Note

CJEU Déjà Vu: Facilitating International Data Transfers and Avoiding Internet Balkanization in the Wake of *Schrems II* by Enacting Targeted Reforms to US Surveillance Practices

*Jordan Francis**

INTRODUCTION

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued its long-awaited decision in *Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*—known to those in privacy spheres as *Schrems II*.[1] The case is the second notable milestone in privacy activist Max Schrems's[2] long-running litigation with Facebook Ireland before the Data Protection Commission of Ireland. Schrems alleges that Facebook Ireland should be prohibited from transferring personal data about him outside the European Union (EU) to Facebook Ireland's parent company, Facebook Inc., because he believes that organizations in the United States (US) cannot guarantee the level of protection that EU law demands under its data protection laws.[3] The Data Protection Commissioner referred the case to the CJEU for a preliminary ruling in 2018,

* J.D. Candidate, 2022, University of Minnesota Law School. Managing Editor, *Minnesota Law Review*, Volume 106. I would like to extend my thanks to my friends, family, and fiancée for their endless patience and support throughout this process; to Professor Fionnuala Ní Aoláin for her outstanding feedback, edits, and encouragement; to Professors William McGeveran and Alan Rozenshtein for their thought provoking courses on data privacy and cybersecurity; and the many *Minnesota Law Review* staffers and editors who worked diligently to improve upon and publish this Note.

1. *Schrems II (aka Schrems 2.0)*, IAPP, https://iapp.org/resources/article/schrems-ii-aka-schrems-2-0 [https://perma.cc/KAP5-3M8E].

2. *See generally* Tim Walker, *Max Schrems: The Austrian Law Graduate Who Became a Champion of Facebook Users*, INDEPENDENT (U.K.) (Oct. 6, 2015), https://www.independent.co.uk/life-style/gadgets-and-tech/news/max-schrems-austrian-law-graduate-who-became-champion-facebook-users-a6683711.html [https://perma.cc/N6WL-85ZR].

3. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 2 (July 16, 2020).

looking for guidance on how to interpret the EU's data protection laws in light of its Charter of Fundamental Rights.

Once stripped of its procedural minutiae, the case's premise was simple: is it legal under EU law to transfer personal data concerning EU citizens from the EU to the US? For privacy professionals, it was a case of déjà vu. The court had addressed the same question only four years prior in the predecessor case, *Schrems I*, in which the court invalidated the framework which many US-based organizations were relying on to engage in transatlantic data transfers. Many commentators expected the CJEU to find similar faults in the replacement program, Privacy Shield, which the US Department of Commerce and European Commission jointly developed in the wake of *Schrems I*. Few were prepared, however, for the court to resoundingly invalidate the Privacy Shield program, finding that electronic surveillance authorized by US national security law violated fundamental human rights under EU law.[4] More than a year since the judgment was announced, privacy professionals still face considerable uncertainty as to the future of transatlantic data transfers.[5] The long-term effects of this decision could profoundly shape geopolitics, international commerce, and the physical infrastructure of the Internet for years to come.

Schrems II raises an existential question about how global commerce can function in a data driven world where different economic and geopolitical powers have competing concepts of data privacy and human rights. The modern economy is data driven and interconnected,[6] and every government in the world grapples with the confluence of e-commerce, globalization, and the ongoing data processing revolution. One of the ways that legal institutions have adapted to this technological-economic transformation is by implementing data pro-

4. *See id.* ¶ 201.

5. Joseph Duball, *A Year After 'Schrems II' Ruling, Uncertainty Remains*, IAPP, https://iapp.org/news/a/uncertainty-aplenty-a-year-after-schrems-ii-ruling [https://perma.cc/C8AG-B68Q].

6. *See* Dan Ciuriak, *The Economics of Data: Implications for the Data-Driven Economy*, CIGI ONLINE (Mar. 5, 2018), https://www.cigionline.org/articles/economics-data-implications-data-driven-economy [https://perma.cc/TW5Y-REGC]; Bruce Kogut, *What Makes a Company Global?*, 77 HARV. BUS. REV. 1 (1999).

tection laws, often referred to as data privacy laws in American discourse.[7] Data protection laws regulate the collection, storage, use, and disclosure of personal data by public and private actors.[8]

The ever-expanding capabilities of data processing are a natural driving force behind data protection laws. An estimated 2.5 quintillion bytes of data are produced every day,[9] and it is now common for public and private actors to collect vast amounts of personal data, including one's name, street address, date of birth, social security number, banking information, browsing history, order history, IP address, biometric information, and sexual orientation.[10] This kind of information, if misused, can lead to identity theft, reputational damage, or systematic discrimination. That risk is heightened by replicability and portability of data. Data processing has become a massive global industry, with some experts estimating its size at $193 billion in the United States alone as of 2021.[11] That figure is just an estimate of monetized data processing. Data processing is a nebulous concept, which can be defined broadly as "[a]ny use of computers to perform defined operations on data."[12] Things as innocuous as entering payroll information

7. Privacy and data protection are separate but interrelated concepts that Americans occasionally conflate. *See* Meg L. Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 97–101 (2020). In short, privacy is a broad gateway right that is concerned with disclosure of information. *Id.* at 97. Data protection can encompass that concern about disclosure but also touches on "concerns about power, fairness, accuracy, security, and accountability when governments and companies hold large amounts of information about individuals." *Id.* at 98.

8. Collection, storage, use, and disclosure are a useful shorthand for the various stages in the lifecycle of data. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 325–26 (2016) (explaining that breaking down how data flows through an organization into these four stages helps conceptualize the different ways that data protection laws function).

9. Jacquelyn Bulao, *How Much Data Is Created Every Day in 2020?*, TECH JURY (Aug. 6, 2021), https://techjury.net/blog/how-much-data-is-created-every-day [https://perma.cc/7ZBJ-WWAZ].

10. *See* Indrajeet Deshpande, *What is Customer Data? Definition, Types of Collection, Validation and Analysis*, TOOLBOX MARKETING (May 26, 2020), https://www.toolbox.com/marketing/customer-data/articles/what-is-customer-data [https://perma.cc/6SKY-HJXM?type=image] (explaining the types of customer data that businesses can potentially collect and methods of collection); *The Importance of Data: The Top Benefits of Collecting Customer Data*, TRUYO, https://insights.truyo.com/consumer-data [https://perma.cc/4S8Z-NDGC] (explaining practical reasons for businesses to collect customer data, including improving market understanding, consumer databases, marketing strategies, and increasing personalization of services).

11. *Data Processing & Hosting Services in the US Market Size 2005–2027*, IBIS WORLD (Apr. 26, 2021), https://www.ibisworld.com/industry-statistics/market-size/data-processing-hosting-services-united-states [https://perma.cc/RA8T-RB49].

12. *Data Processing*, BRITANNICA, https://www.britannica.com/technology/data

into a company database could therefore qualify as data processing. In that sense, data protection regulations could have a far greater reach than many might expect.

Although competing legal structures across countries have always posed a threat to international business, this is a special problem in the context of data processing because of the nature of data[13] and how data protection laws are written.[14] The global leader in data protection is the European Union, who, in passing the General Data Protection Regulation (GDPR) in 2016, has created one of the strictest data protection regimes in the world.[15] The EU recognizes privacy and data protection as fundamental rights,[16] and the GDPR gives substance to those rights via 99 articles and 173 recitals which form a complex regulatory scheme.[17] Two of the most biting features of the GDPR are that it applies extraterritorially, i.e., to the processing of personal data concerning EU citizens wherever that processing takes place, and it places limits on transferring such personal data outside the EU.[18] An American company that wants to transfer personal data concerning EU citizens from the EU to servers in the United States therefore must ensure that data will receive an adequate level of protection in the United States which is "essentially equivalent" to that of

-processing [https://perma.cc/VL6D-RUK9]. Examples of data processing include "staff management and payroll administration," "posting/putting a photo of a person on a website," and "storing IP addresses or MAC addresses." *What Constitutes Data Processing?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [https://perma.cc/JSJ5-DEHG].

13. With data transfer speeds theoretically approaching two-thirds the speed of light, personal data stored on a server in one country can be on the other side of the world in the blink of an eye. *See* Fergal Toomey, *Data, the Speed of Light and You*, TECH CRUNCH (Nov. 8, 2015), https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you [https://perma.cc/GSY2-HMY3].

14. *See* Daniel Solove, *Beyond GDPR: The Challenge of Global Privacy Compliance—An Interview with Lothar Determann*, TEACHPRIVACY (Nov. 13, 2017), https://teachprivacy.com/challenge-of-global-privacy-compliance [https://perma.cc/8C88-PFNH] (discussing the challenges in international data privacy compliance).

15. Ben Waldorf, *What Is GDPR, the EU's New Data Protection Law?*, GDPR EU, https://gdpr.eu/what-is-gdpr [https://perma.cc/C79J-DWAB] (claiming that "[t]he General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world").

16. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 10 [hereinafter Charter] ("Everyone has the right to the protection of personal data concerning him or her.").

17. Council Regulation 2016/679, art. 1, General Data Protection Regulation, 2016 O.J. (L 119) 32.

18. Council Regulation 2016/679, arts. 44–50, General Data Protection Regulation, 2016 O.J. (L 119) 60–65 (placing limits on transfers of personal data to third countries or internal organizations).

EU law.[19] Failure to meet this standard can result in fines of €20 million or 4% of global revenue, whichever is more.[20]

To facilitate data transfers from the EU to the US, data processors and data controllers[21] operating in the United States have relied on one program, Privacy Shield, for many years.[22] Privacy Shield was jointly developed in 2016 by the US Department of Commerce and European Commission to fill the legal void following *Schrems I*.[23] Lacking comprehensive federal data protection regulation that is "essentially equivalent" to that under EU law,[24] Privacy Shield was a workaround by which US organizations voluntarily implemented safeguards and redressability mechanisms meant to mimic those required under EU law.[25] So long as they were compliant with Privacy Shield, participants could legally transfer personal data to the US. The program had its skeptics,[26] however, and the CJEU invalidated the program on July 16,

19. *Id*. at 61 ("A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country . . . ensures an adequate level of protection.").

20. Council Regulation 2016/679, art. 83, General Data Protection Regulation, 2016 O.J. (L 119) 82 (imposing fines "up to 20 000 000 EUR, or . . . up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher").

21. Data controllers are the entities who "determine[] the purposes and means of the processing of personal data." Council Regulation 2016/679 art. 4, General Data Protection Regulation, 2016 O.J. (L 119) 33. A data processor, in contrast, is the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.* These roles are not mutually exclusive. For example, a university that collects data on students would be a data controller, but it could also be a data processor if it is entering that information into a computer database and doing its own processing.

22. *Importance of Privacy Shield*, PRIVACY TRUST, https://www.privacytrust.com/privacyshield/importance-of-privacy-shield.html [https://perma.cc/494B-X5H8] ("In a time of increasing global data transfers it [is] important to have the ability to share data between the US and EU. This could be simply for processing or because a company has data centers located in the US only. Without Privacy Shield companies would find themselves transferring data illegally, and leave themselves open to lawsuits from data subjects.").

23. Ernst-Oliver Wilhelm, *A Brief History of Safe Harbor*, IAPP, https://iapp.org/resources/article/a-brief-history-of-safe-harbor [https://perma.cc/6SCM-99K9] ("With some delay, the EU Commission announced an agreement with the U.S. on a new framework for transatlantic data flows called 'EU-US Privacy Shield.'").

24. *See infra* Parts I.B, I.C.

25. *Privacy Shield Program Overview*, PRIVACY SHIELD, https://www.privacyshield.gov/Program-Overview [https://perma.cc/4NUM-7UP2] (noting that Privacy Shield was developed "to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.").

26. *See, e.g.*, Max Schrems, *The Privacy Shield Is a Soft Update of the Safe Harbor*, 2

2020,[27] a mere four years after it was first implemented. There was no grace period following the invalidation of the program,[28] so the immediate concerns in the decision's wake focused on how organizations should proceed in the short-term to avoid legal liability.[29] Now that time has passed, the most important question looms large: is a long-term successor program possible, and, if not, what does that mean for both the data processing industry and the global economy as a whole?

More than 5,300 US-based organizations relied on Privacy Shield to make necessary data transfers from the EU to the United States.[30]

EUR. DATA PROT. L. REV. 148, 148–49 (2016) (arguing that Privacy Shield was not sufficient to meet the obligations required by the CJEU).

27. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020). The US Department of Commerce is still requiring Privacy Shield participants to comply with their obligations under the program, regardless of whether the program serves any purpose under EU law. Press Release, U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020) [hereinafter Wilbur Ross Statement], https://2017-2021.commerce.gov/index.php/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.html [https://perma.cc/SK6Q-68UL] ("The Department of Commerce will continue to administer the Privacy Shield program . . . . Today's decision does not relieve participating organizations of their Privacy Shield obligations.").

28. Case C-311/18, ¶ 202 ("As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum . . . the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum."). For an overview of Article 49 derogations, see *infra* note 29 and accompanying text.

29. *See* Brian Hengesbaugh, *What Privacy Shield Organizations Should Do in the Wake of 'Schrems II'*, IAPP (July 17, 2020), https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii [https://perma.cc/STZ8-JB23] (providing guidance in the wake of *Schrems II* for Privacy Shield participants). Companies have largely avoided liability since the *Schrems II* judgment by relying on Standard Contractual Clauses (SCCs) and derogations. SCCs are an alternative transfer mechanism that was weakened but not outright invalidated in *Schrems II*. *See infra* Part II.B. Derogations are exceptions built into the GDPR that allow for transfers in the absence of an adequacy decision. They are meant to be used only in rare cases and are not reliable long term. They allow for transfers where (a) the data subject has explicitly consented, (b) the transfer is "necessary for the performance of a contract between the data subject and the controller," (c) the transfer is "necessary for the conclusion or performance of a contract concluded in the interest of the data subject," (d) the transfer is "necessary for important reasons of public interest," (e) the transfer is "necessary for establishment, exercise or defence of legal claims," (f) the transfer is "necessary in order to protect the vital interests of the data subject," or (g) the transfer is "made from a register which according to Union or Member State law is intended to provide information to the public." Council Regulation 2016/679, art. 49, General Data Protection Regulation, 2016 O.J. (L 119) 64.

30. Wilbur Ross Statement, *supra* note 27 ("As our economies continue their post-COVID-19 recovery, it is critical that companies—including the 5,300+ current Privacy Shield participants—be able to transfer data without interruption, consistent with the

As the dust settles and the full fallout of the CJEU's decision comes to light, those organizations face a veritable Scylla and Charybdis as they weigh three unenticing propositions. First, they can continue operating as they did before, risking significant legal liability, in the hope that the US and EU are able to work out a successor program before being subjected to an enforcement action by a data protection authority (DPA) in the EU.[31] Second, they can make their operations more regional by storing and processing data locally within the EU.[32] Or third, they can forgo their European operations altogether. The cost and general undesirability of each of these options makes clear that a successor program is necessary. Indeed, the US Department of Commerce and the European Commission are already discussing an "enhanced EU-U.S. Privacy Shield."[33]

This Note will examine the *Schrems II* judgment and demise of Privacy Shield as a symptom of the deeper, more-fundamental conflict between the US's national security electronic surveillance practices and the broad privacy rights enjoyed by EU citizens. Part I will contrast the comprehensive rights to privacy and data protection in the EU with the US's patchwork, sectoral approach to privacy, which has significant carve-outs for national security concerns. Part I will also explore the faults in the US's prior attempts at complying with EU data protection regulations via the Safe Harbor and Privacy Shield programs. Having framed how disjunct the EU and US approaches to privacy are to one another, Part II will analyze the *Schrems II* judgment to identify Privacy Shield's faults and how those problems apply to potential alternative transfer mechanisms such as Standard Contractual Clauses (SCCs)[34] or a future Privacy Shield replacement program. Finally, Part III will outline a possible legislative solution, termed the

---

strong protections offered by Privacy Shield.").

31. DPAs are independent public authorities that enforce data protection regulations in the EU. Each member state has its own DPA. *See* Eur. Comm'n, *What Are Data Protection Authorities (DPAs)?*, EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [https://perma.cc/5VCB-37EF]. *See also* MCGEVERAN, *supra* note 8, at 269–70.

32. This response is costly and generally undesirable. *See infra* Part II.C.

33. Press Release, U.S. Dep't of Com., Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders (Aug. 10, 2020) [hereinafter Joint Press Statement], https://2017-2021.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.html [https://perma.cc/R6SB-C7DA].

34. Standard Contractual Clauses (SCCs) are model contracts—adopted by the European Commission—that organizations can adopt in order to make data transfers in the absence of an adequacy decision. *See Standard Contractual Clauses (SCC)*, EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [https://perma.cc/

Privacy Shield Enabling Act ("PSEA"). The core features of the PSEA will be (1) narrowing the definition of potential surveillance targets, (2) expanding minimization procedures to cover European citizens, (3) implementing a maximum data retention period, (4) implementing a notice mechanism for data subjects to learn that their data has been acquired by the US government, (5) increasing the power of the Privacy Shield Ombudsperson[35] to order data disgorgement, and (6) creating a private right of action for aggrieved European citizens to challenge the US government's retention of their personal data. These features are meant to enable a Privacy Shield successor program to survive a challenge at the CJEU by rendering US national security access to personal data a proportional interference with fundamental rights under EU law. With a successor program in place, the EU and US economies would both benefit from increased certainty and trade.

I. A TALE OF TWO PRIVACY REGIMES: CONTRASTING COMPREHENSIVE EUROPEAN DATA PROTECTION WITH THE AMERICAN SECTORAL APPROACH

The narrow legal dispute between Max Schrems and Facebook Ireland is a byproduct of the vastly different approaches to privacy protection on either side of the Atlantic. *Schrems II* concerned whether Privacy Shield participants could guarantee data protection for Europeans essentially equivalent to that required under the GDPR in light of the US's significant national security electronic surveillance practices and absence of judicial protection for foreign citizens subject to surveillance. The broader issue, however, is that Privacy Shield would not be necessary if the United States recognized a broader right to privacy akin to that guaranteed in other countries. The mere fact the United States needs to construct these elaborate workarounds to enable American organizations to legally function in Europe undercuts the purposes of globalization and digital commerce. Understanding the *Schrems II* decision and the immediate utilitarian concerns surrounding replacing Privacy Shield thus requires understanding the deeper conflict of values motivating it. That conflict can be seen by

LQU9-BZN2]; *International Transfers*, ICO, http://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers [https://perma.cc/R9P8-HH29] ("You can make a restricted transfer if you and the receiver have entered into a contract incorporating standard data protection clauses adopted by the Commission."). It is unclear whether SCCs are a viable long-term option for US based organizations following *Schrems II*. *See infra* Part II.B.

35. An ombudsperson is "a government official . . . appointed to receive and investigate complaints made by individuals against abuses or capricious acts of public officials." *Ombudsman*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003).

contrasting the decades long development of a strong privacy right in the EU, culminating in the implementation of the GDPR, with the US's sectoral privacy laws, ill-fated attempts to comply with EU regulations, and the electronic surveillance authorized by US national security law. This Part first details the evolution of privacy and data protection in the EU, from its earliest days post-WWII to the implementation of the GDPR in 2018. Section B then details the US's ill-fated attempts to help organizations legally based in the US be compliant with EU regulations through the Safe Harbor and Privacy Shield programs. Finally, Section C provides a brief overview of the US surveillance practices at issue in *Schrems II*.

A. THE EUROPEAN RIGHTS TO PRIVACY AND DATA PROTECTION

Understanding why Privacy Shield was necessary in the first place, and hence why the United States needs a replacement program, requires understanding the incongruity between the United States' absence of significant data privacy protections and the robust data protection regulations employed in the European Union. The General Data Protection Regulation is the modern embodiment of this European regulatory scheme, and the focus of the *Schrems II* judgment, but it is also the product of over half a century of incremental privacy developments in Europe. Understanding that history is essential to understanding why GDPR compliance is so challenging for organizations in the United States who do not operate with that backdrop of a strong right of privacy.

1. The Decades-Long Development of Strong Privacy Rights in Post-War Europe

The evolution of data privacy rights in the EU is fairly logical in light of its history. In the aftermath of World War II, as Europe tried to piece together the shattered fragments of a continent that had just gone through the most devastating war in world history, Europeans cast an eye towards warding off the fascist ideology that marked the opening decades of the century.[36] One notable leap came in 1950, while European federalism was still in its nascent days, when the Council of Europe finished drafting the European Convention for the

36. Eur. Econ. & Soc. Comm., *Fascism on the Rise: Where Does It Come From, and How to Stop It, With a Common European Response*, EUROPA (Oct. 30, 2018), https://www.eesc.europa.eu/en/news-media/news/fascism-rise-where-does-it-come-and-how-stop-it-common-european-response [https://perma.cc/XK3F-FDPE] ("The very promise of the European Union, created from the ashes that resulted from the first attempt of fascism, is enshrined in Article 2 of the Treaty of Fundamental Rights . . . .").

Protection of Human Rights and Fundamental Freedom (ECHR).[37] The ECHR requires member nations to respect certain fundamental freedoms,[38] including the "[r]ight to respect for private and family life."[39] All members of the European Council have ratified the ECHR,[40] and this right of privacy serves as the cornerstone of the sprawling regulatory scheme now in place.

As the world evolved and technological change threatened individual privacy in new and unforeseen ways, governments and private actors recognized that safeguards for privacy rights needed to evolve as well.[41] Within the EU, this data protection revolution took many forms. In 1995, the European Parliament issued Directive 95/46,[42] which was the precursor to the GDPR (and was still in effect when the *Schrems II* lawsuit was commenced).[43] Directive 95/46 established limits on the processing of personal data of EU citizens, required European Economic Area (EEA) member states to implement supervisory authorities to ensure compliance, and placed limits on data processing in countries outside the EEA.[44] Directive 95/46 is important because it both shared many features with the GDPR[45] and the United States' inability to comply with Directive 95/46 directly precipitated the development of Privacy Shield.[46] In 2000, the EU increased privacy rights yet again with the introduction of the Charter of Fundamental

37. *See What Is the European Convention on Human Rights?*, AMNESTY (Aug. 21, 2018), https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights [https://perma.cc/8EKH-KJ4R].

38. *Id.*

39. *See* European Convention on Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

40. *A Convention to Protect Your Rights and Liberties*, COE, https://www.coe.int/en/web/human-rights-convention [https://perma.cc/5RX3-LXBC].

41. *See* Gene Markin, *What Is GDPR and Why You Should Care?*, N.J. L. BLOG (Aug. 28, 2018), https://www.njlawblog.com/2018/08/articles/business-corporate/what-is-gdpr-and-why-you-should-care [https://perma.cc/67GY-BFZL] (discussing the issuance of data protection recommendations in 1980).

42. Directive 95/46, Directive 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).

43. In *Schrems II*, the court framed its legal analysis around both Directive 95/46 and the GDPR because the litigation between Max Schrems and Facebook Ireland has been ongoing for so long that the original complaint was filed before the GDPR took effect in 2018.

44. *See* Directive 95/46, art. 28, 1995 O.J. (L 281) 47 (requiring Member States to establish public authorities to monitor compliance with the Directive); Directive 95/46, art. 3, 1995 O.J. (L 281) 39 (defining the scope of the Directive); Directive 95/46, art. 25, 1995 O.J. (L 281) 45–46 (limiting transfers of personal data outside the EU).

45. *See infra* Part I.B.2.

46. *See infra* Part I.B.

Rights of the European Union ("the Charter"), which guaranteed protection of personal data.[47] EU law must be read in light of the Charter, and the GDPR explicitly acknowledges that it is working to protect the rights identified in the Charter.[48]

In 2018, the GDPR formally supplanted Directive 95/46 and became the primary data protection regulation in Europe.[49] The EU touts the GDPR—which comprises 99 articles and 173 recitals[50]—as "the toughest privacy and security law in the world."[51] Like its predecessor, the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[52] These rules are extraordinarily broad in scope. Personal data is defined capaciously as "any information relating to an identified or identifiable natural person,"[53] and processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."[54] These definitions potentially cover a vast array of ordinary activities.

47. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 10 ("Everyone has the right to the protection of personal data concerning him or her.").

48. *See, e.g.*, Council Regulation 2016/679, General Data Protection Regulation, recitals 1, 4, 2016 O.J. (L 119) 32 ("The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her . . . . This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter . . . .").

49. *See generally* Waldorf, *supra* note 15; Samantha Beaumont, *The Data Protection Directive Versus the GDPR: Understanding Key Changes*, GRC WORLD FS. (Mar. 6, 2018), https://www.grcworldforums.com/gdpr/the-data-protection-directive-versus-the-gdpr/26.article [https://perma.cc/L5JV-SLYN].

50. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 32.

51. Waldorf, *supra* note 15.

52. Council Regulation 2016/679, General Data Protection Regulation, art. 1, 2016 O.J. (L 119) 32.

53. *Id.* at art. 4.

54. *Id.*

The rules imposed on data controllers are very broad as well, delineating a set of guiding principles rather than highly technical regulations: data processing must be lawful,[55] fair, and transparent;[56] personal data collection must be for a limited, explicit purpose;[57] personal data must be minimized;[58] personal data must be accurate and either erased or rectified when found to be inaccurate;[59] personal data must be stored in a way permitting identification for no longer than is necessary;[60] and personal data must be processed with appropriate security measures.[61] There are special rules for the processing of personal data related to children[62] or special categories of data (e.g., data revealing racial or ethnic origin, genetic data, etc.).[63] Additionally, data subjects have a number of substantive rights under the GDPR,[64] including the right to access personal data,[65] a right to rectify inaccurate personal data,[66] a right to erasure (the infamous "right to be forgotten" as it is widely known),[67] a right to data portability,[68] and a right to object to processing.[69] This list is not exhaustive, but it is illustrative of the way in which the GDPR gives substance to the broader fundamental rights to privacy and data protection. These rights are not rhetorical flourishes, but are serious principles vindicated in a rigorous regulatory regime.

---

55. *Id.* at art. 5. Lawful bases include "[when] the data subject has given consent . . . ; performance of a contract to which the data subject is party . . . ; compliance with a legal obligation to which the controller is subject; . . . protect[ing] the vital interests of the data subject or of another natural person; . . . performance of a task carrie[d] out in the public interest . . . ; [and when] processing is necessary for the purposes of the legitimate interests pursued by the controller . . . , except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject . . . ." *Id.* at art. 6.

56. *Id.* at art. 5.

57. *Id.*

58. Minimization is a shorthand for saying data must be "adequate, relevant and limited to what is necessary." *Id.*

59. *Id.*

60. *Id.*

61. This "integrity and confidentiality requirement" requires that processing ensures protection against "unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." *Id.*

62. *Id.* at art. 8.

63. *Id.* at art. 9.

64. *See generally id.* at arts. 12–23 (covering "rights of the data subject").

65. *Id.* at art. 15.

66. *Id.* at art. 16.

67. *Id.* at art. 17.

68. *Id.* at art. 20.

69. *Id.* at art. 21.

For data controllers and processors outside of the EU, there are two essential reasons why understanding the GDPR is crucial: it applies extraterritorially,[70] and violations of the basic principles articulated above carry administrative fines of either €20 million or 4% of annual global revenue, whichever is higher.[71] There are two separate, critical elements to the extraterritorial aspect of the GDPR. First, the regulation "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union . . . ."[72] Under that provision, any business operating in Europe is realistically subject to the GDPR because almost all business operations require processing of personal data in some form.

The second extraterritorial aspect of the GDPR is the limitation on cross border data transfers, which was the impetus behind Privacy Shield.[73] Data is inherently mobile, so a transfer restriction is necessary to prevent data controllers from avoiding GDPR compliance by transferring data to a country that does not impose GDPR-like protections and then processing that data. To effectuate this limit, the GDPR requires that "[a]ny transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if . . . the conditions laid down in this Chapter are complied with by the controller and processor . . . ."[74] A "third country" is any country outside

70. *Id.* at arts. 3, 44–50.

71. *Id.* at art. 83. For a large multinational corporation with annual revenue in the billions, these fines can be shockingly large. For example, in 2021, Luxembourg's data protection commission imposed an eye-watering $888 million fine on Amazon.com for data processing violations of the GDPR. Stephanie Bodoni, *Amazon Gets Record $888 Million EU Fine over Data Violations*, BLOOMBERG (July 30, 2021), https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach [https://perma.cc/VRG4-E79Z]; *see also 5 Biggest GDPR Fines So Far [2020 & 2021]*, DATA PRIVACY MANAGER (Aug. 9, 2021), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020 [https://perma.cc/H9C3-NXS4] (noting Google's €50,000,000 fine in 2019).

72. Council Regulation 2016/679, General Data Protection Regulation, art. 3, 2016 O.J. (L 119) 32.

73. Notice of Availability of Privacy Shield Framework Documents, 81 Fed. Reg. 51,041, 51,042 (Aug. 2, 2016) ("The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with European Union data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.").

74. Council Regulation 2016/679, General Data Protection Regulation, art. 44, 2016 O.J. (L 119) 32.

of the EU,[75] so this provision regulates data transfers to a considerable portion of the world.

To be GDPR compliant and engage in cross-border transfers, a third country or international organization must first obtain an adequacy decision from the European Commission.[76] An adequacy determination is an ex-ante determination by the Commission that the third country in question ensures "an adequate level of protection essentially equivalent to that ensured within the Union . . . ."[77] So long as an adequacy decision is in place, personal data can flow freely from the EU to the third country in question. Article 45 of the GDPR lays out the formal requirements for an adequacy decision,[78] which include, in short, that "the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order . . . ."[79] There is no definition of adequacy beyond this imprecise standard.[80] The adequacy decision requirement is important because the United States, being outside the EU, is an aforementioned "third country." Therefore, for any transfer of personal data to the US to take place, there must be a showing of an adequate level of protection equivalent to that under the GDPR. In order to do this, the United States and the European commission developed Privacy Shield.

Europe's half century development of robust rights of privacy make sense considering the political history of the continent, and they provide the backdrop for the GDPR's vast regulatory scheme. The

---

75. *Transfer of Data to a Third Country*, IMY (Swed.), https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/transfer-of-data-to-a-third-country [https://perma.cc/K4RE-KTZV].

76. *See generally* Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.

77. Council Regulation 2016/679, General Data Protection Regulation, recital 104, 2016 O.J. (L 119) 20.

78. *Id.* at art. 45.

79. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 162 (July 16, 2020).

80. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 70 (Oct. 6, 2015) ("It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment."). This statement by the court notes that adequacy is not defined under the Directive, as opposed to the GDPR. Notwithstanding that distinction, the GDPR retained the Directive's concept of adequacy and likewise failed to make the concept more definite.

GDPR's extraterritorial effect is exemplary of this, demonstrating the EU's unwillingness to trade in on its fundamental rights in exchange for its role in the global marketplace. This strong affirmation of the right to privacy is a stark contrast to the United States, which has taken a decidedly different approach to privacy rights.

B. THE UNITED STATES' ROLE IN EUROPEAN DATA PRIVACY REGULATION

The United States is an aforementioned "third country" under the European regulatory framework, which means that data transfers from the EU to the United States cannot occur unless they comport with the requirements laid out in chapter five of the GDPR. In its most succinct formulation, compliance with those articles requires showing that, after the transfer takes place, that data will receive the same level of protection as required by the GDPR. Compliance therefore raises a difficult problem for US data processors: United States law simply does not guarantee anything close to adequate protections under the GDPR. Although US courts have long recognized a constitutional right to privacy,[81] the United States lacks a comprehensive data protection scheme akin to the GDPR.[82] There are a growing number of privacy laws in the United States,[83] but these are often piecemeal, sectoral laws that are directed to a specific industry or type of data, such as health or biometric data.[84] Without a comprehensive data protection regulation, the United States cannot get an adequacy determination.[85]

Companies therefore need some other mechanism to legally conduct these transfers. One option is SCCs,[86] which many organizations already rely on. SCCs can be difficult to implement because they require integrating their exact language into contracts, which is not an

81. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (recognizing a "zone of privacy created by several fundamental constitutional guarantees") (internal quotations omitted).

82. *But see* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (West) (providing Californians with substantive privacy rights, such as opting out of having their data sold).

83. *E.g.*, ME. REV. STAT. ANN. tit. 35-A, § 9301 (West 2019) ("[P]rohibit[ing] a provider of broadband Internet access service from using, disclosing, selling or permitting access to customer personal information unless the customer expressly consents to that use, disclosure, sale or access."); 740 ILL. COMP. STAT. 14/1 (2008) ("regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.").

84. Some of the most comprehensive examples include the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, and the Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996).

85. The US has never applied for an adequacy decision because it would almost certainly not get one. MCGEVERAN, *supra* note 8, at 270.

86. Joint Press Statement, *supra* note 33 and accompanying text.

easy task.[87] Furthermore, the *Schrems II* decision left SCCs on precarious footing.[88] For that reason, this Note focuses on the second option: enabling the US to pass a new program that provides GDPR equivalent protections in the absence of a broad US data protection law. Privacy Shield was meant to achieve this, but ultimately failed to meet GDPR standards in the eyes of the CJEU. To understand why Privacy Shield was ultimately insufficient requires looking at both its history and features.

1. The Impetus Behind Privacy Shield: *Schrems I* Sank the Safe Harbor Privacy Principles

The need to craft a viable long-term program to facilitate EU to US data transfers is not a new problem. Long before the CJEU's July 16, 2020 decision invalidating Privacy Shield's adequacy determination, Max Schrems, an Austrian privacy advocate,[89] claimed his first victim in his long-running legal dispute with Facebook Ireland: the Safe Harbor Privacy Principles ("Safe Harbor").[90] Safe Harbor was the direct predecessor to Privacy Shield, and its demise was a catalyst for Privacy Shield's development.[91] The faults in Safe Harbor, and the ways in which Privacy Shield did or did not remedy them, are instructive in trying to craft a successor program now that Privacy Shield has joined Safe Harbor in the graveyard of failed privacy programs.

Safe Harbor began development in the late 1990s as the EU and US recognized that some legal mechanism was necessary to keep data transfers flowing in light of the EU's adoption of Directive 95/46 in 1995.[92] The US Department of Commerce proposed the Safe Harbor

87. *See* MCGEVERAN, *supra* note 8, at 505 ("In order to comply, the clauses must be used verbatim, which can lead to inflexibility and somewhat awkward drafting at times.").

88. *See infra* Part II.B.

89. *See generally Max Schrems*, IAPP, https://iapp.org/resources/article/max-schrems [https://perma.cc/VYN3-ZQ2H].

90. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 98 (Oct. 6, 2015) (finding that the Commission's adequacy determination for Safe Harbor, Decision 2000/520, was invalid).

91. *See Update on the U.S.-EU Safe Harbor Framework*, FTC (July 25, 2016) https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework [https://perma.cc/HQA3-WH9U] (noting that Privacy Shield was adopted following Safe Harbor's demise at the hands of the CJEU in 2015).

92. Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455 (2001) ("In October 1998, the United States Department of Commerce and the European Union Commission began discussing how to create uniform standards of data protection while maintaining the free flow of personal data between the European Union and the United States . . . . The United States submitted several safe harbor proposals, predicated on industry self-regulation,

program, and the European Commission granted the program an adequacy decision on July 26, 2000.[93] Safe Harbor was in effect for a remarkable fifteen years before it was invalidated.[94] The key principles of Safe Harbor were "notice, choice, onward transfer, security, data integrity, access, and enforcement."[95] Each of these principles imposed a set of obligations on a participant that were akin to those under Directive 95/46.[96] For example, the notice requirement involved posting a statement "detailing the means and purposes of information collection from individuals" and "the choices and means the organization offers individuals for limiting its use and disclosure."[97] For many years, Safe Harbor principles was deemed adequate under EU law.[98]

In 2015, the CJEU reversed course and invalidated the Commission's adequacy determination in a decision now known as *Schrems I*.[99] Although *Schrems I* concerned Directive 95/46, rather than the GDPR, the two laws are substantially similar[100] and Safe Harbor's deficiencies can still be informative in crafting a replacement for Privacy Shield. The major fault with Safe Harbor was that it was "applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities [were] not required to comply with them,"[101] meaning that, "where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law."[102] Thus, "national security, public interest, or law enforcement requirements ha[d] primacy over the safe harbour principles."[103] This created an interference with the "fundamental right to respect for private life" that the

to the European Union.").

93. Commission Decision 2000/520, art. 1, 2000 O.J. (L 215) 8 ("[T]he 'Safe Harbor Privacy Principles' . . . ensure an adequate level of protection for personal data transferred from the [c]ommunity to organisations established in the United States.").

94. *See generally* Ernst-Oliver Wilhelm, *A Brief History of Safe Harbor*, IAPP, https://iapp.org/resources/article/a-brief-history-of-safe-harbor [https://perma.cc/6SCM-99K9].

95. Shimanek, *supra* note 92, at 473.

96. *See id.* at 472–76 (providing an overview of the Safe Harbor requirements).

97. *Id.* at 473–74.

98. *Id.*

99. *See Update on the U.S.-EU Safe Harbor Framework*, *supra* note 91.

100. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶¶ 3–25 (Oct. 6, 2015) (identifying the legal context of the judgment as Directive 95/46/EC, Decision 2000/520, Communication COM(2013) 846 final, and Communication COM(2013) 847 final).

101. *Id.* ¶ 82.

102. *Id.* ¶ 85.

103. *Id.* ¶ 86 (internal quotations omitted).

EU protects zealously.[104] There were three additional problems that ultimately condemned Safe Harbor: (1) there were not sufficient rules limiting interferences by the United States in the pursuit of legitimate State interests, such as national security;[105] (2) there was a lack of effective judicial remedies for such interferences;[106] and (3) the amount of access that the United States had to personal data was not proportional to the national security interests at stake.[107] Consequently, Safe Harbor was invalid and a successor program was necessary. Enter: Privacy Shield.

2. The Features of Privacy Shield

In the wake of *Schrems I*, the United States needed to rapidly develop a successor program to protect US based data processors.[108] The result was the Privacy Shield program,[109] which was considered by some to be merely a panacea rather than a long-lasting solution.[110] Notwithstanding the criticism it received as being only a partial solution, Privacy Shield contained a number of improvements over its predecessor: the right for data subjects to access their data, the imposition of specific obligations on organizations transferring data onward to a controller or service provider, a data minimization requirement, provision of a free, independent, recourse mechanism that could provide damages to data subjects, etc.[111] The European Commission

104. *Id.* ¶ 87.

105. *Id.* ¶¶ 88, 91 (Identifying that the US lacks any such limits on interference, and then reiterating that under EU law, "legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must . . . lay down clear and precise rules governing the scope and application of a measure and impos[e] minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.").

106. *Id.* ¶ 89 (noting that FTC adjudication is limited to commercial disputes, and private causes of action could only be brought against the organization for failing to adhere to Safe Harbor, not against the United States for interfering with that citizen's privacy rights).

107. *Id.* ¶ 90. This point, although subjective and somewhat nebulous, is of particular importance in the *Schrems II* judgment, which emphasizes the disproportionate scope of the mass surveillance programs whose existence has been disclosed in recent years. *See infra* Part II.A.

108. *See Update on the U.S.-EU Safe Harbor Framework*, *supra* note 91.

109. *Id.*

110. *See, e.g.*, Schrems, *supra* note 26, at 148–49 (claiming that Privacy Shield is a "soft update of Safe Harbor, which does not address any of the material issues identified by the court[,] [and] . . . this proposed system is unfortunately not just questionable, but an outright affront to the highest court of the European Union.").

111. *See generally* Bryan Cave LLP, *A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor"*, IAPP (July 17, 2016), https://iapp.org/media/pdf/

quickly granted Privacy Shield an adequacy decision.[112] Importantly, Privacy Shield was drafted and implemented before the GDPR went into effect, so it was technically designed to be compliant with Directive 95/46. Nevertheless, the two laws are similar in most regards,[113] and the European Commission maintained the power to suspend the adequacy decision following the implementation of the GDPR if it found that Privacy Shield no longer met its adequacy requirements.[114]

Like Safe Harbor before it, Privacy Shield required organizations to self-certify.[115] Once an organization registered, its core requirements broadly included: "[i]nforming individuals about data processing";[116] "[p]roviding free and accessible dispute resolution";[117] "[c]ooperating with the Department of Commerce";[118] "[m]aintaining

resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf [https://perma.cc/Q472-TGTG].

112. Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1. The European Commission worked with the US to develop Privacy Shield, recognizing that facilitating data transfers was in the best interest of both parties. *See Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield*, EUROPA (Feb. 29, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_433 [https://perma.cc/XC7K-DUFL] (sharing supportive statements from members of the European Commission following release of their draft Privacy Shield adequacy decision).

113. *Supra* Part I.A.

114. Commission Implementing Decision 2016/1250, n. 207, 2016 O.J. (L 207).

115. *See Welcome to Privacy Shield*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/PrivacyShield/ApplyNow [https://perma.cc/6N2X-3H2G] (allowing interested parties to create an account with the International Trade Administration if they wish to register for Privacy Shield).

116. *EU-U.S. Privacy Shield Framework Key New Requirements for Participating Companies*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Key-New-Requirements [https://perma.cc/FJF5-CJCY]. The informing requirements include noting Privacy Shield participation in a privacy policy, linking to the Department of Commerce's privacy shield website in that privacy policy, and informing individuals of "their rights to access their personal data, the requirement to disclose personal information in response to lawful request by public authorities, which enforcement authority has jurisdiction over the organization's compliance with the Framework, and the organization's liability in cases of onward transfer of data to third parties." *Id.*

117. *Id.* These requirements include allowing an individual to bring a complaint directly to a Privacy Shield participant and get a response within forty-five days, providing "an independent recourse mechanism by which each individual's complaints and disputes can be investigated and expeditiously resolved" at no cost to the complainant, having the Deptartment of Commerce "receive, review and undertake best efforts to facilitate resolution of the complaint" and respond all within ninety days if an individual submits a complaint to a data protection authority in the EU. *Id.*

118. *Id.* The cooperation requirement includes "respond[ing] promptly to inquiries and requests by the Department of Commerce." *Id.*

data integrity and purpose limitation";[119] "[e]nsuring accountability for data transferred to third parties";[120] "[t]ransparency related to enforcement actions";[121] and "[e]nsuring commitments are kept as long as data is held."[122] These requirements are highly technical and track the requirements imposed by the GDPR. However, none of these principles outright addressed the crux of the Safe Harbor's shortcomings: electronic surveillance authorized by law. Instead, the US attempted to remedy this issue through the introduction of the Privacy Shield Ombudsperson.[123]

The Privacy Shield Ombudsperson was a novel role introduced to address concerns about national security access to data transmitted from the EU to the United States.[124] The premise is that EU citizens who are concerned that their data may be accessed by the US for national security purposes can submit a complaint, which the Privacy Shield Ombudsperson will resolve. This complicated process requires that: (1) an EU citizen submit a complaint to the relevant supervisory authority in their country;[125] (2) the supervisory authority transmit that request to the Ombudsperson after determining that the request is complete and not "frivolous, vexatious, or made in bad faith";[126] (3) the Ombudsperson conduct an initial review, ensuring the request is complete and reaching out to the referring supervisory authority if more information is needed;[127] and (4) the Ombudsperson communicate to the referring supervisory authority that "the complaint has been properly investigated" and either no violation of US law, statutes,

119. *Id.* The maintaining data integrity and purpose requirements include "limit[ing] personal information to the information relevant for the purposes of processing . . . [and] comply[ing] with the new data retention principle." *Id.*

120. *Id.* In order to ensure third party accountability, Privacy Shield participants are required to include particular limitations in their contracts with third parties, such as limiting the purposes for which that third party can process data and requiring the third party to provide notice if it can no longer meet those expectations.

121. *Id.* This principle requires that participants "make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if the organization becomes subject to an FTC or court order based on non-compliance." *Id.*

122. *Id.* This requirement means that organizations must continue to provide the same level of protection to data received while participating in the program after the organization leaves the program if it chooses to retain that data.

123. Notice of Availability of Privacy Shield Framework Documents, 81 Fed. Reg. 51,041, 51,056–58 (Aug. 2, 2016) (explaining the introduction of the Privacy Shield Ombudsperson mechanism).

124. *Id.* at 51,056.

125. *Id.* at 51,057.

126. *Id.* This does not require that an EU citizen demonstrate that their data had actually been accessed by the US government.

127. *Id.*

executive orders, presidential directives, or agency policies has occurred, or such a violation had been remedied.[128]

The Privacy Shield Ombudsperson's unique role within the executive branch and limited powers rendered it an oblique solution. In resolving a complaint, the Ombudsperson will neither confirm nor deny whether the individual who brought the complaint was in fact the subject of surveillance.[129] This leaves data subjects in the dark as to whether their rights have been violated, which is squarely at odds with the GDPRs principles of transparency and notice.[130] Further, the Ombudsperson does not have the power to order a US governmental body to remedy a specific violation. Instead, where a complaint alleges a violation of the law or similar misconduct, the Ombudsperson merely refers the allegation "to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance . . . ."[131] This suggests that the Ombudsperson's role in restraining unlawful access to personal data is more illusory than anything. Finally, the Privacy Shield Ombudsperson reports directly to the Secretary of State[132] and the Under Secretary of State for Economic Growth, Energy, and the Environment currently serves as the Privacy Shield Ombudsperson.[133] This subservience to the State Department diminishes confidence in the position's impartiality, thus undermining the claim that the Ombudsperson mechanism is truly a check on national security surveillance.

Overall, the strengthened principles of Privacy Shield and introduction of the Privacy Shield Ombudsperson were nontrivial improvements over the Safe Harbor program. However, Privacy Shield was subject to exacting scrutiny from its inception, and the program's faults were readily on display. Most notably, Privacy Shield did not—

128. *Id.*

129. *Id.* ("The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied.").

130. *Compare* Notice of Availability of Privacy Shield Framework Documents, 81 Fed. Reg. 51,041, 51,057 (Aug. 2, 2016) ("The Privacy Shield Ombudsperson will . . . [not] confirm the specific remedy that was applied."), *with* Council Regulation 2016/679, art. 12, General Data Protection Regulation, 2016 O.J. (L 119) 40 ("The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request.").

131. Notice of Availability of Privacy Shield Framework Documents, 81 Fed. Reg. 51,041, 51,058 (Aug. 2, 2016).

132. *Id.* at 51,057.

133. *Privacy Shield Ombudsperson*, U.S. DEP'T OF STATE, https://www.state.gov/privacy-shield-ombudsperson [https://perma.cc/FJL6-MHSC].

and could not—directly address the specific problem that doomed Safe Harbor in *Schrems I*: US electronic surveillance.

C. THE US SURVEILLANCE STATE: FISA SECTION 702 AND EXECUTIVE ORDER 12,333

Finally, a brief overview of key elements of the United States' surveillance state is necessary to properly frame the challenge of creating an adequacy mechanism in light of underlying US law. The *Schrems II* opinion singled out Section 702 of FISA and Executive Order 12,333 ("EO 12,333" or "the Order") as being fundamentally incompatible with EU law.[134] These two legal regimes work in tandem, with EO 12,333 applying before that data arrives and FISA applying to surveillance of foreign citizens after their data arrives in the United States.[135]

EO 12,333 was originally passed on December 4th, 1981[136] and was amended in 2008.[137] EO 12,333 is meant for gathering intelligence, with the goal of "provid[ing] . . . [the Executive] with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats."[138] EO 12,333 accomplishes this by authorizing broad surveillance of foreign citizens.[139] The Order sets out a number of guiding principles to achieve this end,[140] but the National Security Agency's ability to access data transmitted via underwater cables in the Atlantic one particular practice has been singled out as highly detrimental to Privacy Shield.[141] This practice is troublesome because of the scale of

134. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 60 (July 16, 2020).

135. *See id.* ¶ 63 ("The referring court found that E.O. 12333 allows the NSA to access data 'in transit' to the United States . . . and to collect and retain such data before arriving in the United States and being subject there to the FISA.").

136. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

137. Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

138. *Id.*

139. *Executive Order 12,333*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/surveillance/12333 [https://perma.cc/W3DX-PP7X] ("This provision appears to have opened the door for the NSA's broad and unwarranted surveillance of U.S. and foreign citizens.").

140. *See* Exec. Order No. 13,470, 73 Fed. Reg. 45,325, 45,325–37 (July 30, 2008) (discussing changes to the "Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts" of the Order).

141. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 63 (July 16, 2020); *see* Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, ATLANTIC (July 16, 2013), https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855 [https://perma.cc/XY34-HTTS]; Amos Toh, Faiza Patel & Elizabeth Goitein,

the data collection[142] and its lack of targeting.[143] Unlike traditional surveillance measures, such as using a pen register to track numbers called from a particular phone line, tapping a cross-continental data line captures a massive volume of data.[144] Another notable challenge with EO 12,333 is the difficulty in establishing standing if an aggrieved party wants to challenge the interception of their data.[145] The GDPR requires that data subjects have actionable rights against authorities interfering with the right to data protection, so this is a sizable barrier.[146]

The other relevant surveillance practice comes from the Foreign Intelligence Surveillance Act of 1978 (FISA), which "authorize[s] electronic surveillance to obtain foreign intelligence information."[147] FISA has undergone numerous revisions that have expanded its scope dramatically over the years.[148] One important addition is Section 702, added in the 2008 amendments.[149] Under Section 702, the Attorney General and Director of National Intelligence are permitted to conduct "targeted surveillance of foreign persons located outside the United States[] *with the compelled assistance of electronic communication ser-*

Overseas Surveillance in an Interconnected World, BRENNAN CTR. 17 (2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf [https://perma.cc/WWW6-W4UZ] (providing a pithy overview of what happens when an NSA analyst accesses data through an undersea cable).

142. Khazan, *supra* note 141 ("The scale of the resulting data harvest is tremendous.").

143. *See* TOH ET AL., *supra* note 141, at 18–19 (describing the differences between "bulk" and "targeted" data collection).

144. Khazan, *supra* note 141 ("A subsidiary program for these operations—Tempora—sucks up around 21 million gigabytes per day and stores the data for a month.").

145. Charlotte J. Wen, *Secrecy, Standing, and Executive Order 12,333*, 89 S. CAL. L. REV. 1099, 1111–24 (2016) (analyzing the difficulty in establishing standing to challenge post 9/11 surveillance programs).

146. Council Regulation 2016/679, art. 1, General Data Protection Regulation, 2016 O.J. (L 119) 68.

147. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 (current version at 50 U.S.C. § 1801).

148. *The Foreign Intelligence Surveillance Act – News and Resources*, ACLU, https://www.aclu.org/other/foreign-intelligence-surveillance-act-news-and-resources [https://perma.cc/8JXW-LR64] (affirming the ACLU's opposition to "the expansion of FISA"); *Foreign Intelligence Surveillance Act (FISA)*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/surveillance/fisa [https://perma.cc/RBY7-DL39] ("FISA was initially limited to electronic eavesdropping and wiretapping. In 1994 it was amended to permit covert physical entries in connection with 'security' investigations, and in 1998, it was amended to permit pen/trap orders.").

149. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, § 702, 122 Stat. 2,436, 2,438–48 (2008) (codified at 50 U.S.C. § 1881a).

vice providers" following approval of the Foreign Intelligence Surveillance Court (FISC).[150] This compelled disclosure is important in light of the CJEU's concerns in *Schrems I* that the self-certification programs relied upon by the US do not excuse participants from obligations under domestic law.[151] Therefore, electronic communications service providers have to turn over requested data if the US government requests it, even if that would otherwise violate their obligations under Privacy Shield. There have been attempts to slow or even scale back this expansion,[152] but for now Section 702 remains a fertile source of mass surveillance.

These practices have come under increasing scrutiny in recent years. Recognizing that public backlash both domestically and abroad, in 2014 the Obama administration released Presidential Policy Directive 28 (PPD-28).[153] This policy directive was meant to ease US allies' apprehensions concerning the scope of signals intelligence[154] practices by refining "why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes."[155] These self-imposed limits are broad and arguably nugatory, but several are relevant to the concerns raised by the CJEU. First, PPD-28 implemented a set of guiding principles, which limit signals intelligence collection by requiring au-

150. Off. of the Dir. Nat'l Intel., *Section 702 Overview*, DNI, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [https://perma.cc/7ACM-QF79] (emphasis added); *see* 50 U.S.C. § 1881 (defining "electronic communication service provider").

151. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 85 (Oct. 6, 2015) (flagging the recognition in the adequacy decision that "[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law.") (internal quotations omitted).

152. Press Release, White House, Off. of the Press Sec., Presidential Policy Directive—Signals Intelligence Activities, OBAMA WHITE HOUSE (Jan. 17, 2014) [hereinafter Obama Statement], https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/3585-TUS4] ("[A]rticulat[ing] principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes.").

153. *Id.*

154. Signals intelligence (SIGINT) is "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions." *Signals Intelligence*, NSA, https://www.nsa.gov/what-we-do/signals-intelligence [https://perma.cc/9DV4-BXFP]. This type of electronic espionage, when conducted without sufficient transparency and safeguards, is counterthetical to EU law. *See infra* Part I.A.1, discussing the *Schrems I* judgment.

155. Obama Statement, *supra* note 152.

thorization, considering privacy and civil liberties in planning intelligence activities, forbidding collection of "foreign private commercial information or trade secrets" except where necessary for national security protection of the US and allies, and tailoring activities by pursuing alternatives to signals intelligence where possible.[156] Second, PPD-28 limits the use of signals intelligence collected in bulk to detecting and countering six different kinds of national security threats, such as espionage by foreign powers, terrorism, etc.[157] Third, PPD-28 refined the process for collecting signals intelligence by requiring that the heads of departments and agencies involved in signals intelligence to "review [annually] any priorities or requirements identified by their departments or agencies . . . ."[158] Finally, PPD-28 implemented a number of safeguards such as broader minimization procedures and the invention of a Privacy and Civil Liberties Policy Official and a Coordinator for International Diplomacy.[159]

It is unclear how effective PPD-28 is in reigning in electronic surveillance. Its existence was important in the European Commission's decision to grant Privacy Shield an adequacy decision,[160] and its proponents have extolled its economic value in preserving cross-border data flows.[161] Others have been critical of PPD-28, going so far as to call its limitations on signals intelligence practices a harmful overreaction.[162] Despite calls to "amend Section 702 to enshrine the PPD-28

156. *Id.* at Sec. 1(a)–(d).

157. *Id.* at Sec. 2.

158. *Id.* at Sec. 3.

159. *Id.* at Sec. 4. Section 4(d) creates the role of "Coordinator for International Diplomacy." This role became the Privacy Shield Ombudsperson once the Privacy Shield framework went into effect. Notice of Availability of Privacy Shield Framework Documents, 81 Fed. Reg. 51,041, 51,057 (Aug. 2, 2016).

160. Commission Implementing Decision 2016/1250, recital 76, 2016 O.J. (L 207) 16. ("Although not phrased in those legal terms, these principles [in PPD-28] capture the essence of the principles of necessity and proportionality.").

161. *See* Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE BLOG (Jan. 17, 2017), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/3MVZ-7JF4] (arguing that then-President Trump should not revoke PPD-28 in light of its importance to the Privacy Shield program and the bipartisan support the directive enjoys).

162. Eric Manpearl & Steve Slick, *Revisiting Legacy Restrictions on the Intelligence Community's Handling of SIGINT Data on Non-Americans*, LAWFARE BLOG (Oct. 17, 2019), https://www.lawfareblog.com/revisiting-legacy-restrictions-intelligence-communitys-handling-sigint-data-non-americans [https://perma.cc/XT7Y-SAMS] (arguing that "President Obama's embrace of a universal right to privacy and decision to restrict the dissemination and retention of personal information lawfully collected by the intelligence community was an exaggerated response to a mostly cynical complaint by our European allies following the Snowden disclosures."); *see also* Eric

protections,"[163] PPD-28 remains a mere policy directive with arguable efficacy.[164]

Foreign intelligence surveillance and national security are complex issues marked by secrecy, blurred partisan lines, and unsettled constitutional questions. Considering the scope of surveillance and absence of safeguards detailed above, EO 12,333 and Section 702 of FISA present a significant problem for data protection efforts in the US. Private entities can take on data protection obligations through the freedom of contract, but they can never contract away their obligation to comply with US law. Privacy Shield was born out of necessity in the wake of *Schrems I*, but it never resolved that underlying problem. That reticence to reform electronic surveillance practices meant that Privacy Shield was fated to a short life.

II. S*CHREMS II*, THE DEATH OF PRIVACY SHIELD, AND THE LOOMING THREAT OF INTERNET BALKANIZATION

Data is the lifeblood of the modern economy, and Privacy Shield was an important facet in $7.1 trillion economic relationship between the US and EU.[165] In the years following Privacy Shield's inception, over 5,300 organizations came to rely on the program to conduct transatlantic data transfers.[166] Privacy Shield afforded legal certainty to organizations hoping to do business in Europe—something incredibly important when a single GDPR violation costs upwards of €10 million.[167] Despite the program's clear value, there were concerns from its inception that the program was destined for the same fate as Safe Harbor.[168] Those concerns proved prescient. On July 16, 2020, the

---

Manpearl, *The Privacy Rights of Non-U.S. Persons in Signals Intelligence*, 29 FLA. J. INT'L L. 303, 355–60 (2017) (noting the potential national costs incidental to PPD-28's implementation).

163. Catherine Read, Note, *The EU-U.S. Privacy Shield: An Uncertain Future*, 3 INT'L COMPAR., POL'Y & ETHICS L. REV. 279, 283 (2019).

164. *See infra* Part II.A (discussing why PPD-28 was not substantive enough to save Privacy Shield).

165. Off. Pub. Affs., *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*, U.S. DEP'T OF COMM. (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 [https://perma.cc/SK6Q-68UL].

166. *Id.*

167. Council Regulation 2016/679, art. 83, General Data Protection Regulation, 2016 O.J. (L 119) 82.

168. Emily Linn, Note, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement*, 50 VAND. J. TRANSNAT'L L. 1311, 1346–48 (2017).

CJEU released its judgment in the *Schrems II* case, invalidating the Privacy Shield program and placing SCCs[169] on precarious footing.

Privacy Shield may be dead, but *Schrems II* provides a roadmap for what a successor program needs to avoid a similar untimely demise. Section A of this Part will analyze the *Schrems II* judgment to identify Privacy Shield's faults and build a roadmap for the potential legislative action in Part III. Section B will explore the other major aspect of *Schrems II*—the enervation of SCCs, which were the most accessible alternative to Privacy Shield participation. Lingering doubt about whether SCCs will be a viable long-term option for cross border data transfers further highlights the need for legislative action. Finally, Section C explores the practical fallout on cross-border data transfers if this issue is not solved.

A. PRIVACY SHIELD POST-MORTEM: FISA SECTION 702, EXECUTIVE ORDER 12,333, AND THE FUNDAMENTAL INCOMPATIBILITY OF EU AND US LAW

The *Schrems II* judgment is long and highly technical, frequently mired in the minutiae of EU law. The portion of the judgment most relevant to this Note is ¶¶ 150–202, in which the court considers the substantive question of whether the European Commission validly granted Privacy Shield an adequacy determination, which is to ask whether Privacy Shield actually guaranteed a level of protection essentially equivalent to that of EU law.[170]

To sustain its adequacy determination, the CJEU needed to find that Privacy Shield "complies with the requirements stemming from the GDPR read in the light of the Charter."[171] This meant that "pursuant to Article 45(3) of the GDPR, [the Commission] must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order . . . ."[172] The European Commission, by granting Privacy Shield an adequacy decision, felt that the program met this bar.[173] However, US surveillance practices did not change in

169. SCCs are model clauses, drafted by the European Commission and granted an adequacy determination, which serve as a transfer mechanism. They are highly technical and have to be inserted into contracts verbatim, which can be challenging. *See* ICO, *supra* note 34; *see also* MCGEVERAN, *supra* note 8, at 505 (discussing the inflexibility of model clauses as a transfer mechanism).

170. *See* Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1.

171. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 161 (July 16, 2020).

172. *Id.* ¶ 162.

173. Commission Implementing Decision 2016/1250, recital 13, 2016 O.J. (L 207) 3 ("[T]he Commission concludes that the United States ensures an adequate level of

the intervening years since *Schrems I*. US intelligence agencies could still obtain personal data of EU citizens in a way that violated their rights under EU law.[174] For that reason, Privacy Shield suffered from the same two fatal flaws that Safe Harbor did: allowing disproportionate interference with fundamental rights and lack of judicial protection.

Like Safe Harbor before it, Privacy Shield did not relieve organizations of their obligations under US law.[175] Privacy Shield allowed for "interference, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."[176] As discussed above, US public authorities access personal data through surveillance programs such as PRISM[177] and UPSTREAM,[178] which are authorized under Section 702 of FISA and EO 12,333.[179]

Interference with fundamental rights is not per se impermissible under EU constitutional law, but requires that the law creating the interference itself define the "scope of the limitation on the exercise of the right concerned."[180] EU law also operates under a rule of proportionality, meaning that any interference cannot be greater than necessary.[181] The broad authority to engage in surveillance, coupled with

---

protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.").

174. *See supra* Part I.A.1.

175. Case C-311/18, ¶ 164 ("[A]dherence to those [Privacy Shield] principles may be limited . . . to the extent necessary to meet 'national security, public interest, or law enforcement requirements.").

176. *Id.* ¶ 165.

177. PRISM is a surveillance program disclosed by Edward Snowden, which allows US intelligence agencies to request data from Internet companies such as Google, Microsoft, and Apple. It is conducted under Section 702 of FISA. Patrick Toomey, *The NSA Continues to Violate Americans' Internet Privacy Rights*, ACLU (Aug. 22, 2018), https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy [https://perma.cc/KK5R-UATB].

178. "Upstream" surveillance generally refers to the NSA's practice of bulk collection of data in transit by tapping into the physical components of the Internet. *See generally* Ashley Gorski & Patrick Toomey, *Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance*, ACLU (Sept. 23, 2016), https://www.aclu.org/blog/national-security/privacy-and-surveillance/unprecedented-and-unlawful-nsas-upstream [https://perma.cc/G3ZM-D7XR].

179. Case C-311/18, ¶ 165.

180. *Id.* ¶¶ 174–75 (citation omitted). PPD-28 is an executive directive from the Obama administration that articulated principles governing the collection of signals intelligence.

181. *See Proportionality*, EUROPA, https://ec.europa.eu/regional_policy/en/policy/what/glossary/p/proportionality [https://perma.cc/5Q39-6BMS].

the lack of protections or targeting measures in Section 702 of FISA and EO 12,333, do not fit that principle. In sum, US law needed sufficient safeguards to be built into the enabling law itself and failed to do so.[182] Access by public authorities can be lawful in the presence of proper safeguards, however, and Part III of this Note will explore potential safeguards that could be implemented in the US.[183]

The second fatal flaw with Privacy Shield is that it failed to provide judicial protection for EU citizens subject to such interferences. Judicial protection means that, wherever a right or freedom guaranteed by the law of the EU is violated, there must be an available effective remedy and a hearing before "an independent and impartial" tribunal.[184] An effective remedy in this context requires legislation that allows an individual to pursue legal remedies, either providing access to personal data relating to them or achieving "rectification or erasure of such data."[185] As for an independent and impartial tribunal, a third country must "ensure effective independent data protection supervision . . . [and] cooperation mechanisms with the Member States' data protection authorities . . . [so that] data subjects [are] provided with effective and enforceable rights and effective administrative and judicial redress."[186] During the development of Privacy Shield, it was well known that there were several avenues of electronic surveillance (notably EO 12,333 and Section 702 of FISA) available to US intelligence authorities that did not provide actionable rights against US authorities in court.[187] The US created the Privacy Shield Ombudsperson position in an attempt to allay concerns over those programs, but it was not enough.[188] Starting from the premise that data subjects "must have the possibility of bringing legal action before an independent and impartial court,"[189] the CJEU found that the Privacy Shield Ombud-

182. Case C-311/18, ¶ 185 ("In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by . . . the Charter.").

183. *See infra* Part III.A.

184. Case C-311/18, ¶ 186 ("Article 47 [of the Charter] requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal . . . . [E]veryone is entitled to a hearing by an independent and impartial tribunal.").

185. *Id.* ¶ 187.

186. *Id.* ¶ 188.

187. *Id.* ¶ 191.

188. *Id.* ¶ 194–96.

189. *Id.* ¶ 194.

sperson failed this in several regards. First, the court doubted the independence of the position, noting that the Ombudsperson is appointed by and reports to the Secretary of State.[190] Second, despite the US government's claim that US intelligence services are required to correct violations detected by the Ombudsperson, the court found that there is nothing to indicate the Ombudsperson "has the power to adopt decisions that are binding on [US] intelligence services" nor is there a mention of "legal safeguards that would accompany that political commitment on which data subjects could rely."[191] For that reason, the Ombudsperson was not a sufficient mechanism to meet the judicial protection element.

In light of this unbridled national security access to personal data and the absence of safeguard and judicial remedies, the CJEU found that Privacy Shield failed to comply with GDPR Article 45(1), and the adequacy decision was therefore invalid.[192] This is a significant problem for organizations relying on Privacy Shield to make necessary data transfers. That problem was exacerbated by the rest of the *Schrems II* judgment, which cast significant doubt on the most likely alternative transfer mechanism—Standard Contractual Clauses.

B. THE PRECARIOUS FOOTING OF STANDARD CONTRACTUAL CLAUSES HIGHLIGHTS THE NEED FOR A PRIVACY SHIELD REPLACEMENT

Privacy Shield was never the only transfer mechanism available to US organizations—many companies also rely on SCCs.[193] The court declined to find SCCs inadequate per se for data transfers to the United States,[194] but the judgment cast doubt on the viability of SCCs by suggesting that data protection authorities in the EU should individually assess whether transfers to the US pursuant to SCCs are susceptible to the same kind of unlawful national security access that rendered Privacy Shield inadequate.[195] This uncertainty surrounding SCCs exacerbates the loss of Privacy Shield because it potentially leaves companies in the US without any valid transfer mechanism. It also highlights

190. *Id.* ¶ 195.

191. *Id.* ¶ 196.

192. *Id.* ¶¶ 199–201.

193. *See Standard Contractual Clauses*, *supra* note 34 (discussing SCCs). Another possible transfer mechanism is Binding Corporate Rules (BCRs). BCRs are essentially an internal code of conduct that a multinational organization can develop to transfer data within its corporate structure. Developing BCRs is a lengthy, costly endeavor, and thus not a feasible option for the vast majority of organizations engaging in cross-border data transfers. MCGEVERAN, *supra* note 8, at 505.

194. Case C-311/18, ¶ 146–49.

195. *Id.* ¶ 146–49.

the need for legislative reform of US foreign surveillance practices because this broad access to personal data is impairing multiple transfer mechanisms.

The court's holding on SCCs contained a procedural question and a substantive question. The procedural question asked whether a supervisory authority[196] is required to suspend or prohibit transfers of personal data to a third country made pursuant to SCCs if that authority determined that the SCCs could not be complied with in the third country, i.e., if the personal data will not receive an adequate level of protection in that third country.[197] The court answered this question in the affirmative,[198] which means that these supervisory authorities are required to suspend transfers if they believe that organizations transferring data to the United States cannot comply with the requirements of the SCCs. The second more substantive question addressed was whether SCCs truly offer "adequate safeguards with respect to the protection of the privacy and fundamental rights of individuals . . . ."[199] The Court ultimately upheld SCCs as a valid transfer mechanism,[200] but qualified that decision:

> [T]he SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision . . . . [U]nless there is a valid Commission adequacy decision, the competent supervisory authority is required, . . . to suspend or prohibit such a transfer, if, in its view[,] . . . those clauses are not or cannot be complied with in that third country . . . .[201]

Although it did not invalidate SCCs, this decision renders them unreliable for organizations transferring data into the United States. If Pri-

196. Supervisory authorities are the independent public authorities that ensure GDPR compliance within a particular member state. Council Regulation 2016/679, art. 51, General Data Protection Regulation, 2016 O.J. (L 119) 65 ("Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation. . . . Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union.").

197. Case C-311/18, ¶ 106.

198. *Id.* ¶ 121 ("[T]he competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.").

199. *See id.* ¶ 27 (quoting the SCC decision).

200. *Id.* ¶ 149.

201. *Id.* ¶ 146.

vacy Shield was inadequate because it could not prevent US intelligence authorities from accessing personal data in a way that contravenes EU law, then SCCs are similarly inadequate because they are not binding on those public authorities either. If a supervisory authority determines that SCCs cannot be complied with in the US—a conclusion that is likely in light of the analysis of US law in the discussion about Privacy Shield—then that supervisory authority is obligated to suspend data transfers to the United States.

This enervation of SCCs, when coupled with the demise of Privacy Shield, leaves organizations transferring personal data to the United States without a reliable transfer mechanism. Privacy Shield is outright unusable and transfers pursuant to SCCs can be suspended by the relevant data protection authority.[202] Companies have survived in the short term, often by relying on the Article 49 derogations.[203] However, absent a long-term solution, these cross-border transfers may cease entirely. The practical fallout of this could be a significant impairment of the transatlantic economy and the death of the global Internet itself.

C. THE POST-*SCHREMS II* LANDSCAPE: THE LOOMING THREAT OF DATA LOCALIZATION AND A "SPLINTERNET"

Schrems I signaled that US surveillance practices and EU privacy law were fundamentally incompatible, and *Schrems II* demonstrated that there is no clever workaround to this issue for US companies; it is the collision of an immovable object and an unstoppable force, and unless one of them changes at a deep level then transatlantic data flows are going to grind to a halt. One major impact of *Schrems II*, therefore, is the looming specter of data localization and a "splinternet." A splinternet, often referred to as Internet balkanization, is the concept of having multiple regional internets rather than a unified global system.[204] This happens when users can only access data stored within their certain geopolitical bounds, i.e., Europeans can only communicate with servers located within the EU.[205]

---

202. As of October 2020, this is already happening. *See, e.g.*, Natasha Lomas, *Facebook Told It May Have to Suspend EU Data Transfers After Schrems II Ruling*, TECHCRUNCH (Sept. 9, 2020), https://techcrunch.com/2020/09/09/facebook-told-it-may-have-to-suspend-eu-data-transfers-after-schrems-ii-ruling [https://perma.cc/NG8D-S6VZ].

203. *See* Hengesbaugh, *supra* note 29 and accompanying text.

204. *See generally* L.S., *What Is the "Splinternet"?*, ECONOMIST (Nov. 22, 2016), https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [https://perma.cc/GR43-XBUG].

205. *See id.*

In the months following the judgment, many commentators—including Max Schrems—suggested that data localization was the solution to the legal problem posed by *Schrems II*.[206] "Stop transferring data" is a trivial solution to the inability to legally transfer data, and the practical implication of this would be that companies doing business in Europe have to host their data in Europe. That solution could be a boost for the European data hosting industry. However, other commentators quickly recognized that data localization is undesirable from both an EU and US perspective for a number of reasons.[207] First, data localization is expensive because it is duplicative.[208] Absent a push for data localization, companies operating in multiple countries can consolidate servers in one location and take advantage of economies of scale to provide their services at a lower average total cost. If a data localization regime is implemented, these companies would have to invest in the same server infrastructure in each region where they operate—a cost that could crowd smaller businesses out of certain markets.[209] Second, the modern economy is premised on free and open global trade, and data localization is antithetical to that goal.[210]

206. Int'l Ass'n Priv. Pros., *The* Schrems II *Decision: The Day After*, LINKEDIN (Jul. 17, 2020, 9:00 AM), https://lnkd.in/gkDciQ7 [https://perma.cc/4GHX-H7D4] (discussing the *Schrems II* decision during a recorded web panel, in which Max Schrems suggests companies should host data in Europe and not transfer it to the United States).

207. *See, e.g.*, Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 778–84 (2020) (addressing why data localization does not protect Europeans from surveillance, and other practical problems raised by data localization); Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (Jul. 17, 2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision [https://perma.cc/5KAR-TUCT] ("Keeping all personal data in Europe would be expensive, and cause numerous technical problems. But more fundamentally, it is hard to imagine how multinational companies and services could carry out their business if data entering the EU cannot emerge from it.").

208. *See* Chander, *supra* note 207, at 782 ("Data localization requires companies doing businesses [sic] in multiple jurisdictions to localize their infrastructure in multiple jurisdictions, which is likely to be an expensive process."). Chander also suggests that this issue of cost has a second order undesirable effect—it will harm smaller businesses because they will not be in a position to make this infrastructure investment.

209. *See id.* "Tech giants" do already host some of their data in the EU, but the investment in infrastructure necessary to do this makes it a non-option for smaller businesses. Recall that over 5,300 organizations relied on Privacy Shield to conduct EU-US data transfers. How many of those organizations can build personal data centers in Luleå, Sweden? *See* Mark Scott, *U.S. Tech Giants Are Investing Billions to Keep Data in Europe*, N.Y. TIMES (Oct. 3, 2016), https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html [https://perma.cc/4UXS-5EXE].

210. *See* Chander, *supra* note 207, at 782 ("The GDPR Recital 101 echoes this goal [of increased trade]: 'Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade

The collection of personal data is an inherent, unavoidable element of modern business. Requiring data localization therefore discourages global trade because it requires businesses to be physically located in a region to do business there. Third, European data localization risks retaliation in kind from other sovereigns, creating a splinternet.[211] If the United States, Canada, the United Kingdom, etc., all respond in kind with their own data localization mandates, suddenly each country has its own Internet. This will harm European-based Internet companies that operate in those other countries because they are they forced to create foreign subsidiaries if they want to operate in global markets. Fourth, data localization might harm privacy by weakening cybersecurity, because having operations in different locations increases the potential points of attack for hackers.[212] Fifth, data localization helps a minority of businesses, such as cloud storage, while raising costs for most others.[213] Finally, and perhaps most persuasively, if the EU wanted data localized within its borders, then it would not have provided for a transfer mechanism at all.[214] For these reasons, the US and EU should do everything they can, within reason, to avoid data localization and facilitate Article 45 data transfers between the EU and US.

Schrems II represents a failure to learn from *Schrems I*, which was unequivocal in its holding that US access to personal data for national security purposes conflicts with EU rights. A self-certification regime that does not relieve organizations of their obligations under US law will not withstand scrutiny at the CJEU, no matter how many versions of the program the US Department of Commerce and European Commission ratify. It is therefore imperative that the US avoids repeating its mistakes once again and does not simply pass an "enhanced Pri-

---

and international cooperation.' Data localization lies in tension with the 'EU [sic] own goals of furthering global data flows . . . .").

211. *See id*. at 783 ("Countries that feel the sting of data localization requirements from their trading partners will respond in kind.").

212. *See id*. at 783 ("By requiring a company to establish, update, and defend multiple versions of its systems across continents, it opens a bigger attack surface for malicious hackers in the form of additional hardware, additional vendors, and additional employees . . . .").

213. *See id*. at 784 ("Much of the benefit of data localization for local enterprise accrues to cloud storage businesses, a relatively small part of the economy . . . . Microsoft in 2015 offered its European customers an alternative: establishing a data trustee in Germany by working with Deutsche Telekom to hold data. But by 2018, Microsoft decided to not accept any more clients to this arrangement. Apparently, the cloud service subcontracted with Deutsche Telekom proved both too expensive and of inadequate quality . . . .").

214. *See generally id*. at 772–74 (discussing "*Schrems II* and mechanisms for cross-border data flows").

vacy Shield" without accompanying legislative action. Like its predecessor case, the *Schrems II* explicitly stated that safeguards and judicial remedies must be present in the legislation enabling interference with the rights to privacy and data protection. If the US truly wants to solve the *Schrems II* problem, it needs to do more than it did in the wake of *Schrems I* and pass legislative reforms of national security surveillance practices. There must be a Privacy Shield Enabling Act.

III. BRIDGING THE GAP: A PRIVACY SHIELD ENABLING ACT ENACTING MODEST FISA REFORMS IS NECESSARY TO ENABLE TRANSATLANTIC DATA TRANSFERS

Read in tandem, the *Schrems* duology conveys one unequivocal message: US and EU privacy regimes, in their current iterations, are fundamentally incompatible. The Department of Commerce and European Commission are working on a successor program to Privacy Shield, but that is a futile effort because Privacy Shield's flaws were external to the program itself.[215] The core issue is the US's underlying surveillance laws. Legislative reform of US surveillance practices is therefore necessary if the US wants access to European data and, consequently, markets. Given the broad geopolitical issues at stake, however, setting the scope of legislative action is a serious challenge. Privacy activists in the US have long advocated for a federal privacy law on the scale of the GDPR, and that would solve this data transfer conundrum.[216] That is an unlikely prospect, at least in the short term. It is easy to say that the US should enact a federal privacy scheme, but it is a Herculean task to get Congressional consensus on such contentious issues.[217] Thus, while a comprehensive federal privacy scheme might be the best solution, a quicker stop-gap measure could be immensely valuable.[218]

---

215. *See generally* Andraya Flor, *The Impact of* Schrems II*: Next Steps for U.S. Data Privacy Law*, 96 NOTRE DAME L. REV. 2035, 2037 (2021) ("Even if a third replacement agreement is reached soon, there is no reason to believe it would not be subject to another challenge from Schrems.").

216. *See id.* at 2051–58 (advocating for a "federal regulation that requires companies to comply with specific minimum standards of data processing" in response to the *Schrems II* decision and highly publicized data disclosures).

217. Politicians in Congress have been debating privacy legislation for years, and there is little consensus on how to proceed. One major sticking point is whether a federal privacy law would preempt state data protection laws, such as the California Consumer Privacy Act. Elizabeth Schulze, *The US Wants to Copy Europe's Strict Data Privacy Law—But Only Some of It*, CNBC (May 23, 2019), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html [https://perma.cc/H4YL-XKGN].

218. Another solution floated by commentators is the development of a multilateral privacy treaty. *See* Jedidiah Bracy, *Is a 'Multilateral Privacy Treaty' the Answer to*

Rather than waiting for a comprehensive US data protection scheme, this Note argues that Congress should pursue a narrower solution and develop a Privacy Shield Enabling Act ("PSEA" or "Act"). Through targeted reforms to US foreign intelligence surveillance, limiting national security access to personal data of EU citizens to only what is strictly necessary, Congress could enable an "enhanced Privacy Shield" program to survive a legal challenge at the CJEU. This solution would not bridge the gap between the US and EU privacy regimes—which is the reason Privacy Shield needs to exist at all—but it would enable organizations who need to transfer personal data across the Atlantic for operational and business purposes to do so. Section A of this Part will discuss the "core requirements" that the PSEA will need to remedy the CJEU's concerns. These proposals are focused on (1) increasing transparency surrounding foreign intelligence surveillance by adding safeguards to prevent unnecessary collection, use, and storage of personal data and (2) strengthening judicial remedies. Section B will then explore the most immediate barriers to passing the PSEA, such as lack of political will and potential constitutional concerns in constraining the Executive's foreign affairs powers.

A. THE PRIVACY SHIELD ENABLING ACT: CORE FEATURES

The *Schrems II* court firmly stated that "the legal basis which permits the interference with [fundamental] rights must *itself* define the scope of the limitation on the exercise of the right concerned"[219] and "the legislation in question . . . 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."[220] Read literally, this language places the onus on Congress to pass a modest legislative act to remedy the specific grievances identified by the CJEU. While it is theoretically possible that an Executive Order might suffice to implement these changes, that position is doubtful in light of both the language cited above as well as court's concern that the Privacy Shield Ombudsperson be independent from the executive.[221] Presidential administrations are ephemeral, and it is difficult to imagine the CJEU sanctifying a successor program so long as the safeguards and judicial remedies

"Schrems II"*?*, IAPP (Mar. 11, 2021), https://iapp.org/news/a/is-a-multilateral-privacy-treaty-the-answer-to-schrems-ii [https://perma.cc/8V78-J9KB].

219. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 175 (July 16, 2020) (emphasis added) (citation omitted).

220. *Id.* ¶ 176.

221. *See id.* ¶ 195.

can be revoked at a moment's notice by a later President.[222] For that reason, legislation is the preferable avenue.

The basic framework of the PSEA can be lifted directly from the *Schrems II* judgment. Like Safe Harbor and Privacy Shield, any future US-EU program will need to satisfy Article 45(3) of the GDPR, read in light of Articles 7, 8, 47 of the Charter of Fundamental Rights.[223] Assuming that a successor program does at least everything Privacy Shield did, then the PSEA only needs to amend US surveillance law in two key ways: adding safeguards and limitations to surveillance practices, such that collection of personal data of EU citizens is limited to what is strictly necessary, and adding effective judicial protections. The following suggestions for implementing those changes are just that—suggestions. *Schrems II* does not make prescriptive judgments about how to fix these issues; it merely diagnoses the ailment. Fortunately, this does not mean that crafting the PSEA is painting on a blank canvas. EU member states have their own electronic surveillance laws, and those practices can be transposed into US law where appropriate. Additionally, academics and privacy professionals were aware of many of Privacy Shield's weaknesses from its inception, and many commentators theorized about how the program could be strengthened in the years preceding *Schrems II*.[224] Finally, interested parties have already raised similar proposals since *Schrems II*. The American

222. This fear is undercut by the fact that an adequacy decision under Article 45(3), against which a successor program would be judged, is subject to review at least every four years. Council Regulation 2016/679, art. 45(3), General Data Protection Regulation, 2016 O.J. (L 119) 61.

223. Case C-311/18, ¶ 162. The relevant articles of the Charter are the respect for private and family life, protection of personal data, and right to an effective remedy and to a fair trial. Charter of Fundamental Rights of the European Union, arts. 7, 8, 47, 2000 O.J. (C364) 10, 20.

224. *See, e.g.*, Read, *supra* note 163, at 293–96. Read's assessment of Privacy Shield's future came in the wake of FISA's renewal and Congress's failure to implement adequate privacy standards at the time. The suggestions for improvement largely focused on the United States' decision not to "fully incorporate" PPD-28, President Obama's nonbinding policy directive aimed at providing extra protections to non-Americans, into Section 702 when renewing the act. Read also noted that the US was not keeping pace in appointing supervisory administrators such as the Privacy Shield Ombudsperson. While both suggestions would be good in their own right, neither likely would have been sufficient under the judgment ultimately issued by the CJEU. *See* Case C-311/18, ¶ 183 ("It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for "'bulk' collection . . . of a relatively large volume of signals intelligence . . . ." That possibility, which allows . . . access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data."); *id.* ¶ 195 (doubting the efficacy of the Privacy Shield Ombudsperson role due to perceived dependence on the Intelligence Community and Executive Branch).

Civil Liberties Union (ACLU) released a letter to the US Department of Commerce in the wake of *Schrems II* detailing potential reforms,[225] and the Center for Democracy & Technology (CDT) highlighted the need for intelligence surveillance reform in early 2021.[226] These various sources, in combination, provide a wealth of reform options that shaped the following proposals.

The PSEA should amend the US Foreign Intelligence Surveillance Act to narrow the scope of data collection, increase transparency surrounding the methods of collection, and add effective judicial remedies for surveillance subjects. To achieve those goals, the PSEA specifically needs to (1) narrow the definition of potential surveillance targets, (2) expand the minimization procedures to cover European citizens as well as United States persons, (3) implement a maximum data retention period and require the United States to demonstrate probable cause to a judge on the FISC to exceed that limit, (4) implement a notice mechanism by which data subjects can learn that their data has been intercepted and is being retained, (5) increase the power of the Privacy Shield Ombudsperson to order data disgorgement, and (6) create a private right of action by which an aggrieved European citizen can, after a hearing before the Privacy Shield Ombudsperson, challenge surveillance of personal data before the FISC. The first three proposals add safeguards to limit interference with fundamental rights to what is strictly necessary, while the latter proposals focus on providing sufficient judicial remedies. Each set of proposals is addressed in the two subsections that follow.

1. Increased Transparency and Meaningful Minimization and Retention Procedures

As discussed above, European constitutional law operates on a principal of proportionality.[227] This gives the PSEA considerable leeway in the potential reforms. Interferences with fundamental rights under the Charter of Fundamental Freedoms do not need to be eliminated; they only need to be limited to what is strictly necessary in light

225. Letter from American Civil Liberties Union to United States Department of Commerce, (July 21, 2020) [hereinafter ACLU Letter], https://www.aclu.org/sites/default/files/field_document/2020-07-21_aclu_schrems_ii_decision_letter.pdf [https://perma.cc/42X5-P59Z].

226. The recommendations in this Note align with those of the CDT, although this Note focuses on imposing the changes legislatively rather than administratively. *See* Greg Nojeim, Schrems II *and the Need for Intelligence Surveillance Reform*, CTR. FOR DEMOCRACY & TECH. (Jan. 13, 2021), https://cdt.org/wp-content/uploads/2021/01/2021-01-13-CDT-Schrems-II-and-Intelligence-Surveillance-Reform-in-the-US.pdf [https://perma.cc/A8H7-A4LE].

227. For an analysis of proportionality, see *supra* Part II.A.

of the countervailing governmental interest. Thus, the PSEA must limit interference to what is strictly necessary. To do this, the CJEU has clarified that the source of law which enables the interference (here, Section 702 of FISA and EO 12,333) must:

> lay down clear and precise rules governing the scope and application of the measure in question and impos[e] 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.[228]

The starting place for reform should therefore be 50 U.S.C. §§ 1801, 1881–1881g, which are the relevant provisions in the US code governing the procedure of foreign electronic surveillance.

First, the scope of collection should be narrowed by changing the definition of permissible targets. Currently, the Director of National Intelligence can authorize, for a period up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[229] This authorization is more expansive than the original Foreign Intelligence Surveillance Act of 1978, which required a probable cause showing that a target be a "foreign power" or "an agent of a foreign power."[230] Scaling back the scope of authorization to the original, higher requirement that a target be a foreign power or agent thereof will reduce the scope of potential targets, thereby reducing the potential abuses of surveillance.[231] The definitional change alone should theoretically reduce the scope of targeting, but this narrowing could be extended further by adding back the probable cause requirement as well.[232]

Second, Congress should mandate that the Attorney General promulgate broader minimization procedures that avoid incidental collection of personal data concerning EU citizens who are not themselves the target of surveillance.[233] Data minimization is one of the basic principles of the GDPR.[234] Section 702 requires the Attorney

228. Case C-311/18, ¶ 176.

229. 50 U.S.C. § 1881a(a).

230. Foreign Intelligence Surveillance Act of 1978, Sec. 105(a)(3), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. § 1881).

231. *See* ACLU Letter, *supra* note 225, at 5 (advocating for a return to these labels).

232. Currently, Section 702 does not require the government to demonstrate probable cause that its surveillance targets are foreign agents or engaged in any harmful activities such as terrorism, which undercuts any argument that the US practice, in its current iteration, is limited to what is strictly necessary. *See id.*

233. *See id.* (suggesting "implement[ing] more stringent minimization requirements").

234. Council Regulation 2016/679, art. 5, General Data Protection Regulation,

General to adopt specific minimization procedures to avoid unnecessary acquisition, retention, and dissemination of nonpublic information concerning "United States persons."[235] These minimization requirements should be expanded by replacing references to "United States persons" with "all natural persons" or requiring minimization procedures specifically for "citizens of the European Union."[236] These expanded minimization requirements would limit incidental collection of personal data concerning EU citizens who are not themselves the targets of surveillance. It is difficult to identify what basic elements these broader minimization procedures would need to have without defeating the purpose of foreign electronic communication surveillance in its entirety. For that reason, this reform would require significant cooperation with the Intelligence Community. Nevertheless, some form of data minimization for European citizens would go a long way to helping the PSEA serve its intended purpose.

In a similar vein, there must also be a data retention limit, which requires the Intelligence Community to disgorge personal data concerning persons located in the EU after a certain amount of time. The CJEU has previously held that data retention for the purpose of investigating serious crimes is appropriate, but that retention period must be clear and based on an objective criterion.[237] Applying that general guideline to US law, Section 702 of FISA permits the Attorney General and the Director of National Intelligence to authorize the targeting of persons (i.e., collection of personal data) for up to one year.[238] A one-year extendable statutory limit for data retention would dovetail nicely with that provision. If the Intelligence Community feels that it

---

2016 O.J. (L 119) 35 (requiring that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed").

235. 50 U.S.C. §§ 1801(h), 1881a(e) (protecting United States persons from dissemination of non-publicly available information). For an example of what these minimization procedures look like once promulgated, see *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978*, OFF. OF DIR. OF NAT'L INTELL, https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf [https://perma.cc/MMB6-TYKE].

236. If the executive branch wanted to retain its foreign surveillance powers to the largest extent possible while still facilitating transatlantic data flows and maintaining good economic relations with Europe, the minimization procedures could instead be expanded to cover only "United States and European Union persons." Such a Western focused exemption would raise serious ethical, racial, and geopolitical concerns, however, that exceed the scope of this Note.

237. Case C-293/12, Digit. Rts. Ir. Ltd. V. Minister for Commc'ns, Marine & Nat. Res., ECLI:EU:C:2014:238, ¶¶ 49, 63–64 (Apr. 8, 2014).

238. *See* Foreign Intelligence Surveillance Act of 1978, Sec. 702, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. § 1881).

needs to retain that data longer that the statutory limit, it would need to go before the FISC and demonstrate probable cause as to why it needs to be retained. Requiring a showing of probable cause to extend the retention period should satisfy the "objective criteria" requirement the CJEU has previously imposed on length data retention periods.

The proposals above are designed to add sufficient safeguards to limit collection, use, storage, and disclosure of personal data concerning EU citizens to what is strictly necessary. The other necessary set of reforms, ensuring sufficient judicial remedies, is a more challenging endeavor from a procedural perspective because of the sensitive and covert nature of foreign intelligence surveillance.

2. Insulating the Privacy Shield Ombudsperson and Expanding the Role of the FISC

Adding appropriate safeguards is only one half of what the PSEA needs to be effective—it also must "ensure effective judicial protection against such interferences."[239] To meet this requirement, anyone who believes his or her rights have been violated must be able to obtain a "hearing by an independent and impartial tribunal,"[240] and all data subjects must have "rights actionable in the courts against the US authorities."[241]

The Privacy Shield Ombudsperson was meant to serve as an impartial tribunal before which affected parties could seek redress. However, the position is neither impartial nor truly offers redress, according to the CJEU, because the Privacy Shield Ombudsperson is subject to removal by the Secretary of State and is not able to order rectification or erasure of data.[242] Both of these issues therefore need to be remedied if the Privacy Shield Ombudsperson is to fulfill its intended purpose under an enhanced Privacy Shield program. As for the independence issue, it is a well-established principle of American constitutional law that "[t]he power of removal is incident to the power of appointment."[243] While the Privacy Shield Ombudsperson could be insulated by imposing a "good cause" removal requirement,[244] the Executive will always be able to assert some degree of influence over the

239. Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 168 (July 16, 2020).

240. *Id.* ¶ 186.

241. *Id.* ¶ 192.

242. *Id.* ¶¶ 194–95.

243. Myers v. United States, 272 U.S. 52, 122 (1926).

244. *See* Humphrey's Ex'r v. United States, 295 U.S. 602, 632 (1935) (holding that members of the Federal Trade Commission could only be removed for one of the

role.[245] Despite that concern, the CJEU has indicated that a fixed term and specific grounds for removal are sufficient to establish independence and impartiality.[246] Regarding the effective redress issue, the Privacy Shield Ombudsperson must be granted the power to order intelligence agencies to rectify or erase data if the Ombudsperson determines that possession or processing of that data improperly interferes with the data subject's rights.[247]

Granting data subjects actionable rights against the US authorities is a tricky problem because electronic surveillance is inherently secretive. Digital espionage would not be effective if data subjects were aware that their personal data were being acquired, but it is impossible to obtain a judicial remedy if someone does not know that their rights are being violated. The PSEA must include some mechanism for notifying surveillance subjects that data concerning them has been collected by the US government after that collection and investigation has ended.[248] The question is at what point after surveillance concludes that notice should occur. The actual practices of EU member states should be highly informative in finalizing this provision.[249] For example, the UK used to alert a subject if they have been "adversely affected by any serious error or by any willful or reckless conduct by

causes named in the statute).

245. *See, e.g.*, Morrison v. Olson, 487 U.S. 654, 692 (1988) (noting that a good cause removal provision did not "impermissibly burden[] the President's power to control or supervise the independent counsel" because "the Executive, through the Attorney General, retain[ed] ample authority to assure that the counsel [wa]s competently performing his or her statutory responsibilities"). Thus, even if the Privacy Shield Ombudsperson were insulated by "good cause" removal, the Executive could still influence the Ombudsperson through the Secretary of State, who would hold removal power.

246. Case C-311/18, ¶ 195 (July 16, 2020) (citing case C-274/14 for the rules governing what constitutes sufficient independence); Case C-274/14, Banco de Santander, ECLI:EU:C:2020:17, ¶¶ 60, 63 (Jan. 21, 2020) ("Those guarantees of independence and impartiality require rules, particularly as regards the composition of the body and the appointment, length of service and the grounds for abstention, rejection and dismissal of its members, in order to dismiss any reasonable doubt in the minds of individuals as to the imperviousness of that body to external factors and its neutrality with respect to the interests before it . . . .") (citation omitted).

247. *See* Case C-311/18, ¶ 196.

248. The ACLU, in its suggested reforms, strongly captures the need for a robust notice requirement: "[O]ne of the primary barriers to effective redress in U.S. courts is lack of notice . . . . As a practical matter, the lack of notice makes it difficult—if not impossible—for litigants to establish standing to challenge unlawful surveillance in U.S. courts." ACLU Letter, *supra* note 225, at 7.

249. For an in-depth analysis of the notification practices in the EU, see generally *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*, EUR. UNION AGENCY FOR FUNDAMENTAL RTS. ch. 13 (2017), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf [https://perma.cc/EHS3-H59N].

a public authority."[250] This Note does not endorse any specific notice standard, because the notice requirement is perhaps the most sensitive and open to debate aspect of the PSEA. It is sufficient for the purpose of this Note to identify that a notice provision in some form is necessary to enact actionable data subject rights, which are in turn necessary to satisfy the transfer requirements of the GDPR. Once a data subject has been afforded notice that their personal data has been acquired by the US, the data subject must have the right to access, rectification, or erasure of said data.

The PSEA, as outlined above, is not a finished article. It is a scaffolding on which policy makers, intelligence agencies, and data scientists should work together to complete a modest reform of US surveillance law. The cooperation of the intelligence agencies is vital in this process. There is much the American public still does not know about the United States' foreign intelligence surveillance, and those intelligence agencies have the most to lose by engaging in reform measures. However, it is the American people, citizens of Europe, and global economy that stand to lose the most if these data transfers cease.[251] For that reason, it is necessary to consider the potential barriers that could prevent the PSEA from achieving its purpose.

B. Political and Constitutional Barriers to a Legislative Remedy

Assuming the PSEA would remedy the conflict with EU law and enable a Privacy Shield replacement program to survive review by the CJEU, it would still need to survive the American political process and judicial review by American courts—neither of which is a certainty. The main domestic barriers to reform are the speed and efficacy of the legislative process, political support for the United States' current surveillance practices, and separation of powers problems arising from Congress interfering with the President's foreign affairs powers.

The concerns about the speed with which Congress could develop and pass a functional version of the PSEA and the mixed support for such a measure are interrelated problems. FISA reform has been a target for privacy activists for many years, and those groups have had middling success.[252] FISA reform may also not be a priority for Congress as domestic terrorism becomes a more salient issue. Although

250. *Id.* at 124.

251. *See supra* Part II.C (analyzing the likely fallout if a long-term data transfer mechanism is not developed).

252. The Electronic Privacy Information Center (EPIC) provides a running overview of its efforts to enact FISA reform. *Foreign Intelligence Surveillance Act Reform*, Elec. Priv. Info. Ctr., https://epic.org/privacy/surveillance/fisa/reform [https://perma.cc/B9JD-64N4].

international terrorism concerns dominated US politics for many years, events such as the attacks of September 11th, 2001, which precipitated much of the 20th century expanded electronic surveillance practices at issue in *Schrems II*, grow more distant in time. In contrast, domestic terror events continue to dominate the news cycle.[253] Congress may shift its focus accordingly,[254] leaving FISA reform as a background concern. As the practical fallout from the *Schrems II* decision fully manifests itself and the need for the PSEA becomes more evident, there may already be irreparable harm to global trade and the infrastructure of the data economy.

Another potential issue in passing the PSEA is the separation of powers. A key aspect of *Schrems II* was that bulk data collection under EO 12,333, which occurs outside the US, violates the fundamental rights to privacy and data protection. With that in mind, the PSEA needs a seventh proposal: (7) end bulk data collection under EO 12,333 by requiring that procedural safeguards detailed above be extended to all foreign intelligence surveillance, regardless of the legal basis for that surveillance. The premise of this provision is that EO 12,333 is independent of FISA, and thus would not be affected by the other reform measures above. For that same reason, it is perhaps unwise to try and append a limitation on EO 12,333 into the FISA provisions. While Congress's ability to amend FISA is undoubted, it is not clear what authority it has to intervene in the President's unilateral

253. *See, e.g.*, *Examining the January 6 Attack on the U.S. Capitol*, FBI (June 15, 2021), https://www.fbi.gov/news/testimony/examining-the-january-6-attack-on-the-us-capitol-wray-061521 [https://perma.cc/5W5J-8EG8] (assessing the riots which occurred at the U.S. Capitol on January 6, 2021 and dominated the news for months afterwards).

254. *See* Karoun Demirjian, *Bipartisan Support Emerges for Domestic-Terror Bills as Experts Warn Threat May Last '10 to 20 Years'*, WASH. POST (Feb. 4, 2021), https://www.washingtonpost.com/national-security/capitol-riot-domestic-terror-legislation/2021/02/04/f43ec214-6733-11eb-8468-21bc48f07fe5_story.html [https://perma.cc/SS5T-2K24]; *Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 25 (2019) (statement of Rep. Bernie G. Thompson, Chairman, H. Comm. on Homeland Sec.) ("[O]ne of the challenges we have is the changing of the threat landscape. When we first started as a committee, we were focused on the international terrorist threat to the homeland. Over time, it appears that that threat, based on testimony, is changing to a different threat."). *But see* Alexandra Limon, *Experts Urge Congress to Focus on Domestic Terrorism Fight*, ABC (Aug. 3, 2021), https://www.abc27.com/news/washington-dc/experts-urge-congress-to-focus-on-domestic-terrorism-fight [https://perma.cc/EH8G-5PMC] (noting the lack of progress by Congress on making domestic terrorism an independent crime following the two-year anniversary of the shootings in El Paso targeting Hispanic Americans).

practices. The President maintains vast power when it comes to foreign affairs.[255] Inserting this seventh proposal, although necessary, could render the PSEA vulnerable to a separation of powers challenge. Excluding EO 12,333 from the PSEA's purview and focusing solely on FISA reform would avoid this possibility, but the PSEA might not achieve its goal without EO 12,333 reform. If Congress and the Executive were aligned on this issue, then the President could unilaterally end the problematic EO 12,333 practices and remedy the issue that way. However, policy changes with administrations, and a future President who is more hawkish on national security could reverse course and reimplement the problematic practices, thereby reigniting this whole problem anew. For that reason, it would be ideal to foreclose that kind of presidential action at all by statute.

Finally, in trying to solve this problem raised by *Schrems II*, it must be noted that there are many stakeholders with competing interests. The European Union has an interest in protecting the rights of its citizens, which is balanced against a desire to participate in the global marketplace. European citizens likewise have an interest in protecting their personal data, while still availing themselves of American services offered over the Internet. Businesses in the United States want to operate in the global market without facing undue administrative fines or data hosting costs. The United States government wants its citizens to thrive in the global economy, but also has a strong interest in maintaining its robust national security intelligence practices. One important stakeholder to bring to the table in resolving this issue is the US Intelligence Community. Participation and transparency by the Intelligence Community will be vital in developing a fully-fledged version of the PSEA that introduces meaningful safeguards but does not unduly threaten national security. The Intelligence Community may be reticent to involve itself in this process because it currently enjoys broad access to personal data for its signals intelligence operations. However, the PSEA could be a boon to the Intelligence Community if it thinks of this as giving a little to keep a lot. If these transatlantic data flows are a beneficial source of information, then failing to implement modest reform risks losing them in their entirety. For that reason, it is in the Intelligence Community's interest to help implement some form of the proposals below. Every party involved

255. *See* United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) (identifying a "very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations[,]" which "accord[s] to the President a degree of discretion and freedom from statutory restriction which would not be admissible were domestic affairs alone involved.").

therefore has factors weighing in favor of both the status quo and enacting the PSEA. Finding common ground between these positions is a difficult task but not impossible.

CONCLUSION

The death of Privacy Shield is a symptom of a broader conflict of values between the US and EU which represents an existential threat to the concept of a globalized economy. During the *Schrems II* litigation, an Advocate General of the CJEU eloquently captured the heart of this problem: there is a tension between "the need to show a reasonable degree of pragmatism in order to allow interaction with other parts of the world, and, on the other hand, the need to assert the fundamental values recognised in the [European Union]."[256] From the US perspective, this becomes a tension between the need for interaction with other parts of the world and the strong desire for robust surveillance in the name of national security. Unfortunately, this tension that came to a head in *Schrems II* is not one in which the US and EU can talk past one another and fail to reach actual compromise. By passing and strictly enforcing the GDPR, the EU has drawn its line in the sand. The onus is therefore on the US to determine which it values more: unbridled national security access to data flows, or the $7.1 trillion economic relationship it has with the EU.[257]

The US and EU will undoubtedly develop a new "enhanced Privacy Shield" program because they must—the political and economic pressures will be too great to do so.[258] That successor program may offer US organizations relief for a short period, but, unless the US adapts its foreign intelligence surveillance laws to resolve this fundamental conflict, this will be a futile effort. Absent such legislative action, any self-certification program akin to Privacy Shield is destined for a similar demise in a future *Schrems III*, and this tireless dance will continue ad infinitum. The US must pass a Privacy Shield Enabling Act to truly resolve this issue. Failure to do so threatens the US's role in the global economy and the very nature of the global Internet.

256. Opinion of Advocate General Saugmandsgaard Øe, Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2019:1145, ¶ 7 (delivered Dec. 19, 2019) (internal quotes omitted).

257. *See* Wilbur Ross Statement, *supra* note 27.

258. *See* Joint Press Statement, *supra* note 33 ("The European Union and the United States recognise the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies.").