The U.S. Perspective on *Schrems II*: The Challenges of the Extraterritorial Application of the EU Perspective

Jordan L. Fischer, Esq.[*]

I. INTRODUCTION

There is an increasingly growing tension between the United States (U.S.) and the European Union (EU) related to personal data. Businesses of all sizes both actively and passively transfer data across multiple borders on a daily basis. In fact, it feels challenging to avoid crossing over borders in interactions with customers, suppliers, and consumers. The increasing reliance on the free flows of data across the globe for businesses across all industries does not fit squarely within the framework of data privacy and security regulations that apply within set jurisdictions and boundaries.

Within an already complex regulatory environment, courts and legislatures are grappling with the tensions of the free flow of data and how to apply their laws while respecting the inherently global nature of the digital economy and the sovereignty of third-country legal systems. Within this backdrop, the EU, with its adoption of the General Data

[*] Jordan L. Fischer is a Professor of Law at the Thomas R. Kline School of Law, Drexel University and a Lecturer at the UC Berkeley School of Information. She is also the Global Privacy Team Lead at Beckage.

Protection Regulation (GDPR), continues to drive global privacy initiatives with its robust privacy protections and enforcement, including the impact of cross-border data transfer of personal data. But its approach to privacy and the regulation of data protection do not always align with the U.S. approach to these domains.

In 2017, the combined Gross Domestic Product of the EU and the U.S. equated to approximately thirty-two percent (32%) of the global Gross Domestic Product.[1] With their combined economic weight, the privacy tensions between the EU and the U.S. dominate the global discussion and demand that the two regions develop a solution to address these continued privacy concerns. This Article provides an overview of the EU and U.S.'s legal jousting to the continued cross-border data transfers between these two regions, focusing on the Court of Justice of the European Union's (ECJ) decision in *Schrems II* to highlight the challenges going forward with regional data protection laws and global data transfers.

Part II will detail the cross-border data transfer requirements under the GDPR, focusing on the evolving agreements between the EU and the U.S. to attempt to create effective cross-border data transfer mechanisms between these two regions. Part III explores the ECJ's decision in *Schrems II*, providing insight into the continued criticism that the EU lodges against U.S. surveillance law. Part IV details the response to *Schrems II* in both the EU and U.S. Finally, Part V highlights challenges in applying the ECJ's decision to the real-world digital economy.

II. CROSS-BORDER PERSONAL DATA TRANSFERS UNDER THE GDPR

The GDPR provides for a number of mechanisms to transfer data out of the EU to a third country.[2] All permissible mechanisms must be applied "in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."[3] Two specific mechanisms under the GDPR for the transfer of personal data from the

[1] *The 2017 Results of the International Comparison Program*, EUROSTAT (May 19, 2020), https://ec.europa.eu/eurostat/documents/2995521/10868691/2-19052020-BP-EN.pdf.

[2] Commission Regulation 2016/679 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), ch. V., 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4227-1-1.

[3] *Id.* at art. 44.

EU to the U.S. are relevant to *Schrems II*: first, the use of Standard Contractual Clauses (SCCs);[4] and second, an adequacy decision.[5]

The GDPR permits the transfer of personal data "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."[6] One of the recognized "appropriate safeguards" is "standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)."[7] At issue in *Schrems II* was Decision 20110/87/EU,[8] whereby the EU Commission adopted the use of the SCCs for the transfer of personal data from an EU-based Controller to a non-EU-based Processor.

Second, under the GDPR, the EU Commission has the authority to adopt an "adequacy decision," thereby finding that "the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection."[9] The factors that should be considered include "how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law."[10]

A. *The U.S.-EU Safe Harbor Provisions*

On July 26, 2000, the EU Commission adopted opinion 2000/520/EC[11] creating the U.S.-EU Safe Harbor Provisions for the transfer of personal data between the EU and the U.S. At that time, EU

---

4 *Id.* at art. 46(2)(c).

5 *Id.* at art. 45.

6 *Id.* at art. 46(1).

7 *Id.* at art. 46(2)(c).

8 *See* Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=en.

9 GDPR, *supra* note 2, at art. 45(1).

10 *Id.* at Recital 104.

11 Commission Decision (EC) No. 2000/520 of 26 July 2000, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=en [hereinafter Decision 2000/520].

data protection operated under Directive 95/46/EC,[12] the precursor to the GDPR. Much like the GDPR, the Directive provided that personal data could be transferred to a third country if that third country "ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer."[13]

Under its July 2000 Decision, the EU Commission held that companies who comply with the safe harbor privacy principles, publicly display their privacy policies, and are subject to the jurisdiction of the Federal Trade Commission (FTC) would be deemed to provide adequate protection for personal data transferred from the EU to the U.S.[14] For the next fifteen years, the Safe Harbor Provisions remained a valid mechanism for companies to transfer personal data between the EU and the U.S.

On October 6, 2015, the ECJ held that the Safe Harbor Provisions were not valid for the transfer of personal data.[15] In support of this invalidation, in the *Schrems I*[16] decision, the ECJ found that:

> "national security, public interest, or law enforcement requirements" have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.[17]

This derogation from the principles of privacy did not include any limit to U.S. interference with personal data transferred to the U.S. or "the existence of effective legal protection against interference of that kind."[18]

---

[12] Commission Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data, 1995 O.J. (L 281) 31, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

[13] Decision 2000/520, *supra* note 11, at ¶ 1.

[14] *Id.* at ¶ 5.

[15] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650; *see also* Press Release, Statement on the Implementation of the Judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), Article 29 Working Party, (Oct. 16, 2015), https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[16] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6785411.

[17] *Id.* at ¶ 86.

[18] *Id.* at ¶¶ 88, 89.

The ECJ did recognize that the term "adequate" does not equate to a requirement that the third country "ensure a level of protection identical to that guaranteed in the EU legal order."[19] Instead, an adequate level of protection sufficient to permit the transfer of personal data

> must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.[20]

Even with this backdrop that the U.S. must not directly match those protections within the EU legal system, the ECJ still found that the Safe Harbor Provisions, coupled with the protections (or lack thereof) within the U.S. legal system, did not sufficiently provide an adequate level of protection for EU personal data transferred to the U.S.

B. *The EU-U.S. Privacy Shield*

The *Schrems I* decision placed the continued transfer of personal data from the EU to the U.S. into a tailspin. Both the EU Commission and the U.S. Department of Commerce were quick to respond.

On July 12, 2016, the EU Commission adopted Decision (EU) 2016/1250[21] finding that the EU-U.S. Privacy Shield provided adequate protection for the transfer of personal data from the EU to the U.S. In its Decision, the EU Commission explained that:

> The EU-U.S. Privacy Shield is based on a system of self-certification by which U.S. organisations commit to a set of privacy principles—the EU-U.S. Privacy Shield Framework Principles, including the Supplemental Principles (hereinafter together: 'the Principles')—issued by the U.S. Department of Commerce and contained in Annex II to this decision. It applies to both controllers and processors (agents), with the specificity that processors must be contractually bound to act only on instructions from the EU controller and assist the

---

[19] *Id.* at ¶ 73.

[20] *Id.*

[21] 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, 2016 O.J. (L 207) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN [hereinafter Decision 2016/1250].

> latter in responding to individuals exercising their rights under the Principles.[22]

Further, the EU Commission specifically found that "[t]he protection afforded to personal data by the Privacy Shield applies to any EU data subject whose personal data have been transferred from the Union to organisations in the U.S. that have self-certified their adherence to the Principles with the Department of Commerce."[23] As it relates to the provision of individual remedies, the EU Commission found that the EU-U.S. Privacy Shield "provides data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by U.S. self-certified companies[,] and to have their complaints resolved, if necessary by a decision providing an effective remedy."[24]

Highly relevant to the subsequent judgment in *Schrems II*, the EU Commission specifically assessed the access and use of any personal data transferred to the U.S. by U.S. Public Authorities.[25] Relying on specific "representations and commitments" made by the Office of the Director of National Intelligence (ODNI), the EU Commission ultimately held that "the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield."[26] The EU Commission based this finding on the following core findings of U.S. law.

First, Presidential Policy Directive 28 (PPD-28) imposes limitations on "signals intelligence" operations. Specifically, "signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose."[27] Further, these surveillance activities must be "as tailored as feasible," and "bulk collection will only occur where targeted collection via the use of discriminants—i.e., an identifier associated with a specific target (such as the target's e-mail address or phone number)—is not possible 'due to technical or operational considerations.'"[28] The EU Commission found that the assurances provided by the U.S. in relation to any surveillance collection

---

22 *Id.* at, ¶ 14.
23 *Id.* at ¶ 16.
24 *Id.* at ¶ 41.
25 *Id.* at § 3.
26 *Id*. at ¶ 136.
27 Decision 2016/1250, *supra* note 21, ¶ 70.
28 *Id.* at ¶¶ 71, 72.

of personal data "capture the essence of the principles of necessity and proportionality."[29]

Second, in its review of the Foreign Intelligence Surveillance Act (FISA) and the Federal Bureau of Investigation's (FBI) use of National Security Letters (NSL), the EU Commission found that "insofar as personal data to be transferred under the EU-U.S. Privacy Shield are concerned, these authorities equally restrict interference by public authorities to targeted collection and access."[30] To the extent any surveillance activities are taken, those activities "consist[] entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made."[31]

Third, the EU Commission received express assurances from the U.S. government that the "U.S. Intelligence Community 'does not engage in indiscriminate surveillance of anyone, including ordinary European citizens.'"[32] Further, the EU Commission found that the U.S. assurances were "supported by empirical evidence which shows that *access requests* through NSL and under FISA, both individually and together, only concern a relatively small number of targets when compared to the overall flow of data on the internet."[33]

Fourth, the surveillance activities within the U.S. are "subject to various review and oversight mechanisms that fall within the three branches of the State,"[34] providing adequate oversight to any surveillance of EU personal data. These oversight measures include "civil liberties or privacy officers, Inspector Generals, the ODNI Civil Liberties and Privacy Office, the Privacy and Civil Liberties Oversight Board, and the President's Intelligence Oversight Board."[35] And, these oversight activities are accompanied by "extensive reporting requirements" to address noncompliance, including Congressional reporting requirements.[36]

Fifth, the EU Commission found that "[a] number of avenues are available under U.S. law to EU data subjects if they have concerns whether their personal data have been processed (collected, accessed, etc.) by U.S. Intelligence Community elements, and if so, whether the

[29] *Id.* at ¶ 76.
[30] *Id.* at ¶ 80.
[31] *Id.* at ¶ 81.
[32] *Id.* at ¶ 82.
[33] Decision 2016/1250, *supra* note 21, at ¶ 82 (emphasis in original).
[34] *Id.* at ¶ 92.
[35] *Id.* at ¶ 95.
[36] *Id.* at ¶¶ 101, 102.

limitations applicable in U.S. law have been complied with."[37] Judicial redress against both the agencies and the individual actors within the agencies, plus the opportunity to learn of surveillance through the Freedom of Information Act (FOIA), combine to create sufficient safeguards for individuals to seek redress for any unlawful surveillance impacting their personal data.[38] In addition, the U.S. made commitments to appoint an Ombudsperson to investigate and address any noncompliance with the Shield principles.[39]

Based on its assessment of the current legal structure in the U.S., and assurances from the U.S. government, the EU Commission ultimately concluded that "the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield."[40]

III. THE ECJ'S DECISION IN *SCHREMS II*

In light of the holdings in *Schrems I*, Max Schrems, the plaintiff in both the *Schrems I* and *Schrems II* cases, reformulated his complaint to address Facebook's continued use of the SCCs to transfer personal data from the EU to the U.S. Again, the High Court of Ireland referred questions regarding the transfer of personal data from the EU to the U.S., specifically questioning the limitations of certain U.S. surveillance laws and the adequacy of the SCCs to ensure appropriate protections for personal data transferred.[41]

In many ways, the *Schrems II* decision feels like a reformulation of the *Schrems I* decision. First, the ECJ made clear that EU data protection regulations still apply both during and after the transfer of personal data from the EU to a third country.[42] Further, the ECJ clarified that the future processing of the personal data for certain national security purposes does not negate the applicability of the GDPR to that personal data once transferred:

> The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing

[37] *Id.* at ¶ 111.

[38] *Id.* at ¶¶ 113, 114.

[39] Decision 2016/1250, *supra* note 21, at ¶¶ 117–22.

[40] *Id.* at ¶ 123.

[41] Case C-311/18, Data Prot. Comm'r v. Facebook Ir., Ltd., 2020 E.C.R. 559, ¶ 68, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=380028.

[42] *Id.* at ¶ 83.

> for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.[43]

Second, the ECJ turned to the continued validity of the Standard Contractual Clauses, and emphasized that "the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country."[44] Further, the GDPR provides that to the extent that a third country does not itself provide an adequate level of protection for personal data, then "the appropriate safeguards to be taken by the controller or processor . . . must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union.'"[45]

The ECJ provided three factors to be used to assess whether a transfer under contractual clauses provides an adequate level of protection: "data subjects must be afforded appropriate safeguards, enforceable rights[,] and effective legal remedies."[46] Ultimately, whether transfers are permitted under EU law is determined by whether data subjects "are afforded a level of protection essentially equivalent to that guaranteed within the EU by that regulation, read in the light of the Charter."[47]

Applying these factors to the SCCs, the ECJ clarified that the SCCs are a general document, and do not apply or address any specific third country's legal adequacy.[48] Further, since the SCCs are a contractual agreement between two parties, the responsibility of confirming the adequacy of their use lies with the

> controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.[49]

---

[43] *Id.* at ¶ 86.

[44] *Id.* ¶ 93.

[45] *Id.* ¶ 95 (citing GDPR, *supra* note 2, at Recital 108).

[46] *Id.* ¶ 103.

[47] Case C-311/18, Data Prot. Comm'r v. Facebook Ir., Ltd., 2020 E.C.R. 559, at ¶ 105.

[48] *Id.* ¶ 133.

[49] *Id.* ¶ 134.

As such, the obligation of confirming the valid use of the SCCs in the transfer of personal data from the EU to a third country is solely placed on the parties to the SCCs themselves. The ECJ expressly directs "the controller established in the European Union and the recipient of personal data to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses in the annex to the SCC Decision."[50]

Third, the ECJ, somewhat on its own initiative, assessed the validity of the EU-U.S. Privacy Shield, ultimately holding that it was an invalid mechanism to transfer personal data under the GDPR.[51] Initially, the ECJ recognized that similar to the Safe Harbor Decision, the EU-U.S. Privacy Shield provides primacy to U.S. national security, public interest, and law enforcement requirements over the principles laid down in the Privacy Shield.[52] And, in order for that primacy to be valid under the GDPR, it must be proportionate and limited to what is strictly necessary to obtain goals associated with the personal data processing. The ECJ states that

> in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[53]

As applied to the U.S. surveillance laws, the ECJ held that "Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-U.S. persons potentially targeted by those programmes."[54] Further, the ECJ held that

> PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy

[50] *Id.* ¶ 141.

[51] *Id.* ¶ 201.

[52] *Id.* ¶ 164.

[53] Case C-311/18, Data Prot. Comm'r v. Facebook Ir., Ltd., 2020 E.C.R. 559, at ¶ 176.

[54] *Id.* ¶ 180.

> Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.[55]

Ultimately, in invalidating the EU-U.S. Privacy Shield, the ECJ held that "neither Section 702 of the FISA, nor EO 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programs based on those provisions cannot be regarded as limited to what is strictly necessary."[56]

IV. THE RESPONSE TO *SCHREMS II*

The ECJ's decision in *Schrems II* launched a grenade into an already tense and impactful area of the law. With economic pressures to allow the continued exchange of personal data between the U.S. and the EU, both the U.S. and the EU immediately signaled a desire to address the concerns raised in *Schrems II* and work toward a solution.

A. *The EU Response*

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), the EU agencies charged with oversight of the GDPR, generally welcomed the decision as a reaffirmation of the need to protect personal data both within and outside of the EU.[57] The EDPB expressly stated that

> EDPB intends to continue playing a constructive part in securing a transatlantic transfer of personal data that benefits EEA citizens and organisations and stands ready to provide the European Commission with assistance and guidance to help it build, together with the U.S., a new framework that fully complies with EU data protection law.[58]

---

[55] *Id.* ¶ 181.

[56] *Id.* ¶ 184.

[57] Press Release, EDPS Statement Following the Court of Justice Ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), European Data Protection Supervisor, (July 17, 2020), https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en; Press Release, Statement on the Court of Justice of the European Union Judgment in Case C-311/18––Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Eur. Data Prot. Bd. (July 17, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20200717_cjeujudgmentc-311_18_en.pdf [hereinafter EDPB Statement].

[58] EDPB Statement, *supra* note 57, at 2.

In an effort to provide clarity to the impact of the *Schrems II* decision, the EDPB provided a "Frequently Asked Questions" document,[59] which addressed the many questions posed by supervisory authorities and businesses. The EDPB clarified that the *Schrems II* decision was not limited in application only to transfers under the SCCs and the Privacy Shield: "the threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country."[60] Further, the EDPB reiterated that as it relates to reviewing whether adequate safeguards are in place to permit the continued transfer of personal data, "it is the primary responsibility of the data exporter and the data importer to make this assessment, and to provide necessary supplementary measures."[61]

In supplemental Recommendations,[62] the EDPB provided a "roadmap" and additional guidance on tools that controllers and processors can implement as supplementary measures to ensure adequate protections for transferred personal data.[63] The EDPB explains that "'supplementary measures' are by definition supplementary to the safeguards the Article 46 GDPR transfer tool already provides."[64] Further, "supplementary measures may have a contractual, technical or organisational nature. Combining diverse measures in a way that they support and build on each other may enhance the level of protection and may therefore contribute to reaching EU standards."[65] Examples of supplementary measures include encryption, pseudonymization, and split or multi-party processing.[66]

Even in light of this guidance, the EU continues to assess the validity of cross-border data transfers under *Schrems II*. Individual EU member states have also weighed in on this influential decision. Within a week of the release of the ECJ's decision, Member State Supervisory

---

[59] *See Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18––Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, EUROPEAN DATA PROT. BD. (July 23, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[60] *Id*. at 2.

[61] *Id*. at 5.

[62] *See Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUR. DATA PROT. BD. (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[63] *Id*. ¶ 6.

[64] *Id*. ¶ 45.

[65] *Id*. ¶ 47.

[66] *Id*. at Annex 2.

Authorities began to weigh in with varying responses. Certain Member States affirmed the ruling but pledged to work with companies to develop solutions to the invalidation of the EU-U.S. Privacy Shield.[67] Yet other Member States, notably Germany and Ireland, called into question the continued transfer of personal data to the U.S.[68] The Berlin Commissioner for Data Protection and Freedom of Information went so far as to advise companies to transfer all personal data to Europe and process only within Europe.[69]

B. *The U.S. Response*

The U.S., like the EU, immediately issued responses to *Schrems II*. U.S. Secretary of Commerce Wilbur Ross issued a statement expressing that he was "disappointed" in the decision, but reiterated that the U.S.

> w[ould] remain in close contact with the European Commission and European Data Protection Board on this matter and hope[s] to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments.[70]

Further, in September 2020, the U.S. Department of Commerce, in conjunction with the Department of Justice and the Office of the Director of National Intelligence issued a white paper, "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II".[71] The White Paper addressed

---

[67] *See, e.g.*, *Updated ICO statement on the judgment of the European Court of Justice in the Schrems II case*, INFO. COMM'RS OFFICE (July 20, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case.

[68] *See, e.g.*, *DPC statement on CJEU decision*, DATA PROT. COMM'N (July 16, 2020), https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision (noting that the EJC "ruled that the SCCs transfer mechanism used to transfer data to countries worldwide is, in principle, valid, although it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable"); *Schwere Zeiten für den internationalen Datenaustausch*, DPA HAMBURG (July 16, 2020), https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems.

[69] *Nach „Schrems II": Europa braucht digitale Eigenständigkeit*, DPA BERLIN (July 17, 2020), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf.

[70] Press Release, U.S. Dep't. of Commerce, U.S. Sec'y of Commerce Wilbur Ross Statement on *Schrems II* Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://2017-2021.commerce.gov/index.php/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.html.

[71] U.S. DEP'T OF COMMERCE ET AL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER *SCHREMS II* (2020),

three key areas. First, many companies are not subject to laws that would permit the U.S. Intelligence Community to access the data collected and processed.[72] Second, information collected by the Intelligence Community is often shared between the U.S. and the EU as part of diplomatic relations.[73] Third, the U.S. legal framework maintains privacy protections that restrict governmental access to personal information.[74]

The White Paper directly addressed two of the key sources relied on by the ECJ's *Schrems II* decision: Executive Order 12333 (EO 12333) and Section 702 of the Foreign Intelligence Surveillance Act (FISA § 702).[75] First, the White Paper dismissed summarily the risks associated with EO 12333, which it stated relates to general surveillance matters and provides no specifics related to accessing personal information collected and stored by private companies.[76]

Second, the White Paper provides analysis of FISA § 702, which permits the U.S. government to conduct targeted surveillance of non-U.S. citizens located outside of the U.S.[77] Surveillance requests under FISA § 702 relate only to communications obtained via the assistance of an electronic communications service provider. The White Paper highlighted that FISA § 720 establishes a judicial process regarding data acquisition for non-U.S. persons. And "the overwhelming majority of companies have never received orders to disclose data under FISA § 702 and have never otherwise provided personal data to U.S. intelligence agencies."[78]

Further, before U.S. surveillance agencies can obtain information under FISA § 720, they must obtain approval from the Foreign Intelligence Surveillance Court (FISA Court) and the surveillance agency must inform the service provider.[79] The FISA Court ensures that U.S. surveillance is "targeted," and limits the "purpose of the surveillance to a specified type of foreign surveillance."[80] Further, the White Paper

https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaper FORMATTEDFINAL508COMPLIANT.PDF [hereinafter WHITE PAPER].

72 *Id.*

73 *Id.*

74 *Id.*

75 *Id.* at 2.

76 WHITE PAPER, *supra* note 71, at 2.

77 *Id.* at 2.

78 *Id.*

79 *Id.* at 6–7.

80 *Id.*

makes clear that "[t]he government must record in every case the reasons a specific person was targeted."[81]

Continuing to highlight the deficiencies in the ECJ's analysis, the White Paper infers that the ECJ took theoretical possibilities to be truths, which distorted the view of U.S. surveillance laws:

> The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data. Moreover, this theoretical possibility exists with respect to data held anywhere in the world, so the transfer of data from the EU to the United States in particular does not increase the risk of such unilateral access to EU citizens' data.[82]

The White Paper directly addresses a concern raised by the ECJ, "namely, whether U.S. law provides individual redress for violations of the FISA 702 program."[83] The White Paper outlined a number of redress mechanisms, including the FISA statute itself, which provides individuals with the ability to seek compensatory and punitive damages, and the Electronic Communications Privacy Act, which "provides a separate cause of action for compensatory damages and attorney's fees against the government for willful violations of various FISA provisions."[84]

Finally, the White Paper outlined the measures taken since 2017, when Congress considered whether to reauthorize FISA. Specifically, Congress removed the ability to seek communications "about" an individual, and instead limited communication collections to only those that are to or from the individual targeted by surveillance. This change "reduces the potential for collection of personal data of EU (and other non-U.S.) citizens because their communications now may no longer be acquired under FISA 702 solely because a communication contains a reference to a lawfully tasked selector."[85]

Additionally, Congress passed amendments in 2018 that incorporated additional privacy protections into data collections under FISA § 702. These amendments included annual certifications of more targeted data collection, increasing the agencies required to maintain a

---

81 *Id.* at 8.

82 *Id.* at 3.

83 WHITE PAPER, *supra* note 71, at 12.

84 *Id.*

85 *Id.* at 14.

Privacy and Civil Liberties Officer, and heightened reporting requirements.[86] The White Paper encourages companies to be aware of, and use, these amendments to demonstrate that privacy protections are upheld for personal data transferred from the EU to the U.S.[87]

Overall, the White Paper seeks to refute the ECJ's conclusions regarding U.S. surveillance law. In fact, the White Paper highlights that there are numerous protections within the U.S. legal system that the ECJ did not address in its decision:

> There are numerous other privacy safeguards in this area of U.S. law, not discussed by the ECJ in its review of Commission Decision 2016/1250 in *Schrems II*, that ensure that U.S. intelligence agencies' access to data is based on clear and accessible legal rules, proportionate access to data for legitimate purposes, supervision of compliance with those rules through independent and multi-layered oversight, and effective remedies for violations of rights.[88]

Ultimately, this response sought to provide clarity into the U.S. legal system and directly refute many assertions made in the ECJ decision and in lower court decisions related to U.S. surveillance law.

V. MOVING FORWARD: THE FUTURE OF LEGAL SOVEREIGNTY WITH CROSS-BORDER DATA TRANSFERS

Schrems I and *Schrems II* expose the challenges in applying one region's legal framework to data that flows freely across borders and around the world. The ECJ's approach creates two inherent oppositions to explore, one practical and one legal. On the practical side, the ECJ decision places a hard border on a borderless digital domain. On the legal side, the ECJ decision attempts to apply EU law beyond its borders in a strong, extraterritorial manner. Each is explored in turn below.

The Internet, and technology in general, have benefited from years, if not decades, of uninhibited growth and development. Many of the largest technology companies today (i.e., Apple, Google, and Facebook) sit in historically unregulated industries, or at most very lightly regulated. Because companies have been free to collect data, including personal data, with few restrictions, these companies have built infrastructures that span borders and seamlessly move data between various regions on any given day.

Ultimately, this decision, which is forcing companies to move data processing activities within the EU borders, could lead to the exclusion

86 *Id.*
87 *Id.* at 15.
88 *Id.* at 22.

of the EU from innovative services and new technologies. In essence, the ECJ's decision could become a nontariff barrier to trade that isolates the EU economy and hinders its global participation.[89]

In addition, it is dangerous for one jurisdiction to opine on the application and breadth of another country's legal infrastructure. While there are certainly instances where a court or regulatory authority will address another jurisdiction's law, it is generally accepted that the court will also accept the holdings and assertions made by that jurisdiction and will not conduct its own de novo review of the other jurisdiction's law.[90]

In *Schrems II*, the ECJ conducted a "cursory, and frequently unclear," review of U.S. surveillance law, and used that review to invalidate an influential international agreement between two strong economic regions.[91] This resulted in a lack of true clarity as to the ECJ's real concerns with the continued transfer of personal data to the U.S. For example, "it is not apparent what aspects of section 702 expand collection beyond what is strictly necessary or lack minimum safeguards. The court's incomplete analysis therefore provides little guidance regarding the validity of current and future adequacy decisions."[92]

Further, because of the more macro-level review, the ECJ did not necessarily understand the global picture of surveillance law in the U.S. and the intended limitations on those laws that attempt to address privacy concerns. By finding, in essence, that U.S. surveillance law and EU data protection requirements are per se incompatible, the ECJ failed to recognize areas where compatibility either already exists or could more easily be found between the two regions.

The ECJ's continual invalidation of the agreements between the EU Commission and the U.S. as it relates to personal data transfers appears to be driven by cursory reviews that do not include a deep dive into, or complete understanding, of the U.S. law at issue. As such, the ECJ is creating an increasingly high burden for the EU Commission and the U.S. in order to facilitate the continued growth of mutually beneficial trade between the two regions.

---

89 Elisabeth Meddin, *The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services*, 35 AM. U. INT'L L. REV. 997, 1017–18 (2020).

90 *See*, Andrew T. Guzman, *Determining the Appropriate Standard of Review in WTO Disputes*, 42 CORNELL INT'L L.J. 46, 53 (2009).

91 *Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield––Case C-311/18,* Data Prot. Comm'r v. Facebook Ireland Ltd., *ECLI:EU:2020:559 (July 16, 2020)*, 134 HARV. L. REV. 1567, 1571 (2021).

92 *Id.*

Additionally, the ECJ's decision does not recognize that within EU law itself, there are exceptions for access to personal data by public authorities for national security, public interest, and police activities. The GDPR expressly recognizes these exceptions: "This Regulation does not apply to the processing of personal data . . . by competent authorities for the purposes of the prevention, investigation, detection[,] or prosecution of criminal offences[,] or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[93] And, "[t]his Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union."[94]

As such, even under EU law, the activities outlined by the ECJ as incompatible with data protection requirements may, in fact, be conducted by EU Member States themselves. The ECJ does rely on its conclusion that the U.S. surveillance laws are not "necessary and proportionate" to balance an adequate level of protection for personal data while permitting activities necessary for national security.[95] Yet, the question remains if that is a true assessment of the complete legal infrastructure in the U.S. regarding the application of U.S. surveillance laws and whether the ECJ in the best position to make that assessment.

In essence, the ECJ's decision illustrates the dangers of one country opining on another country's legal infrastructure. This is, even more, the case here, where the ECJ made findings directly adverse to the assertions made by the U.S. government, both in response to *Schrems II* and in its discussions with the EU Commission in the drafting and adoption of the EU-U.S. Privacy Shield. This leaves an awkward path for the EU and the U.S. to move forward: if the ECJ will not accept the current representations by the U.S. government, what will it accept?

VI. CONCLUSION

Ultimately, the ECJ's decision in *Schrems II* highlights the challenges in creating regulatory and legal approaches that ensure that privacy protections are adequately upheld while also recognizing, and respecting, the law of different jurisdictions. The ECJ has dominated the conversation, continually questioning the adequacy of protections provided by the U.S. legal system for EU personal data. Yet, the ECJ may

93 GDPR, *supra* note 2, at art. 2.

94 *Id.* at art. 2.

95 Case C-311/18, Data Prot. Comm'r v. Facebook Ir., Ltd., 2020 E.C.R. 559, ¶ 184, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=380028.

be overstretching itself by reviewing, and disregarding, interpretations of U.S. law beyond its own jurisdiction.

It remains unclear where the EU and the U.S. will go from here. A real question remains whether companies will be able to comply with the movement toward data localization requirements when infrastructures were built with the idea of the free flow of data. Compliance and the risk of noncompliance, however, do create a meaningful incentive to determine a path forward. The EU and the U.S. represent two large economic powerhouses, and not finding a path forward to transfer personal data between these two regions is not an option.