC concluded that the United States "ensures effective legal protection against interferences by the intelligence authorities" and that transfers under the Privacy Shield provided an "adequate level of protection."[30]

In addition to adequacy determinations under Article 45, such as the Privacy Shield Decision, the EC has also issued several sets of SCCs for transfers from EU controllers to non-EU recipients.[31] SCCs are template contract terms set by the EU that require the organization receiving the data to commit to EU-equivalent standards of data protection, even where no such protection exists under the domestic law of the receiving organization's nation.[32]

D. Linebaugh.

[23] *EC Privacy Shield Decision*, *supra* note 16, at paras. 61–63.

[24] *Id.* at paras. 64–124.

[25] *Id.*

[26] *Id.* at para. 76.

[27] *Id.* at paras. 87–88.

[28] *Id.* at para. 115.

[29] *Id.* at paras. 116–122.

[30] *Id.* at paras. 123, 136.

[31] *See Standard Contractual Clauses (SCC)*, European Comm'n (Dec. 21, 2020), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[32] *Id.*

Schrems II

Overview

In *Schrems II*, the CJEU invalidated the EC's Privacy Shield decision but preserved the validity of SCCs.[33] *Schrems II*, in brief, involved a complaint by an Austrian privacy activist, Maximillian Schrems, about Facebook's transfer of his data from its Irish subsidiary to its servers located in the United States.[34] The crux of his argument was that the United States does not provide adequate protection of his personal data, in light of its surveillance activities.[35] To resolve the action, the CJEU evaluated both the EC's Privacy Shield decision and its adoption of SCCs.[36]

On the Privacy Shield issue, the CJEU rejected the EC's conclusion that the United States ensures an adequate level of protection.[37] Its decision primarily rested on two observations about U.S. surveillance under FISA 702 and E.O. 12333: (1) the lack of ex-ante limitations ensuring that surveillance programs abide by the "principle of proportionality" (i.e., that the programs only collect data that is strictly necessary); and (2) the ineffective ex-post redress for individuals whose personal data is subject to these surveillance programs.[38]

On the first point, the CJEU explained that a public authority's collection of personal data "constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter."[39] Consequently, such an interference must "satisfy the requirement of proportionality" set forth of Article 52 of the Charter.[40] Under this proportionality requirement, the collection must be limited to what is "strictly necessary" and be governed by "clear and precise rules" and "minimum safeguards" that allow data subjects to effectively protect their personal data "against the risk of abuse."[41]

Turning to the U.S. surveillance regime, the CJEU concluded that surveillance under Section 702 of FISA and E.O. 12333 failed to meet this proportionality standard.[42] The CJEU reasoned that, for intelligence gathering programs under Section 702 of FISA, there is little judicial supervision. The CJEU observed that the U.S. Foreign Intelligence Surveillance Court (FISC) authorizes surveillance programs based on whether they relate to the objective of acquiring foreign intelligence information, but it does not review whether individuals are properly targeted for surveillance.[43] The CJEU also noted that, under E.O. 12333, U.S. authorities could intercept data in transit to the United States, such as by accessing underwater cables that traverse the Atlantic, "without that access being subject to any judicial review."[44] The CJEU acknowledged that

[33] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) [hereinafter *Schrems II*].

[34] *Id.* at paras. 50–52.

[35] *Id.* at paras. 52, 54.

[36] *Id.* at paras. 122–202.

[37] *Id.* at para. 197.

[38] *Id.* at para. 168.

[39] *Id.* at para. 171.

[40] *Id.* at paras. 174–176.

[41] *Id.* at para. 176.

[42] *Id.* at para. 184.

[43] *Id.* at para. 179.

[44] *Id.* at para. 183.

intelligence programs under Section 702 of FISA and E.O. 12333 are subject to PPD-28's restrictions on bulk collection, but it dismissed the idea that these restrictions are adequate, explaining that PPD-28 still allows bulk collection of data in situations where "the Intelligence Community cannot use an identifier associated with a specific target" to "focus the collection."[45]

Along with the lack of ex-ante limitations on these programs, the CJEU also concluded there is not effective ex-post legal redress for data subjects.[46] According to the CJEU, Article 47 of the Charter entitles "everyone whose rights and freedoms" are violated "to a hearing by an independent and impartial tribunal."[47] The CJEU explained that the surveillance programs based on Section 702 of FISA and E.O. 12333, even as limited by PPD-28, fail to meet this standard because they do not give data subjects "rights actionable in the courts against the US authorities."[48] It further rejected the EC's position that the Privacy Shield Ombudsperson could provide sufficient redress, as nothing indicated that "the ombudsperson has the power to adopt decisions that are binding on those intelligence services."[49] Given these reasons, the CJEU concluded that "Privacy Shield is invalid."[50]

In contrast to Privacy Shield, the CJEU upheld the EC's adoption of SCCs for the transfer of personal data to processors outside of the EU.[51] According to the CJEU, the important distinction between the EC's Privacy Shield decision and its SCC decision is that, under Article 46 of the GDPR, the EC is not required to "assess the adequacy of the level of protection ensured by the third country" before adopting SCCs.[52] SCCs, the CJEU explained, are inherently of a "contractual nature" and "cannot bind the public authorities of third countries."[53] Thus, the CJEU concluded that, when relying on SCCs to transmit data, it is up to the data controller to "verify, on a case-by-case basis" whether "the law of the third country of destination ensures adequate protection, under EU law" and to adopt "supplementary measures" where necessary to ensure compliance with the level of protection required under EU law.[54]

Transfers after *Schrems II*

While *Schrems II* invalidated Privacy Shield, it still left room for data transfers to the United States based on SCCs or other mechanisms under Article 46 of the GDPR. Even when relying on these mechanisms, the CJEU explained that data exporters must still analyze the law of the non-EU country and adopt any "supplementary measures" necessary to ensure the adequate protection required under EU law.[55] Although *Schrems II* did not detail what these "supplementary measures" might look like, on November 11, 2020, the European Data Protection Board ("EDPB") published recommendations (EDPB Recommendations) listing example measures.[56]

[45] *Id.* at paras. 183–184.

[46] *Id.* at paras. 186–197.

[47] *Id.* at para. 186.

[48] *Id.* at para. 192.

[49] *Id.* at para. 196.

[50] *Id.* at para. 201.

[51] *Id.* at paras. 122–149.

[52] *Id.* at para. 130.

[53] *Id.* at para. 132.

[54] *Id.* at paras. 133–135.

[55] *Id.*

[56] *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, European Data Protection Bd.* (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/

These primarily include "technical measures" such as (1) pseudonym[ization] of data so that it can "no longer be attributed to a specific subject," (2) encrypting the data in such a way that neither the recipient nor the relevant public authorities can decrypt it, or (3) splitting the data between two or more independent processers in different jurisdictions such that no individual processor can "reconstruct the personal data in whole or in part."[57]

Nevertheless, according to the EDPB there are some scenarios where "no effective" supplemental measures can be found.[58] In particular, the EDPB pointed to situations where an exporter transfers data to a "cloud service or other processor" in a third country who needs access to the data "in the clear" (i.e., unencrypted or unaltered) "in order to execute the task assigned."[59] In such situations, the EDPB said it is "incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights," given the current state of technology.[60] It did not, however, "rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear."[61]

One point of debate following *Schrems II* is whether supplementary measures are always required before transferring data potentially subject to U.S. surveillance. On the one hand, the EDPB Recommendations indicate that supplemental measures are always required in such situations.[62] Specifically, the EDPB read *Schrems II* to hold that "the level of protection of the programs authorised [*sic*] by 702 FISA is not essentially equivalent to the safeguards required under EU law."[63] Consequently, "if the data falls under 702 FISA," then it may be transferred to the United States only if "additional supplementary technical measures make access to the data transferred impossible or ineffective."[64] Although the EDPB Recommendations only mention FISA 702, its logic arguably applies to data subject to surveillance under E.O. 12333, which the CJEU also found problematic.[65] On the other hand, the U.S. government released a White Paper following *Schrems II* that took a less categorical approach than the EDPB.[66] The White Paper maintains that *Schrems II* "was *not* a ruling on whether privacy protections in U.S. law *per se* . . . are consistent with EU law."[67] Rather, according to the White Paper, the CJEU "ruled only on the validity" of the Privacy Shield decision, and its "assessment of U.S. law accordingly relied primarily on the limited findings about U.S law recorded by the EC in 2016 in [the Privacy Shield decision]."[68] The White Paper then outlines additional safeguards and redress options in U.S. law not captured

consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [hereinafter EDPB Recommendations].

[57] *Id.* at 22–26.

[58] *Id.* at 26.

[59] *Id.*

[60] *Id.* at 27.

[61] *Id.*

[62] *Id.*

[63] *Id.* at 15.

[64] *Id.*

[65] See the section "Schrems II."

[66] *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after* Schrems II, White Paper, U.S. Department of Commerce, U.S. Department of Justice, Office of the Director of National Intelligence (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

[67] *Id.* at 6.

[68] *Id.*

by the *Schrems II* decision in order to assist companies in "determining whether the law of the United States ensures adequate protection as afforded in EU law."[69]

A Closer Look at U.S. Intelligence Law Discussed in *Schrems II*

As noted above, the CJEU invalidated the EC's Privacy Shield decision because it determined that FISA Section 702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality and do not provide EU data subjects with effective judicial redress. In order to provide additional context for understanding the CJEU's decision, this section briefly discusses the relevant statutory and executive restrictions on foreign intelligence surveillance.

FISA Section 702

Congress enacted FISA in 1978 to regulate electronic surveillance conducted for national security or foreign intelligence purposes.[70] As originally enacted, electronic surveillance under FISA generally requires the government to apply for a court order with respect to each target of surveillance.[71] FISA requires the government to include information in its applications that demonstrates that probable cause exists to believe that the target of surveillance is a foreign power or an agent of a foreign power.[72] Such applications are made to, and evaluated by, the specialized FISC, which is comprised of sitting Article III judges who have been designated for that role by the Chief Justice of the U.S. Supreme Court.[73]

Congress added Section 702 in the FISA Amendments Act (FAA) of 2008 to provide less restrictive procedures for acquiring foreign intelligence information targeting non-U.S. persons who are not within the United States.[74] Surveillance under Section 702 is subject to supervision by the FISC, but the provision does not require the FISC to review individual targets of surveillance.[75] Instead, under Section 702, the FISC reviews generally applicable targeting and minimization procedures and guidelines submitted by the U.S. Attorney General and the Director of National Intelligence to determine whether they are "reasonably designed" to: (1) ensure that surveillance only targets persons who are reasonably believed to be outside the United States; and (2) prevent the intentional acquisition of purely domestic communications.[76] Once the FISC approves those procedures and guidelines, the government may issue directives to electronic communication service providers requiring them to provide the government with "all information,

[69] *Id.* at 6–22.

[70] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013); S. Rept. Nos. 95-604 (1977), 95-701 (1978).

[71] 50 U.S.C. § 1804.

[72] *Id.*

[73] *Id.* § 1803, 1804(a); *About the Foreign Intelligence Surveillance Court*, FOREIGN INTEL. SURVEILLANCE CT., https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Jan. 12, 2021).

[74] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101 (2008) [codified at 50 U.S.C. § 1881a]; s*ee also* CRS Report R44457, *Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, by Edward C. Liu.

[75] 50 U.S.C. § 1881a(j).

[76] *Id.*

facilities, or assistance" needed to conduct the surveillance in a manner that does not undermine its secrecy.[77]

The information must also be acquired from an "electronic communication service provider," or with the assistance of such a provider.[78] As used in Section 702, the term "electronic communication service provider" includes communications providers (such as telephone, email, or internet service providers (ISPs)) as well as remote computing service providers that provide "computer storage or processing services" to the public.[79] Although Section 702 requires the target of surveillance to be outside the United States (e.g., an EU citizen in Europe), the information may be acquired from facilities within the United States, such as data centers operated by U.S.-based electronic communication service providers.[80] If the government targets a non-U.S. person through an acquisition that occurs *outside* the United States, that acquisition would not necessarily be governed by FISA, including Section 702, but would still need to comply with E.O. 12333, as discussed in the following section.[81]

For example, the government has used FISA 702 to implement *downstream* (previously referred to as "PRISM") and *upstream* collection programs.[82] In downstream collection, the government typically directs consumer-facing communications service providers—such as ISPs, telephone providers, or email providers—to provide all communications "to or from" a "selector" (e.g., an email address).[83] Upstream collection similarly involves the collection of all communications "to or from" a selector, but the requests are directed at telecommunications "backbone" providers (i.e., companies that operate the long-distance, high-capacity internet cables that interconnect with ISPs' local networks) and it does not involve collection of telephone calls.[84] Under the government's procedures, the National Security Agency (NSA) is the primary intelligence agency that collects data through the downstream and upstream programs, although the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) also receive data from these programs in more limited circumstances.[85]

---

[77] *Id.* § 1881a(i).

[78] 50 U.S.C. §§ 1881a(h)(2)(A)(vi), 1881a(i).

[79] *Id.* § 1881(b)(4).

[80] *Id.* § 1881a(b) (incorporating the definition of "remote computing service" at 18 U.S.C. § 2711(2)).

[81] *See* 50 U.S.C. § 1801(f) (defining "electronic surveillance" to primarily cover the "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States"); *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and CIVIL LIBERTIES OVERSIGHT BD., 107, n. 471 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf ("FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes.") [hereinafter *PCLOB Report*].

[82] *See PCLOB Report*, *supra* note 81, at 7 ("There are two types of Section 702 acquisition: what has been referred to as 'PRISM' collection and 'upstream' collection."); NSA Stops Certain Section 702 "Upstream" Activities, NSA (April 28, 2017), https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/ ("Under Section 702, NSA collects internet communications in two ways: 'downstream' (previously referred to as PRISM) and 'upstream.'") [hereinafter *NSA Press Release*].

[83] *PCLOB Report*, *supra* note 81, at 7.

[84] *Id.* While upstream collection used to include communications "about" the selector (e.g., the target email address is referenced in the body or text of the email but they are not a party to the communication), the NSA announced in 2017 that it would no longer collect communications that are solely "about" the target. *NSA Press Release*, *supra* note 82.

[85] PCLOB Report, *supra* note 81, at 7 (explaining that the CIA and FBI each receive a "select portion of PRISM

In *Schrems II*, the CJEU cited Section 702's limitations on judicial remedies for EU citizens as falling short of the GDPR's requirements.[86] An electronic communication service provider may challenge a government directive, in which case the FISC reviews the directive to determine whether it complies with Section 702.[87] Additionally, if the government elects to use evidence derived from Section 702 surveillance against an individual in a criminal prosecution or other enforcement action, the defendant must generally be given notice that such surveillance occurred, and a court may review the legality of the surveillance in that context.[88] However, absent these circumstances, there is generally no opportunity for targets of surveillance to know whether their communications or information have been acquired by the government under Section 702, and as a result, fewer opportunities may exist to seek judicial review of that acquisition.

The CJEU did not appear to object to traditional FISA surveillance (i.e., FISA surveillance outside of Section 702), even though such surveillance also has the same limits on post-hoc judicial remedies as Section 702. However, because traditional FISA surveillance requires the U.S. government to obtain an individualized court order to proceed, the lack of such requirements in Section 702, combined with the lack of fulsome post-hoc judicial review under FISA generally, may have drawn particular attention from the CJEU.

Executive Order 12333

In its *Schrems II* decision, the CJEU also objected to surveillance conducted under E.O. 12333, United States Intelligence Activities, which addresses the organization and allocation of foreign intelligence surveillance responsibilities among elements of the U.S. Intelligence Community.[89] E.O. 12333 addresses all U.S. foreign intelligence surveillance activities, including those which may fall outside of FISA's statutory scheme, such as activities conducted overseas targeting non-U.S. persons.[90] Under E.O. 12333, the NSA may "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions."[91] As described in a 2014 report by the Privacy and Civil Liberties Oversight Board:

> The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within

collection" and that "upstream collection is received only by the NSA" and "neither the CIA nor the FBI has access to unminimized upstream data."); Foreign Intelligence Surveillance Court Memorandum Opinion and Order at 11–12 (FISA Ct. Apr. 26, 2017), available at https://assets.documentcloud.org/documents/3718776/2016-Cert-FISC-Memo-Opin-Order-Apr-2017-1.pdf (Explaining that, "under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702" but that "FBI Targeting Procedures" come into play in certain classified circumstances.)

[86] See the section "*Schrems II*."

[87] 50 U.S.C. § 1881a(i)(4).

[88] *Id.* § 1806. Amendments to Section 702 made in 2018 created additional protections for querying of information collected under Section 702 or use of such information in criminal prosecutions, but these protections primarily apply to U.S. persons. Pub. L. No. 115-118, §§ 101, 102.

[89] *See* Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981) (as amended).

[90] *See* Brennan Ctr., *Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page* (Oct. 25, 2018), https://www.brennancenter.org/our-work/research-reports/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333.

[91] Exec. Order No. 12333, § 1.7(c)(1).

> the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.[92]

E.O. 12333 also includes some privacy protections generally applicable to U.S. foreign intelligence surveillance, but these do not appear to extend to non-U.S. persons. For example, with respect to surveillance conducted abroad, the order requires the Attorney General to determine that probable cause exists to believe that the target of surveillance is an agent of a foreign power, but only if the surveillance is against a U.S. person under circumstances in which a warrant would have been required for law enforcement purposes.[93] Furthermore, the order also expressly states that it does not create any legally enforceable right or benefit against the United States.[94] As a result, the CJEU found that EU data subjects did not have enforceable rights under E.O. 12333, and that the order did not include sufficient protections to limit surveillance to only what was strictly necessary.[95]

Presidential Policy Directive 28

In 2014, President Obama issued PPD-28 in the aftermath of allegations by Edward Snowden that the government had been collecting intelligence data in "bulk."[96] "Bulk" collection refers to the gathering by intelligence agencies of large quantities of intelligence data without the use of "discriminants" such as "specific identifiers" or "selection terms."[97] While PPD-28 recognizes that bulk collections must sometimes be used to identify threats, it limits intelligence agencies' ability to use data gathered through bulk collections. In particular, this data may only be used to detect and counter:

> (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[98]

Along with bulk collection limitations, PPD-28 also contains requirements designed to safeguard individuals' personal information without regard to their nationality or place of residence. For instance, PPD-28 only allows intelligence agencies to disseminate or retain personal information if the dissemination or retention of comparable information concerning U.S. persons would be permitted under E.O. 12333.[99] PPD-28 also contains data security and access requirements, which, among other things, limit access to personal information to "authorized personnel with a need to know the information to perform their mission."[100]

---

[92] *PCLOB Report*, *supra* note 81, at 107.

[93] Exec. Order No. 12333, § 2.5.

[94] *Id.* § 3.6(c).

[95] *Supra Schrems II* at paras. 184, 192.

[96] Press Release, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[97] *Id.* at n. 5.

[98] *Id.*

[99] *Id.*

[100] *Id.*

Like E.O. 12333, PPD-28 does not purport to provide judicially enforceable rights for private persons who may have been subject to surveillance in violation of the directive's provisions. Similarly, the CJEU suggested that because PPD-28 may allow for bulk data collection and did not provide non-U.S. citizens with actionable rights in court, it also fell short of the requirements under the GDPR.[101]

Considerations for Congress

The CJEU's Privacy Shield ruling has significant implications for data transfers between the United States and the EU. As discussed in CRS In Focus IF11613, *U.S.-EU Privacy Shield*, by Rachel F. Fefer and Kristin Archick, transatlantic data flows are an integral part of the $5.5 trillion U.S.-European economic relationship. Before *Schrems II*, many businesses and organizations relied on the Privacy Shield framework to make international transfers: the program had 5,380 participants as of July 2020.[102] At the same time, the impact of *Schrems II* extends beyond organizations that relied on Privacy Shield. Under *Schrems II* and the EDPB Recommendations, even exporters relying on SCCs and similar transfer tools must now make case-by-case evaluations to see if U.S. intelligence laws and practices (such as surveillance programs under FISA Section 702) "impinge on the effectiveness" of the transfer tool.[103] If they do, these exporters must adopt any necessary "supplemental measures."[104] This standard may, in some cases, prohibit transfers altogether. For instance, the EDPB Recommendations suggest that, under current technology, there may not be any supplemental measures that would allow an exporter to transfer data to a U.S.-based cloud service provider who "needs access to the data in the clear in order to execute the task assigned."[105]

Some Members of Congress have expressed interest in resolving the issues raised by *Schrems II*, with the U.S. Senate Committee on Commerce, Science, and Transportation holding a hearing on the topic in December 2020.[106] The CJEU did not give a precise roadmap of what steps the United States needs to take to provide an adequate level of protection to EU data subjects. However, governmental solutions could come from several directions:

- **Executive Action.** Purely executive action could address some of the intelligence collection concerns raised in *Schrems II*. For instance, the President could issue an Executive Order that further limits bulk intelligence collections and that provides additional redress mechanisms, such as an executive office or tribunal with the power to adjudicate complaints and issue binding decisions on the Intelligence Community.
- **Diplomacy.** U.S. and EU government officials could negotiate a diplomatic solution. For instance, the U.S. executive branch and the EC might agree to a new a framework that would replace Privacy Shield and result in a new adequacy determination by the EC. The U.S. Department of Commerce and the EC have already initiated discussions to "evaluate the potential for an enhanced EU-U.S.

[101] See the section "*Schrems II*."

[102] CRS In Focus IF11613*, U.S.-EU Privacy Shield,* by Rachel F. Fefer and Kristin Archick.

[103] EDPB Recommendations, *supra* note 62, at 3.

[104] *Id.*

[105] *Id.* at 26–27.

[106] *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing before the S. Comm. on Commerce, Science, and Transp.*, 116th Cong. (2020) [hereinafter *Privacy Shield Hearing*].

Privacy Shield framework" that would comply with *Schrems II*.[107] However, as happened with Privacy Shield, the CJEU could invalidate any new adequacy decision if it determines the decision is inconsistent with the GDPR or the Charter of Fundamental Rights. Alternatively, the United States and the EU could enter into a treaty governing data transfers between the two jurisdictions.[108] While a treaty would have superior legal force to EU regulations, such as the GDPR, it would not prevail over primary sources of EU law, such as the Charter of Fundamental Rights.[109]

- **Legislation.** Congress might adopt statutory requirements addressing the CJEU's concerns. For instance, it could amend FISA to prohibit bulk intelligence collections and require court approval with respect to each target of surveillance. It could further create a cause of action that would allow foreign subjects to bring complaints before a tribunal if they believe intelligence agencies have collected or used their data in an unlawful way. These solutions may raise complex constitutional issues, such as separation of powers and Article III standing concerns, both of which are beyond the scope of this Report.

While not directly addressing the issues raised in *Schrems II*, some commentators have also maintained that the United States' adoption of a comprehensive federal data protection law applicable to commercial entities could facilitate transatlantic data transfers.[110] Assuming the surveillance concerns are also addressed, a comprehensive data protection law could result in the EC determining that the United States provides an "adequate level of protection" under Article 45 of the GDPR. Such a determination would mean that data exporters would no longer need to rely on international executive agreements such as Privacy Shield or on mechanisms such as SCCs in order to transfer data to the United States.[111]

[107] *See* Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders, U.S. DEP'T OF COMMERCE (Aug. 10, 2020), https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.

[108] For a discussion of the U.S. treaty process, see CRS Report RL32528, *International Law and Agreements: Their Effect upon U.S. Law*, by Stephen P. Mulligan. For a discussion of the EU treaty process, see *Ratification Process*, EUR-LEX, https://eur-lex.europa.eu/summary/glossary/ratification_process.html (last visited Feb. 23, 2021).

[109] *See Sources of European Law*, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14534 (last visited Feb. 23, 2021).

[110] *See Privacy Shield Hearing*, *supra* note 106 (written statement of Prof. Neil M. Richards) ("Comprehensive consumer privacy reform from this Committee, coupled with federal surveillance reform could result not just in another second-best international data transfer agreement, but in an adequacy determination by the European Commission.") (written statement of Peter Swire) ("I believe that enactment of comprehensive commercial privacy legislation would greatly improve the overall atmosphere in Europe for negotiations between the EU and the U.S. about the effects of *Schrems II*.").

[111] While a discussion of a comprehensive data protection law is beyond the scope of this report, data protection issues are discussed more fully in CRS Report R45631, Data Protection Law: An Overview, by Stephen P. Mulligan and Chris D. Linebaugh. Furthermore, CRS Legal Sidebar LSB10441, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, by Jonathan M. Gaffney, discusses the various data protection bills proposed in the 116th Congress.

Author Information

Chris D. Linebaugh
Legislative Attorney

Edward C. Liu
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.