Fordham Law Review

Volume 90 | Issue 1 Article 6

2021

Schrems's Slippery Slope: Strengthening Governance Mechanisms to Rehabilitate EU-U.S. Cross-Border Data Transfers After Schrems II

Edward W. McLaughlin
Fordham University School of Law

SCHREMS'S SLIPPERY SLOPE: STRENGTHENING GOVERNANCE MECHANISMS TO REHABILITATE EU-U.S. CROSS-BORDER DATA TRANSFERS AFTER *SCHREMS II*

*Edward W. McLaughlin**

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield Framework, the central data governance mechanism that once governed cross-border data transfers from the European Union (EU) to the United States. For the second time in five years, Europe's top court invalidated the primary method of cross-border data transfers. Both times the CJEU found that the United States's surveillance laws were, and remain, overbroad and fail to provide EU citizens with protections that are essentially equivalent to those guaranteed under the EU's General Data Protection Regulation (GDPR) in light of the Charter of Fundamental Rights of the European Union.

As a result, more than 5400 companies that utilized the Privacy Shield Framework are now scrambling to implement new mechanisms to govern their data transfers along with what they hope are effective supplementary technical, operational, or contractual measures to achieve an essentially equivalent level of protection for their cross-border data transfers from the EU to the United States.

Currently, there exists minimal guidance about how companies may satisfy the GDPR's requirements. Even if the United States and the EU negotiate and implement a "Privacy Shield 2.0" in the near future, a new framework is unlikely to remedy some of the faults the CJEU has consistently identified in U.S. surveillance law. This Note argues that a combination of private-law enhancements, contractual and technical, along with minor modifications to the administrative and judicial oversight of U.S. intelligence agencies, is required to create a sound and stable framework that achieves the needs of EU individuals' privacy rights and still enables the United States to exercise legitimate foreign surveillance in the interest of national security.

* J.D. Candidate, 2022, Fordham University School of Law; M.S., 2012, Syracuse University; B.S., 2011, Syracuse University. I would like to thank Professor Olivier Sylvain for his guidance and expertise throughout this process. I would also like to thank my editor, Abigail Sia, for her comments and suggestions and the editors and staff of the *Fordham Law Review* for their diligent editing. Finally, I would like to thank my wife, my parents, my sister, and all my friends and family for their constant love, encouragement, and support.

INTRODUCTION

As part of the modern, digital, and international economy, companies of all sizes transfer the personal information of their users or customers across international borders as part of their normal business operations.[1] Naturally, such transfers are subject to the laws and regulations of the respective jurisdictions in which the transfers transpire.

The General Data Protection Regulation (GDPR) permits the transfer of European Union (EU) subjects' data from the EU to third-party ("non-EU") countries only if the transfers utilize certain approved transfer mechanisms.[2] The mechanisms are acceptable under European law so long as the data protections in those non-EU countries are "essentially equivalent" to those of the EU.[3]

The EU and the U.S. Department of Commerce created the Privacy Shield Framework ("Privacy Shield") as an approved transfer mechanism to facilitate efficient data transfers to the United States based on the GDPR's mandate.[4] The Privacy Shield is a series of data privacy and security principles that U.S. companies agree to abide by in processing or transferring personal information between the EU and the United States.[5] The EU determined the Privacy Shield provided adequate safeguards and protection for EU data subjects that was consistent with the requirements under European law.[6] Therefore, by self-certifying and remaining compliant with the Privacy Shield, U.S. companies were able to execute their relevant business in the EU.

Then, in July 2020, the Court of Justice of the European Union (CJEU), the EU's highest court, held that U.S. protections for individual data rights under the Privacy Shield were inadequate,[7] in part because of U.S. authorities' broad ability to access the data.[8] As a result, EU and U.S.

---

1. Before the Privacy Shield was declared invalid in July 2020, more than 5400 companies, 70 percent of which were small- and medium-sized enterprises, used the Privacy Shield for their EU-U.S. cross-border data transfers. *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. 5–6 (Dec. 9, 2020) (testimony of James M. Sullivan, Deputy Assistant Secretary for Services, International Trade Administration, U.S. Department of Commerce), https://www.commerce.senate.gov/services/files/8F72849E-3625-4687-B8F5-71AFF4640D1F [https://perma.cc/99VY-MY47].

2. *See generally* Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

3. *Id.* recital 104.

4. *See id.* recital 108.

5. *See* Commission Implementing Decision 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 48 (EU) [hereinafter Privacy Shield Decision].

6. *See id.*

7. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems (*Schrems II*), ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020).

8. *See id.* ¶ 180 (holding that U.S. law supporting the Privacy Shield does not impose limitations on the power of U.S. authorities to implement certain surveillance programs and, therefore, cannot ensure a level of protection "essentially equivalent" to that in the EU under the GDPR and the Charter of Fundamental Rights).

companies can no longer rely on the Privacy Shield for their cross-border transfer needs.[9] The decision caused immediate problems for more than 5400 companies that relied on the Privacy Shield[10] because it did not allow for any grace period during which firms could continue to be protected by the practice while a new solution was created.[11]

In *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*[12] (*Schrems II)*, the CJEU rendered its decision in two parts. First, it upheld the validity of standard contractual clauses (SCC), a type of private-law solution, in principle.[13] Second, however, the CJEU emphasized that data controllers and processors (the contracting companies or entities)[14] are still obligated to make sure adequate protections exist in the relevant third-party countries.[15] The CJEU's invalidation of the Privacy Shield applied specifically to the EU-U.S. framework.[16] The SCC decision applies generally to the standard clauses used between companies in any third-party country and places the onus on the parties to determine the adequacy of protection in their respective countries or territories.[17] However, the court's assessment of U.S. law's inadequate data protections—mainly that U.S. authorities are too broadly authorized to access and analyze data and that EU subjects lack adequate judicial redress against such abuse—means cross-border transfers to the United States using SCCs suffer the same inadequate protections in practice as those that relied on the now-defunct Privacy Shield.[18]

The decision marks the second time in five years that the CJEU declared the primary EU-U.S. cross-border data transfer mechanism invalid. The CJEU reached the same conclusion previously in 2015 in *Maximillian*

9. *See id.* ¶ 201.

10. *See* Press Release, Wilbur Ross, Sec'y of Com., 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), 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/MT3D-XJJE] [hereinafter Statement on Schrems II Ruling].

11. *See* EUROPEAN DATA PROT. BD., FREQUENTLY ASKED QUESTIONS ON THE JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION IN CASE C-311/18–*DATA PROTECTION COMMISSIONER V FACEBOOK IRELAND LTD AND MAXIMILLIAN SCHREMS* 2 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf [https://perma.cc/75TN-83M9].

12. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

13. *See id.* ¶ 148.

14. For the purposes of this Note, it is sufficient to understand that controllers and processors are the entities involved in the collection, storage, dissemination, or other processing of personal data and transfer of that data to recipients. *See* GDPR, *supra* note 2, art. 4(7)–(8). In this context, a controller will typically be the EU-based data exporter and the processor will be the U.S.-based importer. *See id.* However, a more detailed explanation and definition of the roles is in Article 4 of the GDPR. *See id.*

15. *See Schrems II*, C-311/18, ¶ 131.

16. *See id.* ¶ 199.

17. *See id.* ¶ 134.

18. *See* EUROPEAN DATA PROT. BD., *supra* note 11, at 2.

Schrems v. Data Protection Commissioner[19] (*Schrems I*). *Schrems I* invalidated the Safe Harbor Framework, which had been the cross-border data transfer agreement in place between the United States and the EU since 2000.[20]

Both cases were the result of complaints initially brought by Austrian privacy activist, Maximillian Schrems, in response to Edward Snowden's 2013 public revelations about the scale and scope of some of the U.S. intelligence authorities' surveillance programs.[21] Schrems's suits asserted that, based on those surveillance programs, the law and practice in the United States did not ensure "adequate protection" of his personal data.[22] In both cases, the CJEU agreed and held that the United States does not ensure adequate protection of EU data subjects' information.[23]

This Note explores the implications of *Schrems II*, as well as the practical difficulties thousands of companies across the United States and Europe now face in the continuation of their business. It examines the most compelling proposals to fix the immediate operational problem for companies engaged in cross-border data transfers, while also examining the need and advocating for practical adjustments to U.S. surveillance law that could provide much needed stability. To adequately address the redress issues raised in *Schrems II*, this Note proposes technical and operational recommendations, like encryption and SCCs, as a partial solution, while advocating for more substantive, yet pragmatic, legislative change in the United States.

Part I of this Note explores the landscape of governance mechanisms for cross-border data transfer under the GDPR. In this context, it examines the EU's principles and requirements, the mechanisms U.S. firms used to execute transfers in compliance, and the reasons the CJEU invalided the EU-U.S. Privacy Shield in *Schrems II*. Part II examines the precarious situation in which the decision leaves technology companies and presents potential proposals for how the companies and the U.S. may adapt to the decision. Part III advocates for pragmatic private-law solutions to enhance protections for data subjects and proposes a relatively narrow adjustment to the jurisdiction of the Foreign Intelligence Surveillance Court (FISC) to allow for appropriate redress under certain circumstances. Such a solution is most likely to adequately address the concerns articulated by the CJEU with minimal disruption to U.S. interests in foreign surveillance.

---

19. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015).

20. *See* Daniel Solove, *Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer*, TEACHPRIVACY (Oct. 13, 2015), https://teachprivacy.com/sunken-safe-harbor-5-implications-of-schrems-and-us-eu-data-transfer/ [https://perma.cc/ABB3-RQRV].

21. *See* Press Release, Ct. of Just. of the European Union, The Court of Justice Declares That the Commission's U.S. Safe Harbour Decision Is Invalid (Oct. 6, 2015), https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf [https://perma.cc/5KSA-X6AV]; *see also Schrems II*, C-311/18 ¶¶, 50–55.

22. *See* Press Release, *supra* note 21; *see also Schrems II*, C-311/18 ¶¶, 50–55.

23. *See* Press Release, *supra* note 21; *see also Schrems II*, C-311/18 ¶¶, 50–55.

I. PRINCIPLES OF EUROPEAN DATA PROTECTION AND THE U.S. SURVEILLANCE LANDSCAPE

To understand why the CJEU declared the EU-U.S. Privacy Shield to be inadequate under the GDPR's requirements, it is necessary to understand what those requirements are and how they relate to some basic provisions of the U.S. legal surveillance apparatus. This part will first describe the GDPR provisions that are relevant to cross-border data transfers and then explain why the CJEU determined U.S. laws do not meet the GDPR's requirements under EU law. Part I.A describes Europe's relevant fundamental principles and requirements for acceptable cross-border data transfer mechanisms under the GDPR. Part I.B discusses the relevant U.S. surveillance laws. Part I.C explains the *Schrems II* court's reasoning that the Privacy Shield does not satisfy the tension between U.S. surveillance laws and European data subjects' privacy rights and thus fails to meet the GDPR's requirements.

A. GDPR Data Requirements

The European Parliament enacted the GDPR in 2016 to account for the transformation of society and the economy through technological development and globalization, while ensuring a high level of personal data protection.[24] The GDPR permits cross-border data transfers only when those transfers are: (1) executed in accordance with an adequacy decision,[25] (2) implemented with other appropriate safeguards,[26] or (3) deemed necessary or as satisfying other circumstances to derogate from the approved mechanisms.[27]

Part I.A.1 outlines the GDPR's protections and the foundational European data protection principles on which the GDPR operates. Part I.A.2 explains the adequacy decision requirement and the European Commission's conclusion that the Privacy Shield met those requirements. Part I.A.3 examines acceptable mechanisms in the absence of an adequacy decision. Part I.A.4 explores the parameters that allow cross-border transfers without a prior European Commission decision.

1. An Overview of the GDPR and the EU's Foundational Principles

The GDPR provides data protections for subjects in the EU and the European Economic Area (EEA).[28] These protections include prohibiting

24. *See* GDPR, *supra* note 2, recital 6.
25. *See infra* Part I.A.2.
26. *See infra* Part I.A.3.
27. *See infra* Part I.A.4.
28. The EEA refers to the EU member states, plus three additional European nations (Norway, Lichtenstein, and Iceland) that are within the economic sphere. *See* Agreement Between the European Union, Iceland, Liechtenstein and Norway on an EEA Financial Mechanism 2014–2021, 2016 O.J. (L 141) 3. Under the EEA Agreement, EU legislation relating to the movement of goods, services, persons, and capital are applicable to the EU member states, as well as these three EEA nations. *See id.*

the transfer of personal data outside of the EEA, unless certain conditions providing appropriate protections are met.[29]

The protections are built on fundamental rights recognized by Europe in the Charter of Fundamental Rights of the European Union ("the Charter"),[30] which the Treaty of Lisbon[31] made legally binding on the EU in 2009.[32] The Charter contains rights pertaining to: dignity,[33] freedoms,[34] equality,[35] solidarity,[36] citizens' rights,[37] and justice.[38]

Most relevant to this Note (and the CJEU's *Schrems II* analysis) are the privacy rights under Articles 7 and 8, as well as the right to effective judicial redress in Article 47.[39] Article 7 articulates a broad respect for private and family life, stating "[e]veryone has the right to respect for his or her private and family life, home and communications."[40] Article 8 protects privacy with respect to one's personal data, stating "[e]veryone has the right to the protection of personal data concerning him or her" and that "[s]uch data must be processed fairly for specified purposes and on the basis of consent . . . or some other legitimate basis."[41] Article 47 expressly provides for the right to a "fair and public hearing within a reasonable time by an independent and impartial tribunal" for anyone whose rights and freedoms are violated.[42]

In addition, Article 52 states that any legal limitations placed on the rights and freedoms found in the Charter must, "[s]ubject to the principle of proportionality, . . . be made only if they are necessary and genuinely meet objectives of general interest."[43] Taken together, the Charter enshrines EU subjects' substantive and procedural rights, which may be limited for legitimate purposes, so long as those limitations "do not go beyond what is

29. *See* GDPR, *supra* note 2, art. 4450.
30. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.
31. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon].
32. *Why Do We Need the Charter*?, EUROPEAN COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en [https://perma.cc/R364-NQFL] (last visited Aug. 9, 2021).
33. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 396.
34. *See id.* at 397.
35. *See id.* at 399.
36. *See id.* at 401.
37. *See id.* at 403.
38. *See id.* at 405.
39. *Id.* art. 7, 8, 47.
40. *Id.* art. 7.
41. *Id.* art. 8.
42. *Id.* art. 47.
43. *Id.* art. 52(1).

necessary and proportionate in a democratic society."[44] These principles are part of the cultural and legal foundation on which the GDPR was built.[45]

The GDPR applies to any processing of EU subjects' personal data even if the controller or processor is located outside of the EU.[46] Therefore U.S.-based companies involved in the processing of EU subjects' data are governed by the GDPR's regulation.[47] This means U.S.-based companies are also subject to very large penalties for violations arising from improper cross-border data transfers. These penalties may amount to twenty million euros or up to 4 percent of a company's total worldwide revenue, whichever is greater.[48]

Enforcement of the GDPR falls primarily on the independent supervisory authorities, or Data Protection Authorities (DPA) of each of the member states.[49] However, the European Data Protection Board (EDPB), consisting of the heads of each of the DPAs, is the EU body in charge of enforcing the GDPR.[50] The EDPB issues enforcement guidelines, as well as binding rules, that facilitate consistency across the EU.[51]

The GDPR encourages stable and predictable mechanisms for data transfers like official adequacy decisions,[52] while also accepting SCCs, binding corporate rules, and other appropriate safeguards that may be sufficient in the absence of an adequacy decision.[53] The law also permits

---

44. EUROPEAN DATA PROT. BD., RECOMMENDATIONS 02/2020 ON THE EUROPEAN ESSENTIAL GUARANTEES FOR SURVEILLANCE MEASURES 4 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf [https://perma.cc/P8SH-VR5M]. While the EU member states themselves determine what is "necessary and proportionate" in the context of their own national security concerns, the CJEU determines what that means in the foreign context—in this case, as it applies to U.S. surveillance law. *See* Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation Is Just a Start*, BROOKINGS (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ [https://perma.cc/T53Y-QCTY]. Any discussion of hypocrisy or "dissonance between what the EU is expecting of other governments and what it is able to ask of its member states" is beyond the scope of this Note. Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, BROOKINGS (Aug. 5, 2020), https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ [https://perma.cc/S3GC-X5BM]. Instead, this Note intends to identify a clear and effective path forward for EU-U.S. cross-border data transfers based on the CJEU's binding decision in *Schrems II* without evaluating the validity of the decision.

45. *See* Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 395.

46. GDPR, *supra* note 2, art. 3.

47. *See id.*

48. *See id.* art. 83(5).

49. *See generally id.* ch. VI (outlining the independence, tasks, and powers of the supervisory authorities to monitor and enforce the GDPR).

50. *See id.* art. 63–76.

51. *See id.*

52. *See id.* art. 45. For a discussion on adequacy decisions, see *infra* Part I.A.2.

53. *See* GDPR, *supra* note 2, art. 46.

derogations in certain circumstances[54] and allows for some transfers out of necessity or with the data subjects' explicit consent.[55]

2. The Process of and Requirement for Adequacy Decisions

Article 45 of the GDPR permits cross-border data transfers that are executed pursuant to an "adequacy decision,"[56] the mechanism by which the Privacy Shield was approved.[57] An adequacy decision is a determination by the European Commission ("the Commission"), implemented by an act,[58] that a specific non-EU country, or specified entities or sectors within that country, provide adequate protection in accordance with the EU's protection principles.[59] If cross-border transfers are executed within the parameters of an adequacy decision, the transferring parties do not need to receive specific case-by-case authorization of the transfers by the appropriate member state's DPA.[60]

The Commission considers a number of factors when it assesses the adequacy of a third-party country's protections.[61] It considers "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data."[62] The Commission also contemplates the "existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject"[63] and any commitments the third-party country or organization has entered into "arising from legally binding conventions or instruments."[64]

3. "Appropriate Safeguards" in the Absence of an Adequacy Decision

Although the Privacy Shield was a preferred and efficient mechanism because of its official adequacy status, the GDPR also supports other legitimate mechanisms that permit cross-border transfers even to third-party countries or territories with inadequate protections not qualifying for an adequacy decision. Article 46 of the GDPR outlines several private-law safeguards or governance methods that could be used to authorize

54. *See infra* Part I.A.4.
55. *See* GDPR, *supra* note 2, art. 49.
56. *See id.* art. 45.
57. *See infra* Part I.C.1.
58. *See* GDPR, *supra* note 2, art. 45(3).
59. *See id.* art. 45(1).
60. *See id.*
61. *See id.* art. 45(2).
62. *Id.* art. 45(2)(a).
63. *Id.* art. 45(2)(b).
64. *Id.* art. 45(2)(c).

cross-border data transfers absent a Commission adequacy decision.[65] These include standard data protection clauses, which are also called SCCs.[66]

In 2010, the Commission approved twelve of these SCCs in its "SCC Decision."[67] The effect of the decision was that private controllers and processors would be allowed to "cut and paste" those SCCs into their individual contracts, thereby imposing approved data protection obligations on the parties when transferring data to third-party countries.[68] The SCC Decision was enacted prior to the introduction of the GDPR's enhanced protection language, and it was meant to address data transfers to third-party countries that did not provide an adequate level of protection.[69] Following the *Schrems II* decision, the Commission, to replace the outdated SCCs, enacted updated SCCs that incorporate a wider range of data transfer and processing activity consistent with the GDPR.[70] SCCs remain valid in principle following *Schrems II*, but it is not clear how practically valid they remain after the CJEU's reasoning for the invalidation of the Privacy Shield.[71]

---

65. *See id.* art. 46(1).

66. *See id.* art. 46(2)(c)–(d). Article 46 also permits other transfer tools such as binding corporate rules (BCR), *see id.* art. 46(2)(b), codes of conduct, *see id.* art. 46(2)(e), certification mechanisms, *see id.* art. 46(2)(f), or ad hoc contractual clauses, *see id.* art. 46(2)(a). All of the tools available under Article 46 are contractual in nature. Because SCCs were the focus of the CJEU's *Schrems II* decision and because the CJEU and EDPB require exporters to conduct the same analysis of the third-party country's legislation for any of the mechanisms under Article 46, this Note focuses on SCCs specifically, but it would be appropriate to apply the same reasoning to any of these other tools under Article 46. *See* EUROPEAN DATA PROT. BD., RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA, ¶¶ 23–24 (2d ed. 2021).

67. Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5 [hereinafter SCC Decision].

68. *See id.* recital 7. For example, clause 12 outlines the "Obligation after the termination of personal data-processing services" as:

> The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

Id. cl. 12.

69. *See id.* at 5–6, recitals 7–8; *see also* Daniel Solove, *The Impact of the Schrems II Decision: An Interview with Wim Nauwelaerts*, TEACHPRIVACY (Sep. 9, 2020), https://teachprivacy.com/the-impact-of-the-schrems-ii-decision-an-interview-with-wim-nauwelaerts/ [https://perma.cc/J9BP-GYBH] (explaining SCCs and BCRs were designed for the purpose of transferring data to "recipients in countries where the (privacy) laws do not ensure an adequate level of protection").

70. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31.

71. *See infra* Part I.C.3.

If parties utilize Article 46 SCCs, personal data may be transferred to a third-party country because those SCCs are the "appropriate safeguards" implemented by the contracting parties,[72] so long as the data subjects have "enforceable" rights and "effective legal remedies."[73] The mechanisms under Article 46, therefore, may provide an avenue for controllers and processors to engage in safe transfers of data to third-party countries—even when the Commission has not implemented an adequacy decision or when the parties are not a part of an approved adequacy decision framework.[74]

4. "Necessity" and Other Derogations for Certain Circumstances

Lastly, the GDPR carves out a number of instances in which data transfers may be permitted even without the protective safeguards outlined in Articles 45 and 46. These exceptions are known as "derogations."[75] The principal carve-outs most relevant to this Note are the provisions permitting transfer (1) when the data subject has explicitly consented to the transfer after being informed of the potential risks[76] and (2) if it is necessary to execute a contract between the data controller and data subject or if it is in the interest of the data subject.[77]

The Article 49 derogations are exemptions to the GDPR's central objective to ensure that personal data is only transferred to third-party countries if there is an adequate level of protection.[78] Thus, under a valid derogation, personal data may be transferred even where protections are inadequate. Because of this possibility, the EDPB advised that the derogations "must be interpreted restrictively so that the exception does not become the rule."[79] So, while the CJEU may have indicated some allowances under this provision,[80] which may provide the solution to companies following the *Schrems II* decision, the EDPB has reiterated the "exceptional nature" of Article 49 and asserted that the derogations must continue to be interpreted restrictively[81] and applied only to transfers that are "occasional and not repetitive."[82]

72. *See* GDPR, *supra* note 2, art. 46(2)(c).
73. *Id.* art. 46(1).
74. *See id.*
75. *Id.* art. 49.
76. *See id.* art. 49(1)(a).
77. *See id.* art. 49(1)(b)–(c). Data transfers are also permitted for the public interest, *see id.* art. 49(1)(d),(g), as part of a legal claim, *see id.* art. 49(1)(e), and when it is necessary to protect the subject's vital interest but the subject is unable to give consent, *see id.* art. 49(1)(f).
78. *See* EUROPEAN DATA PROT. BD., GUIDELINES 2/2018 ON DEROGATIONS OF ARTICLE 49 UNDER REGULATION 2016/679, at 4 (2018).
79. *Id.*
80. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 202 (July 16, 2020) (holding that a "legal vacuum" was unlikely to result from the court's decision because of the parameters outlined in Article 49); *see infra* Part II.B.3.
81. *See* EUROPEAN DATA PROT. BD., *supra* note 66, at 13.
82. *See* EUROPEAN DATA PROT. BD., *supra* note 78, at 4.

B. Relevant U.S. Surveillance Law

The CJEU's analysis of U.S. surveillance law[83] in *Schrems II* focuses on three pieces of law that are most relevant to cross-border data transfers: (1) Section 702 of the Foreign Intelligence Surveillance Act (FISA),[84] (2) Executive Order 12333 ("EO 12333"),[85] and (3) Presidential Policy Directive 28 (PPD-28).[86] A basic overview of the powers the intelligence community derives from these laws is helpful for understanding why the CJEU determined that the United States does not currently afford essentially equivalent protection to EU subjects.

Congress enacted FISA in 1978 to "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes."[87] The statute created a process for the government to obtain "ex parte judicial orders authorizing domestic electronic surveillance upon a showing that, inter alia, the target of the surveillance was a foreign power or an agent of a foreign power."[88] FISA also created the FISC, which is comprised of Article III district court judges who "hear applications for and grant orders approving electronic surveillance."[89]

FISA requires the government to obtain warrants or court orders for certain foreign surveillance activity.[90] The act also created the FISC so that the independent judiciary could review those requests and grant the orders when appropriate.[91] Such orders can direct electronic communications service providers to provide the public authority with access to the data that the provider has.[92]

FISA also requires the U.S. Attorney General to adopt "specific minimization procedures governing the retention and dissemination by the [government] of [information] received . . . in response to an order."[93] These procedures include strictly securing the data using secure networks and restricting use of that data only for the purposes approved by the court order.[94] Programs authorized under FISA are subject to oversight by the U.S. Department of Justice, the FISC, and Congress, as well as to audits and program reviews by the intelligence agencies' own internal privacy and civil liberties officers.[95]

---

83. *See infra* Part I.C.2.
84. 50 U.S.C. § 1881a.
85. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).
86. Press Release, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/UJM8-FRT3] [hereinafter Presidential Policy Directive].
87. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).
88. Klayman v. Obama, 957 F. Supp. 2d 1, 12 (D.D.C. 2013).
89. 50 U.S.C. § 1803(a)(1).
90. Am. C.L. Union v. Clapper, 959 F. Supp. 2d 724, 731 (S.D.N.Y. 2013).
91. *Id*.
92. *See id.*
93. 50 U.S.C. § 1861(g)(1).
94. *See* Am. C.L. Union v. Clapper, 785 F.3d 787, 797–98 (2d Cir. 2015).
95. *See id.*

EO 12333 does not compel companies involved in cross-border data transfers to provide U.S. public authorities with that data; however, it does permit U.S. public authorities to collect data extraterritorially, meaning data can be intercepted while in transit prior to arriving in the United States.[96] As they relate to surveillance programs relevant to this Note, activities conducted under EO 12333 are not governed by statute,[97] nor are they subject to judicial oversight.[98]

In 2014, the implementation of PPD-28 extended some protections of FISA and EO 12333 to non-U.S. persons.[99] PPD-28 states that intelligence activities should be "as tailored as feasible."[100] While the directive is binding on the intelligence community, it does not provide parameters or oversight mechanisms to enforce the tailoring of those intelligence activities.[101]

The existing oversight mechanisms that do cover parts of these laws are meant to hold the intelligence community accountable for its programs, but they do not allow individuals to challenge the public authorities' actions.[102] Only the recipient of an order to disclose data under FISA has the "right [to] judicial review of the order before the FISC."[103] However, that recipient must also keep the order a secret; recipients cannot disclose to anyone, including the subject of the data, their receipt of such an order.[104] Congress did not imagine that third parties, such as the subjects of the collected data, would ever *know* about the existence of the court orders, much less challenge their legality under the statute because of the deliberately secret nature of surveillance and the prohibition on disclosure.[105]

In a 2013 case concerning surveillance of U.S. persons that emerged in light of the Snowden revelations,[106] the U.S. Supreme Court stated that to

96. An example of interception while in transit would be capturing the data directly from underwater cables on the floor of the Atlantic Ocean, a tactic U.S. authorities employ under EO 12333. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 63 (Jul. 16, 2020).

97. *See id.*

98. *See id.* ¶ 65.

99. *See* Presidential Policy Directive, *supra* note 86, § 4.

100. *See id.* § 1.

101. *See Schrems II*, C-311/18, ¶ 181.

102. *See supra* text accompanying note 95; Am. C.L. Union v. Clapper, 785 F.3d 787, 797–98 (2d Cir. 2015).

103. Klayman v. Obama, 957 F. Supp. 2d 1, 13 (D.D.C. 2013).

104. *See id.*; *see also* 50 U.S.C. § 1861(d)(1) (stating that the recipient of an order to produce data may not "disclose to any other person that the [public authority] has sought or obtained" an order).

105. *See, e.g.*, H.R. REP. NO. 109-174, at 128, 268 (2005).

106. In 2013, Edward Snowden made classified NSA materials public, which led to more than 120 revelations about secret U.S. government surveillance programs. *Snowden Revelations*, LAWFARE, https://www.lawfareblog.com/snowden-revelations [https://perma.cc/Z2LM-M42J] (last visited Aug. 9, 2021) (cataloging all revelations that emerged from Snowden's disclosure to date). Among the most significant were the PRISM and UPSTREAM data collection programs, which were conducted according to FISA Section 702 and EO 12333 and which were the subject of much of the CJEU's analysis of U.S. surveillance law in *Schrems II*. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 61, 165, 179 (July 16, 2020); Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013, 3:23 PM),

establish standing, "an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[107] Further, the Court "reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[108] As it pertains to the questions presented in *Schrems II*, if EU data subjects do not know that their data has been improperly collected and, therefore, cannot show injury, then they will usually lack standing to challenge any action of the U.S. public authorities under FISA.[109]

To try to remedy this redress deficiency, the United States expanded the oversight role under PPD-28 to create an ombudsperson mechanism. The ombudsperson is a U.S. Department of State senior coordinator—at the level of under-secretary—who receives and addresses concerns about U.S. signals received by intelligence from foreign governments and who utilizes compliance review mechanisms under U.S. law to ensure proper remedies are granted.[110] But the response to complaints is limited and may only alert the individual that any noncompliance has been remedied, without more.[111]

Overall, the surveillance infrastructure under these three laws permits the United States to collect the personal data of EU subjects in bulk without the knowledge of those data subjects,[112] and it does not grant non-U.S. data subjects "actionable rights before the courts against the US authorities."[113]

C. Schrems II *Decision and Rationale*

Whether the third-party country's protections are "essentially equivalent to that ensured within the Union" is the consistent lodestar the Commission should consider when assessing the adequacy of extraterritorial data protections under the GPDR.[114] The law specifically highlights that the third-party country should have effective independent data protection supervision and that the data's subjects should be afforded administrative and judicial redress for violations of their data protection rights.[115] The CJEU emphasized these exact principles in its analysis of the Privacy Shield in *Schrems II*.[116] Understanding the court's reasoning explains why its

---

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/PLC4-WM9Z].

107. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).

108. *Id.* (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)) (alteration in original).

109. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 45 (July 16, 2020).

110. *See* Privacy Shield Decision, *supra* note 5, recitals 116, 120.

111. *See id.* recital 120.

112. *See Schrems II*, C-311/18, ¶ 183.

113. *Id.* ¶ 181.

114. GDPR, *supra* note 2, recital 104.

115. *See id.*

116. *See Schrems II*, C-311/18, ¶ 181 (holding that U.S. law supporting the Privacy Shield does limit the power of U.S. authorities to implement certain surveillance programs and, therefore, cannot ensure a level of protection "essentially equivalent" to that in the EU under the Charter). The Privacy Shield itself was a response to an earlier CJEU ruling in Case

declaration of the inadequacy of the Privacy Shield creates such a significant problem and vulnerability for companies that engage in cross-border data transfers from Europe to the United States, whether they used the Privacy Shield or the other mechanisms available, mainly SCCs.

First, Part I.C.1 describes how the Commission initially determined the Privacy Shield to be adequate under the GDPR. Part I.C.2 examines the CJEU's rationale for declaring the Privacy Shield to be inadequate. Part I.C.3 then highlights questions that have arisen over whether other GDPR data transfer mechanisms, like SCCs, can be implemented given the CJEU's conclusion that the U.S. government's surveillance abilities violate GDPR requirements, which operate independently of the individual companies' internal privacy and security policies.

1. The Commission's Prior Adequacy Decision

The Privacy Shield's status as the preferred data transfer mechanism was secured via an adequacy decision pursuant to Article 45 of the GDPR.[117] The principles presented in the Privacy Shield were developed by the Department of Commerce in consultation with the Commission.[118] The Privacy Shield consists of data privacy and security principles primarily concerned with notice, choice, security, subjects' right to access, recourse, and other principles that the Commission determined met the GDPR's requirements.[119] Upon self-certifying and committing to the principles and obligations of the Privacy Shield, participating companies were able to engage in cross-border data transfers based on a pre-authorized status[120]—a much more efficient process than case-by-case authorizations.

In the Privacy Shield adequacy decision, the Commission emphasized that FISA provides some remedies that are available to non-U.S. persons.[121] However, the Privacy Shield decision also acknowledged that it may be difficult for non-U.S. individuals to establish the standing required to pursue those remedies in U.S. courts.[122] To try to remedy this deficiency, PPD-28 created an ombudsperson mechanism, as discussed in Part I.B.[123]

Based on these assurances from the United States about compliance, the Commission determined that the United States ensured adequate data protection to organizations that were part of the Privacy Shield.[124] The

C-362/14, *Schrems I*, ECLI:EU:C:2015:650 (Oct. 6, 2015), which declared the previous Safe Harbor Framework inadequate based on similar principles applicable under the pre-GDPR regulation.

117. *See generally* Privacy Shield Decision, *supra* note 5.

118. *See id.* annex II.

119. *See id.*

120. *See id.* recitals 13–14.

121. *See id.* recital 112 (referring to the possibility of a civil cause of action for money damages against the United States or U.S. government officials in their personal capacities and challenging the legality of the surveillance in the event the United States plans to use the information gathered against the individual in proceedings in the United States).

122. *See id.* recital 115.

123. *See id.* recitals 116, 120.

124. *See id.* recital 136.

Commission also acknowledged that any interference with those protections by the U.S. public authorities for "national security, law enforcement or other public interest purposes" could be restricted to what was "strictly necessary" to achieve the legitimate public interest and could therefore be acceptable because of the aforementioned legal protections against such intrusions.[125]

2. CJEU's *Schrems II* Finding of Inadequacy

As discussed in Part I.B, the CJEU made its *Schrems II* determinations based on the same three U.S. legal instruments that the Commission considered when it initially made the Privacy Shield adequacy decision but arrived at the opposite conclusion.[126]

The CJEU determined that the Commission's adequacy decision[127] was improper because the United States does not ensure a level of protection for personal data that is essentially equivalent to that of the EU on two grounds.[128] First, U.S. surveillance laws are overbroad and do not meet the limited standards required under the GDPR and the principles of proportionality and necessity in the Charter.[129] Second, data subjects lack access to appropriate redress via judicial or tribunal remedies in the United States, as is required under the GDPR in accordance with the Charter.[130]

As the court highlighted with regard to its first point, and as the Commission acknowledged in its adequacy decision, Section 702 of FISA does not authorize individual surveillance.[131] Instead, Section 702 authorizes entire programs, and the FISC only approves the programs based on their relation to the goal of acquiring foreign intelligence information—not on the basis of properly targeting foreign individuals.[132] As such, FISA does not impose any limitations on the power it confers to execute broad surveillance or address any rights or remedies for non-U.S. persons potentially targeted by these broad surveillance powers.[133] Since Section 702 does not limit its scope, it cannot satisfy the principle of proportionality[134] and, therefore, cannot ensure a level of protection that is "essentially equivalent" with the EU's.[135]

Similarly, the court found that EO 12333 also "does not confer rights which are enforceable" against the United States in the courts[136] because that particular legal basis for U.S. surveillance lacks any judicial redress

125. *See id.* recital 140.
126. *See id.* recitals 67–135; Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 178–84 (July 16, 2020).
127. Privacy Shield Decision, *supra* note 5.
128. *See Schrems II*, C-311/18, ¶¶ 180–81.
129. *See id.* ¶ 180.
130. *See id.* ¶ 181.
131. *See id.* ¶ 179.
132. *See id.*
133. *See id.* ¶ 180.
134. *See id.* ¶ 176; *see also supra* note 43 and accompanying text.
135. *Id.* ¶ 180.
136. *Id.* ¶ 182.

mechanism.[137] Therefore, the CJEU concluded that these laws taken together with PPD-28 failed to provide the minimum safeguards that are required under EU law's principle of proportionality because the surveillance programs authorized under them cannot be "limited to what is strictly necessary."[138] Because of this failure, the CJEU concluded that the surveillance programs cannot be "essentially equivalent" to those that are found under EU law.[139]

The court maintained that, in assessing the possibility of individual remedies, the Commission relied too heavily on the parameters outlined in PPD-28, which limits intelligence activity to be "as tailored as feasible"[140] and specifically creates an ombudsperson within the role of the senior coordinator/undersecretary to liaise with foreign governments that may have concerns about U.S. "signals intelligence activities."[141] However, the creation of an ombudsperson under PPD-28 "does not grant data subjects actionable rights before the courts against the US authorities" and **"**cannot ensure a level of protection essentially equivalent to that arising from the Charter."[142] This is because Article 47 of the Charter establishes that anyone whose rights or freedoms are guaranteed by EU law has the right of an effective remedy via a hearing before an "independent and impartial tribunal."[143] The court determined that the ombudsperson did not meet this standard based on concerns about the ombudsperson's independence.[144] The court held that, because the ombudsperson is part of the U.S. State Department and is appointed by the U.S. Secretary of State, the subordinate relationship "undermine[s] the Ombudsman's independence from the executive."[145]

In addition, the ombudsperson is not part of the independent judiciary.[146] Therefore, because of the lack of rights actionable in U.S. courts against U.S. authorities, data subjects did not have an effective remedy as required by EU law.[147] For all these reasons, the CJEU concluded the Commission's prior Privacy Shield decision to be invalid, nullifying the entire Privacy Shield.[148]

3. A Lingering Question Concerning the Validity of SCCs

While the CJEU declared the Privacy Shield invalid, the court maintained the legitimacy of SCCs.[149] The CJEU held that the SCC adequacy decision

137. *See* Privacy Shield Decision, *supra* note 5, recital 115; *Schrems II*, C-311/18, ¶ 191.
138. *Schrems II*, C-311/18, ¶ 184.
139. *Id.* ¶ 185.
140. Presidential Policy Directive, *supra* note 86, § 1(d).
141. *Id.* § 4(d).
142. *Schrems II*, C-311/18, ¶ 181.
143. *Id.* ¶ 186 (citing Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) art. 47.
144. *See id.* ¶ 195.
145. *Id.*
146. *See id.*
147. *See id.* ¶ 197.
148. *See id.* ¶ 201.
149. *See id.* ¶¶ 131–32.

itself[150] does not require an assessment of any specific third-party country's data protection regime.[151] Instead, that responsibility to assess the adequacy of a third-party country's legal protections falls on controllers or processors involved in the transaction.[152]

The Commission's SCC decision contains an important footnote acknowledging that the recipient, or data importer, may have to comply with applicable national legislation that is "not in contradiction" with SCCs, so long as the national legislation does not go beyond what is "necessary in a democratic society . . . to safeguard national security."[153] The court left open the question of how exactly private data controllers and processors are to assess whether the legislation in the third-party country stops at what is "necessary in a democratic society."[154]

The court emphasized that SCCs, being inherently contractual, cannot bind public authorities in third-party countries because the authorities are not parties to the contract.[155] Of course, then, adequate legal protections for data subjects in third-party countries cannot be enacted via SCCs in a private contract.[156] Therefore, to ensure the level of protection required by the GDPR, controllers, processors, and data recipients may need to adopt "supplementary measures" as required to "ensure compliance with that level of protection."[157]

The court failed to elaborate on just what supplemental measures or additional safeguards private controllers could implement to ensure the appropriate level of data protection for European subjects.[158] Part II of this Note examines some proposed safeguards. However, without direction from the court, commentators note that it is unclear if any privately added safeguard can rectify the inadequacy of the data subject protections in the United States, particularly for the problem of a lack of a judicial remedy.[159]

The CJEU's analysis of U.S. surveillance law under the Privacy Shield decision is equally applicable to the use of SCCs for firms transferring private

150. *See generally* SCC Decision, *supra* note 67.
151. *See Schrems II*, C-311/18, ¶ 130.
152. *See id.* ¶ 134.
153. SCC Decision, *supra* note 67, cl. 5 n.1.
154. *Schrems II*, C-311/18, ¶ 141.
155. *See id.* ¶ 125.
156. *See id.* ¶ 132.
157. *Id.* ¶ 133.
158. *See* Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUROPEAN L. BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ [https://perma.cc/CH3X-MZ8S] (noting the court suggested "using 'supplementary measures' . . . to protect data under the SCCs, but d[id] not explain what measures these could be" (quoting *Schrems II*, C-311/18, ¶ 133)).
159. *See* Jennifer Daskal, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers*, JUST SEC. (July 17, 2020), https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/ [https://perma.cc/BA7S-TP25] (noting there is "nothing that companies can do to provide the kind of back-end judicial review that the Court demands").

data to the United States.[160] Therefore, one commentator notes that the court would hold that SCCs alone will not work for those transfers without additional provisions.[161] This remains the case as the updated SCCs also require exporters to assess the third-party country's surveillance laws and practices to determine what protections may be warranted.[162] Then the question is: What additional safeguards can data controllers and processors take, in practice, to ensure compliance with the level of protection mandated by EU law?[163]

II. PRACTICAL PATHS FORWARD IN THE POST-*SCHREMS II* LANDSCAPE

In *Schrems II*, the CJEU declined to allow the Privacy Shield to remain in place while a new solution was developed.[164] The court reasoned that a "legal vacuum" was unlikely in the wake of its decision because of the appropriate safeguards available under Articles 46 and 49 of the GDPR, which provide conditions defining when transfers may take place without an adequacy decision.[165] However, without concrete assurance from European authorities about what additional appropriate safeguards will be considered acceptable in accordance with Article 46 or about how necessity or consent principles from Article 49 could be utilized for ongoing activity, thousands of companies are currently trying to navigate their way through this confusing legal landscape.[166]

The questionable legitimacy of using SCCs to transfer data to the United States is especially troublesome because SCCs "were specifically designed to transfer personal data outside of the EEA, to recipients in countries where the (privacy) laws do not ensure an adequate level of protection."[167] As a result, companies and thought leaders are trying to find immediate practical solutions that will permit continued operations without business delays, as well as considering long-term structural reform to provide more stability and protection between the regions.[168] Part II.A outlines the regulatory guidance

160. *See* Daniel Solove, *Schrems II: Reflections on the Decision and Next Steps*, TEACHPRIVACY (July 23, 2020), https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/ [https://perma.cc/JYN3-F6XP] (noting that the "SCC don't really survive, at least not for the US" after *Schrems II* and that "the SCC cannot work as a means to transfer EU personal data to the US without some kind of additional protections against US government surveillance").

161. *See id.*

162. *See* Kenneth Propp, *Progress on Transatlantic Data Transfers?: The Picture After the US-EU Summit*, LAWFARE (June 25, 2021, 10:16 AM), https://www.lawfareblog.com/progress-transatlantic-data-transfers-picture-after-us-eu-summit [https://perma.cc/QJT3-A4AK].

163. *See Schrems II*, C-311/18, ¶ 137.

164. *See id.* ¶ 202.

165. *Id.*; *see supra* Parts I.A.3–4.

166. *See* Statement on Schrems II Ruling, *supra* note 10 (noting that more than 5300 companies relied on the Privacy Shield).

167. Solove, *supra* note 69 (describing this transfer scenario as the "raison d'être!" for SCCs and BCRs).

168. *See* Nick Clegg, *Securing the Long Term Stability of Cross-Border Data Flows*, FACEBOOK (Sep. 9, 2020), https://about.fb.com/news/2020/09/securing-the-long-term-

to date. Parts II.B and II.C then explore the proposed solutions that data exporters and recipients are implementing.

A. The EU and U.S. Regulatory Response to Schrems II

Immediately following the CJEU's decision in *Schrems II*, the EDPB issued guidance that emphasized the holding and stated that it would provide more guidance in the future.[169] In the interim, the EDPB did provide some basic guidance emphasizing the CJEU's holding that in order to utilize SCCs to transfer data to the United States, the data exporters and importers must make independent assessments regarding the adequacy of the data protection provided by the SCCs and provide necessary supplementary measures.[170] The board emphasized that it was "looking further into what these supplementary measures could consist of and will provide more guidance," but the board did not provide a timetable for that guidance.[171] In June 2021, nearly a year after *Schrems II* was decided, the EDPB issued final recommendations to European exporters.[172]

In the United States, the Department of Commerce issued guidance stating that while the Privacy Shield was invalid for the purposes of meeting GDPR standards, the obligations of the participants under the Privacy Shield were still intact.[173] The Department of Commerce explained that part of the purpose of maintaining the obligations and enforcement of the Privacy Shield was to allow organizations to demonstrate their "serious commitment to

---

stability-of-cross-border-data-flows/ [https://perma.cc/6XZY-ASRY]; Marc Zwillinger et al., *Supplementing SCCs to Solve Surveillance Shortfalls*, ZWILLGEN (June 10, 2021), https://www.zwillgen.com/international/supplementing-sccs-solve-surveillance-shortfalls/ [https://perma.cc/DDZ5-8777].

169. Press Release, EDPS Statement Following the Court of Justice Ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II") (July 17, 2020), https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en [https://perma.cc/99W2-L697].

170. *See* EUROPEAN DATA PROT. BD., *supra* note 11, at 1, 3, 5.

171. *Id.* at 5.

172. *See generally*, EUROPEAN DATA PROT. BD., *supra* note 66. The EDPB issued draft guidance in November 2020 and solicited comments from the public through December 21, 2020, which were considered for the final recommendations that were published in June 2021. *See Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUROPEAN DATA PROT. BD., https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en [https://perma.cc/XUB9-NPY2] (last visited Aug. 9, 2021). The analysis in this Note is based on the June 2021 recommendations, as those recommendations are the most recent guidance available. *See* EDPB Adopts Final Version of Recommendations on Supplementary Measures, Letter to EU Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro, and Designates Three EDPB Members to the ETIAS Fundamental Rights Guidance Board, EUROPEAN DATA PROT. BD (June 21, 2021), https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en [https://perma.cc/CG72-XNCZ].

173. *See* Statement on Schrems II Ruling, *supra* note 10.

protect personal information" in a way that offers "meaningful privacy protections and recourse for EU individuals."[174]

The Department of Commerce and the Commission confirmed that the institutions have initiated discussions to explore the potential for an enhanced Privacy Shield to comply with the needs emphasized in *Schrems II*.[175] However, it remains unclear when such an agreement could happen.[176] As Professor Daniel Solove highlights, based on the CJEU's reasoning, any new framework would involve at least some changes to U.S. surveillance law to accommodate for the current deficiencies.[177]

In addition, the Department of Commerce, the Department of Justice, and the U.S. Office of the Director of National Intelligence jointly issued a white paper emphasizing that, for the vast majority of parties, U.S. intelligence authorities are not interested in the data they transfer or collect.[178] The white paper provides an "up-to-date and contextualized discussion" of the relevant U.S. intelligence surveillance laws that companies relying on SCCs can use in their own assessments.[179] That discussion provides support for companies to take a risk-based approach to their cross-border data transfers by articulating that the overwhelming majority of transfers are of no interest to the U.S. intelligence agencies and that most companies have never received an order for data under FISA 702.[180]

In the final draft guidance, the EDPB may indicate openness to such a risk-based approach.[181] The recommendations are meant to provide exporters with steps to follow to assess whether a third-party country's laws may impinge on the data subjects' rights,[182] and if so, potential supplemental

174. *FAQs–EU-U.S. Privacy Shield Program Update*, PRIV. SHIELD FRAMEWORK (Mar. 31, 2021), https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update [https://perma.cc/46CQ-BVPE].

175. *See* Statement on Schrems II Ruling, *supra* note 10.

176. *See* Propp, *supra* note 162 (highlighting the generic statements and the hope that there will be some agreement by the end of 2021).

177. *See* Solove, *supra* note 160 (noting any new framework would have to "provide a lot of limitations on government surveillance involving EU personal data, plus a right to pursue remedies in court"); *see also* Propp, *supra* note 162 (emphasizing the sides remain "far apart" on the lack of independent oversight and redress available in the United States).

178. *See* U.S. DEP'T OF COM. ET AL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER *SCHREMS II* 1 (2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [https://perma.cc/Q24L-E3KY].

179. *Id.*

180. *See id.* at 2–3 (explaining that businesses would have no basis on which to believe that U.S. intelligence agencies would seek to collect data from transfers involving ordinary business activity like "employee, customer, or sales records" and adding that "[i]ndeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies").

181. *See* Theodore Christakis, *"Schrems III"?: First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 2)*, EUROPEAN L. BLOG (Nov. 16, 2020), https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ [https://perma.cc/4HMY-D6YD].

182. *See* EUROPEAN DATA PROT. BD., *supra* note 66, at 3.

measures[183] that they may choose to implement so that the protection is essentially equivalent to that of the EU.[184]

In this guidance, the EDPB advises that if an exporter still wishes to proceed with a data transfer to a country lacking legislation clearly governing the circumstances in which public authorities may access the data, then those exporters may consider the "practices of the third country's public authorities" to help determine if the safeguards will sufficiently protect the personal data transferred.[185] Therefore, to inform what supplemental measures, if any, may be used, the EDPB appears to be amenable to an exporter's assessment, considering not only the rights and laws that exist but also the discretion that the public authorities of the third-party country may exercise in enforcing the laws.[186]

The EDPB's guidance proposes supplemental measures that exporters and importers may choose to implement to establish essentially equivalent protections for data subjects.[187] However, the guidance reiterates that it is exporters' duty to perform an assessment of the protections in the third-party country and implement appropriate protections.[188] The EDPB's guidance is meant to clarify the process for European exporters,[189] but it does not make any conclusions about which, if any, of the supplemental recommendations may be used to establish the required level of data protection for transfers from the EU to the United States.[190]

The result is that the main regulatory authorities on both sides of the Atlantic have made it very clear that the Privacy Shield is not valid for GDPR compliance, but the regulatory authorities lack a viable replacement solution. Without an official adequacy decision under Article 45, private entities must determine the level of protection in a third-party country and then determine and implement measures that they believe will provide essentially equivalent data protections.

183. *See infra* Part II.B.

184. *See* EUROPEAN DATA PROT. BD., *supra* note 66, at 3.

185. *Id.* ¶ 43.

186. *See id.* ¶ 43.3.

187. *See generally id.*

188. *See id.* at 3 (emphasizing the CJEU's holding in *Schrems II* that "controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the [GDPR transfer mechanism]").

189. *See id.* (stating "[t]hese recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place").

190. The EDPB's guidance merely states that when identifying and implementing a supplemental measure, the exporter "may ultimately find that no supplementary measure can ensure an essentially equivalent level of protection for [the exporter's] specific transfer," thereby avoiding any conclusory holdings that any of the suggested recommendations may ensure adequate data protection. *Id.* at 4.

B. Addressing the Reach of U.S. Surveillance

Schrems II articulated that the existing surveillance systems in the United States do not allow European data subjects to enjoy protection that is essentially equivalent to that which is available in the EU.[191] However, it also clearly articulated that private parties may be able to implement supplemental measures that, in practice, may provide adequate protection.[192] Yet, such private obligations do not bind the public authorities in the respective third-party country.[193]

Because the regulatory bodies in the EU and United States are unable to quickly resolve the misalignment between fundamental rights in the EU and surveillance law in the United States, private entities are forced to find alternative bases or methods for transferring personal data from Europe to the United States to continue their operations with minimal interruption. The technological enhancements, additional contractual provisions, or use of a different mechanism entirely in the EDPB's draft recommendations, all utilize private law to attempt to avoid the overbroad reach of U.S. surveillance law and provide essentially equivalent protection, as required by the GDPR.[194]

Parts II.B.1 and II.B.2 consider, respectively, the technological and organizational changes that companies are implementing as legal solutions to mitigate risk of personal data being captured by U.S. intelligence agencies. Part II.B.3 assesses the utilization of consent and necessity derogation methods under Article 49 as a means to transfer data to the United States. Part II.B.4 explores contractual legal supplements that attempt to enhance compliance closer to the GDPR's requirements.

1. Encryption

Perhaps the most immediately actionable protection companies can take to enhance their SCCs is the utilization of robust encryption when personal data is transferred to U.S. firms. Such technical measures can make accessing data more difficult, in practice, for public authorities in the United States.[195] Even if the authorities do access the data, tokenization could render the data meaningless to those other than the controller and recipient—and may be more helpful.[196]

---

191. *See supra* Part I.C.2.
192. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 133–34 (July 16, 2020).
193. *See id.* ¶¶ 125, 132.
194. *See generally* EUROPEAN DATA PROT. BD., *supra* note 66.
195. *See* Solove, *supra* note 69.
196. *See* Ruth Boardman & Ariane Mole, Schrems II*: Privacy Shield Invalid, SCCs Survive. What Happens Now?*, INTELL. PROP. & TECH. L.J., Sept. 2020, at 3, 6 (2020). Tokenization is the process of turning a piece of data into a random string of characters called a token that has no meaningful value if breached because there is no key that can be used to derive the original date, unlike encryption which uses a mathematical process to transform the sensitive information into the encrypted data. *See Tokenization vs Encryption*, MCAFEE, https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/tokenization-vs-

These technical measures change the personal data such that it is useless if breached and so may be employed as a legal solution to provide effective protection against intelligence authorities' ability to access the data. The EDPB's final recommendation provides guidance regarding technical measures, including data encryption or pseudonymization,[197] and when they may or may not provide sufficient supplemental protection.[198] According to that guidance, the potential suitability of technical measures hinges on whether the public authorities in third-party countries will be able to identify or know information about the specific data subjects.[199] The EDPB's recommendations are meant to be applicable[200] whether the public authority in the third-party country accesses the data from the lines of communications themselves[201] (similar to how U.S. authorities access data in accordance with EO 12333)[202] or if the intended data importer is required to turn the data over to the authorities[203] (similar to the obligations of electronic communications providers under Section 702 of FISA).[204]

The EDPB outlined five use cases where the technical measures employed may provide adequate protection.[205] In four of the five adequate scenarios, the technical measures are deemed adequate because the processor or importer in the third-party country has access to neither the unprotected data nor the keys needed to unprotect the data in order to perform its processing task.[206] These four scenarios are: (1) when an exporter stores encrypted data in the third-party country for backup or other purposes, but the importer does not need to access that data "in the clear" (i.e., unencrypted, not pseudonymized, decryption keys transported to the importer or a vulnerable party);[207] (2) where pseudonymized data is transferred to the importer for analysis but without the information necessary to attribute the data to specific subjects;[208] (3) when the data is accessible by public authorities while in transit;[209] and (4) when the processing of the data is split or among multiple parties in different jurisdictions.[210] In each of these scenarios neither the unencrypted or de-pseudonymized data nor the keys to unencrypt or

encryption.html [https://perma.cc/X26H-HM7T] (last visited Aug. 9, 2021). The technical details of encryption and tokenization are beyond the scope of this Note.

197. Pseudonymization means the processing of personal data such that it can no longer be attributed to a specific data subject on its own without additional information, which is kept separately so the data is not attributable to an identifiable person. GDPR, *supra* note 2, art. 4(5).

198. EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 77.

199. *See id.* ¶ 79.

200. *See id.* ¶ 81.

201. *See id.* ¶ 80(a).

202. *See supra* Part I.B.

203. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 80(b).

204. *See supra* Part I.B.

205. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶¶ 84–92.

206. *See id.*

207. *Id.* ¶ 84.

208. *See id.* ¶ 85.

209. *See id.* ¶ 90.

210. *See id.* ¶ 92.

de-pseudonymize the data are accessible to the public authorities. The fifth use case occurs when the data importer is specifically protected by the third-party country's laws, such that the importer is protected from having to disclose the personal data to the public authorities.[211] If that is the case, the importer may have the decryption key but must still make sure to use state of the art end-to-end encryption and/or pseudonymization so that the public authorities cannot access the sensitive data in transit.[212]

Therefore, the EDPB determination of legal adequacy based on technical measures appears to be based primarily on the secured or unsecured nature of the data when in the third-party country. If (1) the data is encrypted or pseudonymized prior to transfer, (2) the decryption keys are not transferred to the importer or any vulnerable party within the third-party country, and (3) the encryption is state-of-the-art such that the public authorities in the third-party country would not be able to determine any personal information about the protected data subjects, then the EDPB is likely to consider the technical action an effective supplemental measure, under the GDPR, that the exporter could contract for and implement to execute cross-border data transfers.[213]

Conversely, if (1) the importer/processor in the third-party country requires access to the data "in the clear" in order to execute its task, (2) the laws of the third-party country that grant public authorities to the transferred data go "beyond what is necessary and proportionate in a democratic society,"[214] and (3) the laws are applied in practice to the transfers in question, then the EDPB is "incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights."[215] As the EDPB emphasizes, in scenarios where unencrypted personal data of EU data subjects are technically necessary for the importer to execute its tasks, any level of encryption will not be an effective supplementary measure capable of "ensur[ing] an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys."[216]

Professor Theodore Christakis explains that the EDPB's use cases from the earlier draft recommendations suggest that the transfers will be accepted "only if the data are rendered non-readable for the importer in the recipient country."[217] The EDPB's explanation of two situations where technical measures would likely not be acceptable emphasizes the strict acceptability of technical measures alone.[218] The first suggests that an exporter could not use a cloud service provider to process data in a third-party country, while the second considers that an exporter could not make personal data available

211. *See id.* ¶ 91.
212. *See id.*
213. *See id.* ¶¶ 84, 85, 90, 92.
214. *See id.* ¶¶ 94(3), 96(3).
215. *Id.* ¶¶ 94, 96.
216. *Id.* ¶¶ 95, 97.
217. *See* Christakis, *supra* note 181.
218. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶¶ 93–97.

to parties in a third-party country, such as a "branch of the same company or subcontractors," to be utilized for a shared business purpose.[219] As Professor Omer Tene highlights, the lack of acceptability for these two scenarios may not solve the problem as much as they add to it because they "account[] for the vast majority of real world transfers."[220]

These analyses were conducted based on the draft recommendations, not the final recommendations published in June 2021. The major development is that the EDPB's final guidance permits exporters to consider how the law or authority impacts the transfer *in practice* as part of its assessment.[221] That could lead those exporters to conclude that while the laws of the third country violate EEA principles, they do not affect this transfer in practice and the supplemental measures may thus be permissible.[222]

Therefore, technical measures may constitute a supplementary measure that ensures the adequate level of protection as required by EU law under certain circumstances, but companies may have to bolster those supplementary measures with other mechanisms to reinforce the protections.

2. Data Localization

Another potential solution is to avoid the transfers altogether by localizing data storage exclusively in Europe.[223] If no data transfer occurs, then firms do not need to utilize an adequate mechanism; however, it has been suggested that, while the solution may appear to be adequate in the short term, this idea likely is not compatible with the global needs of firms who transfer data anyway.[224]

One commentator, Professor Anupam Chander, explains that, practically speaking, localizing data fails to actually keep data local.[225] Data transfers happen on such a large global scale because businesses operate on a global scale.[226] Therefore, even if EU data is stored and maintained in Europe, customer service representatives based outside of the EU will still be able to access that data; similarly, if Facebook stores an EU subject's profile on servers in Ireland, peers in the United States and elsewhere will still be able to access the profile.[227] In addition, because the internet is international, an EU subject accessing EU-stored data may attain that access after being routed

219. *See* Christakis, *supra* note 181 (referring to the scenarios in the earlier draft EDPB Recommendations of 2020, which are copied nearly verbatim in the final version discussed in this Note).

220. Omer Tene, *Quick Reaction to EDPB Schrems II Guidance*, LINKEDIN (Nov. 12, 2020), https://www.linkedin.com/pulse/quick-reaction-edpb-schrems-ii-guidance-omer-tene [https://perma.cc/9K9Z-TQZ9].

221. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 30.

222. *See id.* at 20–21.

223. *See* Solove, *supra* note 160 (suggesting one path forward is for companies to "try to keep the data in the EU").

224. *See generally* Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771 (2020).

225. *See id.* at 781–82.

226. *See id.*

227. *See id.* at 781.

through the United States, or elsewhere, so cross-border data transfers still occur.[228] Jurisdictions could erect systems or firewalls to avoid such routing, but that would substantially increase costs for internet access generally, reducing the value of the service overall.[229]

Second, there are legitimate questions about whether localization would align with the purpose of the *Schrems II* decision. The court ruled that existing transfers to the United States were not permitted because U.S. surveillance law fails to provide adequate protection for EU subjects.[230] But U.S. surveillance also occurs outside of the geographical boundaries of the United States and is less restrained abroad.[231]

Despite these potential shortcomings, some companies started to use localization in the aftermath of the decision.[232] For example, France's health data hub has not only moved to data localization but also discontinued using Microsoft's cloud service (which could still operate in the EU) to avoid being subject to U.S. surveillance law under Section 702 of FISA.[233]

3. Necessity or Consent

In *Schrems II*, the CJEU indicated that Article 49 of the GDPR provides at least a short-term solution for companies that rely on the legitimacy of transferring personal data from Europe to the United States.[234] The two potentially relevant avenues available under Article 49 are necessity or consent.[235] Part II.B.3.a and Part II.B.3.b discuss necessity and consent as possible justifications for data transfers.

---

228. *See id.* at 782.

229. *See id.*

230. *See supra* Part I.C.

231. 50 U.S.C. §§ 1881–1885c; Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 714–18 (2015). Also, while comparisons of the U.S. surveillance rules to those of other countries are beyond the scope of this Note, it is worthwhile to recognize that many European countries like the United Kingdom, Sweden, France, Germany, and the Netherlands all have robust surveillance operations in Europe, so localizing the data may not even solve the underlying concern of improperly protected surveillance. *See* Chander, *supra* note 224, at 778.

232. Indeed, prior to the EDPB's general guidance in November 2020, German DPAs advised exporters in that member state that data encryption with key localization was likely the only way to comply with the *Schrems II* holding. *See* Annette Demmel & Mareike Lucht, *German DPA Issues Guidance on Schrems II and the Transfer of Personal Data to Non-EU Countries*, NAT'L L. REV. (Sep. 23, 2020), https://www.natlawreview.com/article/german-dpa-issues-guidance-schrems-ii-and-transfer-personal-data-to-non-eu-countries [https://perma.cc/2FQA-XETR].

233. Romain Dillet, *France's Health Data Hub to Move to European Cloud Infrastructure to Avoid EU-US Data Transfers*, TECHCRUNCH (Oct. 12, 2020, 1:48 PM), https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers/ [https://perma.cc/5DYM-53BK].

234. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 202 (July 16, 2020) (stating that a "legal vacuum" was unlikely to result from the court's decision because of the parameters outlined in Article 49).

235. *See supra* notes 76–77 and accompanying text.

a. Seeking Legitimacy by Necessity

Since the *Schrems II* decision, Facebook has adopted the necessity approach after being notified by Ireland's Data Protection Commission to stop using SCCs.[236] In response to an inquiry from NOYB (a consumer privacy advocacy group initiated by Maximillian Schrems)[237] about if and how Facebook transfers user data outside of the EU, Facebook said the legal basis for doing such transfers was that they were "necessary to provide [Facebook's] contractual services."[238] Therefore, it appears that since the *Schrems II* decision, Facebook now relies on Article 49 of the GDPR as the legal basis for its cross-border data transfers, despite the fact that previous EDPB guidance stated that necessity cannot be used for systemic transfers, only "occasional" transfers.[239] It is accepted, however, that actions like booking a flight or hotel in the United States or sending an email to the United States would be derogations for necessity.[240] So then, Professor Chander questions whether communicating with peers in the United States via Facebook is a similar activity that could be justified by the same reasoning?[241] That question remains unanswered, but Professor Chander emphasizes the EDPB's guidance, which reiterates that Article 49 transfers, including necessity, are "narrowly construed."[242]

b. Seeking Legitimacy by Consent

Obtaining data subjects' consent to transfer their data is the other avenue presented by Article 49 that seems viable for some businesses. However, Professor Chander notes that the burden for consent is quite high under the GDPR.[243] First, consent from the subject must be "specific, informed, and unambiguous."[244] The subject must also be able to withdraw her consent at any time.[245] Second, the costs of acquiring such complete and adequate

236. *See* Clegg, *supra* note 168 (stating that Ireland's Data Protection Commission "has suggested that SCCs cannot in practice be used for EU-US data transfers").

237. *Our Detailed Concept*, NOYB, https://noyb.eu/en/our-detailed-concept [https://perma.cc/4AXL-ESYH] (last visited Aug. 9, 2021).

238. NOYB, OPENING PANDORA'S BOX: HOW COMPANIES ADDRESSED OUR QUESTIONS ABOUT THEIR INTERNATIONAL DATA TRANSFERS AFTER THE CJEU'S RULING IN C-311/18–SCHREMS II 18 (2020), https://noyb.eu/files/web/Replies_from_controllers_on_EU-US_transfers.pdf [https://perma.cc/4SSY-Q28P].

239. EUROPEAN DATA PROT. BD., *supra* note 78, at 9; EUROPEAN DATA PROT. BD., *supra* note 11, at 4.

240. *Next Steps for Users & FAQs*, NOYB (July 24, 2020), https://noyb.eu/en/next-steps-users-faqs [https://perma.cc/6XUH-9UZZ].

241. Chander, *supra* note 224, at 776.

242. *Id.*

243. *Id.*

244. *See* GDPR, *supra* note 2, art. 4(11).

245. *See International Transfers After the UK Exit from the EU Implementation Period*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ [https://perma.cc/UNC7-GFE2] (last visited Aug. 9, 2021).

consent from every applicable data subject will be quite high.[246] Third, while there is some basis for the assertion that consent, unlike necessity, may be used for repeated, ongoing transfers,[247] that theory has also been refuted by earlier EDPB direction[248] and reiterated by subsequent EDPB guidance.[249]

If either of these Article 49 derogations are acceptable, questions about the scope of their applicability are still open because they are likely to be more suitable for consumer-facing companies executing direct transactions with consumers, rather than any company that deals in cross-border data transfers.

4. Supplemental Clauses

While the *Schrems II* court did not specify what "additional safeguards" companies could implement when they determine the protections of a third-party country are insufficient,[250] some companies are providing supplemental contractual provisions (in addition to the new SCCs) that attempt to counter specific deficiencies.[251] Indeed, the EDPB's final June 2021 recommendations assess a number of supplemental contractual provisions that may provide adequate supplemental measures,[252] including transparency disclosure obligations,[253] technical protections or procedural challenges,[254] and opportunities to empower the data subjects to enforce their rights.[255]

A core issue of *Schrems II* was the public authorities' access to data. Since the authorities are not bound by contractual terms, it is difficult to see how additional terms that only bind the contracting parties and not the authorities would be useful.[256] Therefore, the EDPB advises that private contractual obligations would likely need to be combined with other technical or organizational solutions in order to be considered adequate measures.[257] For example, additional contractual provisions will not rule out the possible application of FISA Section 702, which may oblige an electronic communications provider or importer in the United States to comply with orders to disclose data it receives to the public authorities.[258] Because the

246. *See* Chander, *supra* note 224, at 776.

247. Stéphanie Faber, *Does the GDPR Allow for the Use of Consent for the International Transfer of Data?*, NAT'L L. REV. (Jan. 7, 2019), https://www.natlawreview.com/article/does-gdpr-allow-use-consent-international-transfer-data [https://perma.cc/LXN5-RSNM].

248. *See generally* EUROPEAN DATA PROT. BD., *supra* note 78.

249. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 25.

250. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 134 (July 16, 2020).

251. *See* Zwillinger et al., *supra* note 168 (explaining that ZwillGen, a Washington, D.C.-based law firm that specializes in data-related legal questions, has worked with clients to implement supplemental clauses following the *Schrems II* decision).

252. *See* EUROPEAN DATA PROT. BD., *supra* note 66, at 36–43.

253. *See infra* Part II.B.4.a.

254. *See infra* Part II.B.4.b.

255. *See infra* Part II.C.1.

256. *See* Boardman & Mole, *supra* note 196, at 6.

257. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 99 (citing *Schrems II*, C-311/18 ¶ 125).

258. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 101 (citing *Schrems II*, C-311/18, ¶ 132).

EDPB's recommendations are for exporters assessing transfers to third-party countries generally and not specifically for data transfers moving from the EU to the United States,[259] it is critical to determine if the recommendations can be utilized so that those transferring data to the United States can do so while providing data protection essentially equivalent to that of the EU.

Even so, additional contractual measures recommended by the EDPB can create enhanced obligations that may be used to help establish protections that are essentially equivalent to those of the EU. Part II.B.4.a examines potential transparency obligations.[260] Part II.B.4.b analyzes potential obligations for the importers to take specific actions[261] or use specific technical measures.[262] Then, Part II.B.4.c considers recommendations that may empower data subjects to exercise rights to redress.[263]

a. Transparency Obligations

The EDPB recommends several potential contractual terms that would require importers to disclose to exporters, based on their best efforts, the public authorities' access to data.[264] Such proactive disclosure would help the exporter with its task of assessing the level of protection in the third-party country.[265]

The information to be disclosed could include the laws and regulations of the third-party country that would permit public authorities' access and define the scope of that access.[266] These terms could also require importers to disclose any and all requests that they may have previously received from public authorities seeking access to the relevant data and to disclose how they complied.[267] In addition, the exporter may seek to include clauses where the importer certifies it has not deliberately created "back doors" that could be used by the public authorities to access data and that the law does not require them to create any mechanisms that would facilitate such access for the public authorities.[268] These additional contractual protections, which limit the risk of U.S. public authorities that actually acquire the personal data, may satisfy the essentially equivalent protection requirement of the GDPR.[269]

Unlike FISA Section 702, EO 12333 does not have the authority to compel companies involved in cross-border data transfers to provide U.S. public

259. *See generally* EUROPEAN DATA PROT. BD., *supra* note 66.
260. *See id.* at 37.
261. *See id.* at 40.
262. *See id.* at 36.
263. *See id.* at 42.
264. *See id.* ¶ 105.
265. *See id.*
266. *See id.* ¶ 106(1).
267. *See id.* ¶ 106(4).
268. *See id.* ¶ 109.
269. *See* Zwillinger et al., *supra* note 168 (asserting that the essential equivalence standard is consistently assessed under the GDPR based on a risk-based approach, like in Article 32 and Article 25).

authorities with that data.[270] Instead, cooperation by any private company under the executive order is purely voluntary.[271] Therefore, U.S. companies can make contractual promises about how they will or will not assist the U.S. government with surveillance.[272] Promising not to assist under EO 12333 could provide some assurance to the EU party of enhanced data protection.

FISA Section 702, however, does provide some authority to compel a U.S. company's cooperation.[273] However, even that authority may be limited by contractual assurances. First, not all data operators are eligible to receive such a directive from the U.S. government compelling disclosure of the relevant personal data; only electronic communication service providers can receive such a command.[274] Therefore, many U.S. data importers could provide contractual assurances to the EU exporter of their ineligibility and provide assurances that any such directive would be fought to the fullest extent possible.[275]

If an importer is an electronic communication service provider, it may still achieve essentially equivalent protection by making assurances that it has never been issued such a directive (as appears to be the case for the majority of firms)[276] and that even if such a directive is issued, it will use any and all available judicial mechanisms to fight that directive.[277] Further, if it has complied with a directive, the importer could promise to include the number and volume of affected users in transparency reports that can be made available to the EU firm. The EU firm could then compare that information to the total volume of users' data it exports, enabling it to make an informed risk assessment that could justify the continued transfers.[278]

Alternatively, rather than relying on the importers' assurances, exporters may seek access to the importers' processing logs to determine for themselves if any data has been disclosed to public authorities.[279] Such audits were already permitted under the earlier SCCs between controllers and processors[280] or could be executed via alternative Article 46 mechanisms like certification or a code of conduct.[281]

The EDPB's final transparency recommendation is a contractual measure that establishes a "warrant canary."[282] This term would commit the importer

270. *See supra* Part I.B.

271. *See* Zwillinger et al., *supra* note 168 (highlighting that EO 12333 "provides no mechanism for forcing importers to assist the government").

272. *See id.* (explaining that "importers can contractually commit to not voluntarily assist the government in conducting operations under EO 12333").

273. *See* 50 U.S.C. § 1881a.

274. *See* Zwillinger et al., *supra* note 168.

275. *See id.*

276. *See id.* (highlighting that at the time of the Snowden revelations, it was reported that fewer than 10 companies were receiving such Section 702 orders).

277. *See id.*

278. *See id.*

279. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 111.

280. SCC Decision, *supra* note 67, cl. 5(f).

281. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 111 n.96.

282. *See id.* ¶ 116.

to publishing regularly (perhaps at least daily) a "cryptographically signed message" to the exporter that, as of that date and time, the importer has not received any request or order for protected data.[283] Under such a scheme, the absence of this message could indicate to the exporter that the situation has changed.[284] In order for this to be effective for transfers to the United States, the critical question is whether FISA's prohibition on disclosure would apply such "passive notification."[285] It is not clear whether such an action would constitute improper disclosure under Section 702.

No matter what transparency clauses may or may not be effective for transfers to the United States, it is likely necessary that they also include obligations for importers to take certain actions with respect to protecting the transferred data.

b. The Obligation to Take Specific Actions

In addition to providing mechanisms for importers to disclose any access public authorities have gained, the parties could institute contractual measures to ensure actions on the part of the importer. Should the parties find technical measures are warranted,[286] the contract should indicate which measures are required for the transfers to take place[287] so that both parties commit to the supplemental measure.[288] In the event that an importer in the United States is eventually served with an order to disclose data to the public authorities, the importer may commit to challenge complying with the order to the best of its ability.[289]

C. Addressing Individual Redress in the United States

While the EDPB and private industry recommend and utilize what they believe are permissible supplemental measures that limit the accessibility of one's data to what is necessary and proportionate as required under EU law, the second prong of the CJEU's reason for finding inadequacy—the lack of individual redress before an independent body—must also be addressed. This part assesses two main avenues that have been proposed to remedy that deficiency. Part II.C.1 briefly examines the EDPB's proposed private contractual solutions meant to enable the individual to exercise his or her rights. Part II.C.2 examines a proposal to make a moderate modification to FISA to provide a mechanism for individual redress before an independent judiciary.

283. *See id.*
284. *See id.*
285. *See id.* ¶ 117.
286. *See supra* Part II.B.1.
287. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 103.
288. *See id.* ¶ 104.
289. *See id.* ¶ 118.

1. Empowering Data Subjects to Exercise Rights

In addition to the supplemental measures explored in Part II.B, which may be employed to mitigate the risk of public authorities gaining access to subjects' data,[290] the EDPB's final recommendations from June 2021 include measures that may assist the data subjects in exercising their rights to redress.[291] These measures include obligations for the importer and/or exporter to notify the data subject when public authorities of a third-party country request or order access to their data or when the importer can no longer comply with the contractual commitments protecting the data for whatever reason.[292] They also include committing to assist the data subject in their exercise of their rights in the third-party country, so long as the country provides for redress.[293] The effectiveness of both of these measures depends on the rights to redress in the third-party country and the importer's ability to disclose the request or order in the first place.[294]

2. Statutory Change to Enable Redress

In *Schrems II*, the CJEU noted that the relevant U.S. surveillance programs conducted under Section 702 of FISA and EO 12333 do not allow the subjects of the surveillance meaningful or actionable redress before "an independent and impartial court."[295] Similar reasoning was given as part of why *Schrems I* invalidated the earlier Safe Harbor Framework[296] and why the ombudsperson mechanism was developed as part of the Privacy Shield.[297] However, the CJEU observed that the ombudsperson, as under secretary of state, was part of the executive branch, not independent from it, and could not take actions to bind the intelligence community.[298]

To adequately address what the CJEU perceives as deficiencies in judicial redress, some commentators argue that the United States will have to address two dimensions: (1) legitimate fact-finding concerning classified surveillance activity in order to ensure protection of individuals' rights, and (2) the ability to appeal to an independent judicial body that can remedy any potential violation.[299]

---

290. *See supra* Part II.B.4.
291. *See* EUROPEAN DATA PROT. BD., *supra* note 66, at 42.
292. *See id.* ¶ 124.
293. *See id.* ¶ 126.
294. *See id.* ¶ 125.
295. Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 194 (July 16, 2020).
296. *See* Case C-362/14, *Schrems I*, ECLI:EU:C:2015:650, ¶ 90 (Oct. 6, 2015) (emphasizing the lack of opportunity for EU data subjects to access judicial or administrative redress in relation to U.S. surveillance programs).
297. *See* Kenneth Propp & Peter Swire, *After Schrems II: A Proposal to Meet the Individual Redress Challenge*, LAWFARE (Oct. 9, 2020, 7:28 PM), https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge [https://perma.cc/RP4L-RBPG] (explaining the ombudsperson's role "to receive requests from Europeans regarding possible U.S. national security access to their personal data, and to facilitate action by the U.S. intelligence community to remedy any violation of U.S. law").
298. *See Schrems II*, C-311/18, ¶¶ 195–96.
299. *See* Propp & Swire, *supra* note 297.

Factual inquiries may be appropriate for administrative groups so long as they are sufficiently independent. Professors Kenneth Propp and Peter Swire note that enabling privacy and civil liberties officers (PCLOs) that already exist within the intelligence community to conduct the fact-finding inquiry may be viable.[300] PCLOs already have the statutory charge to investigate possible violations of privacy and civil liberties and also already have access to relevant Top Secret and classified databases.[301] Alternatively, the Privacy and Civil Liberties Oversight Board (PCLOB), a small independent federal agency, could be empowered to conduct the necessary fact-finding duties.[302]

Professors Propp and Swire argue that there are a number of advantages of PCLOs which may speak to their competency to take on expanded fact-finding duties.[303] PCLOs are competent to assess how agencies handle data because they are responsible for performing "Privacy Impact Assessments" of any new surveillance systems that an intelligence agency wishes to implement and are also responsible for issuing regular reports concerning the intelligence agency's activities.[304] Structurally, PCLOs report directly to senior officials, which may be helpful should they encounter problems in the course of conducting an investigation.[305] Lastly, PCLOs have existing staff and resources that are likely able to accommodate any new investigative responsibilities, such as responding to complaints from the EU.[306]

While PCLOs may be most practically equipped to assume factual inquiry duties because they are part of the intelligence agencies themselves, another commentator notes that they may not satisfy the independence requirement outlined by the CJEU.[307] Meanwhile, the PCLOB studied Section 702 of FISA and EO 12333 in the past six years and the EU recognizes and respects the PCLOB's independent voice on these subjects.[308] And like the PCLOs, the PCLOB has access to classified and Top Secret resources necessary for it to conduct adequate factual investigations.[309]

However, enabling the PCLOB with this expanded responsibility poses logistical challenges based on its current structure and resources. Because its statutory mandate currently only relates to oversight and policy at the

300. *See id.*
301. *See id.*
302. *See id.*
303. *See id.*
304. *See id.* Privacy Impact Assessments are reports done prior to implementation that determine how a particular program (or product or service if done by a company) impacts user or subject privacy. *See id.*
305. *See id.*
306. *See id.*
307. *See* Christopher Docksey, *Schrems II and Individual Redress–Where There's a Will, There's a Way*, LAWFARE (Oct. 12, 2020, 10:40 AM), https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way [https://perma.cc/M9H4-B744] (noting that PCLOs are structured more like data protection officers or chief privacy officers that are found within companies, rather than independent supervisory authorities like DPAs and, therefore, could not alone satisfy independent oversight or judicial redress).
308. *See* Propp & Swire, *supra* note 297.
309. *See id.*

program level, expansion into investigatory tasks would require a statutory update, which in turn requires congressional action. Conversely, any expansion of PCLO investigatory duties could be done based on administrative direction.[310] In addition, the existing scope of the PCLOB's mandate is limited to antiterrorism; therefore, Congress would also have to agree to expand that scope to include counterintelligence and national security more broadly for the PCLOB to be able to conduct effective fact-finding.[311] Lastly, to properly empower the PCLOB, Congress would have to not only expand its statutory mandate but also support the body with proper resources and staffing, including maintaining a staffed board.[312]

Whichever administrative body assumes the role of fact-finder, Professors Propp and Swire observe, the results shared with the complainant will likely be similar to those that the ombudsperson would also share—that there was no violation of the law or that any violation has been corrected.[313] The agency decision could then be appealed to an Article III judge for independent judicial review.[314] The FISC would be capable of the task because it is comprised of Article III judges who have experience handling foreign intelligence and U.S. surveillance matters.[315]

Structuring the complainant's request like a Freedom of Information Act[316] (FOIA) request could solve the potential standing issues[317] the CJEU highlighted in *Schrems II*.[318] Under FOIA, an individual can request information or documents from an agency without having to demonstrate any "injury."[319] The receiving agency is then required to conduct an investigation and either provide the information or explain why it will not supply the documents.[320] The requesting individual could appeal that agency decision to a federal court to assess the agency's investigation and can order changes to the outcome should there be a mistake.[321]

In this context, when an individual seeks redress suspecting their data has been improperly used as part of national security, the FISC could review the administrative body's factual investigation to ensure the agency met its statutory requirements and could issue orders to correct or delete data or demand additional fact-finding if necessary.[322] This sort of review of agency action or decision-making is common under the Administrative Procedure

310. *See id.*
311. *See id.*
312. *See id.* (stating "there have been periods since its establishment in 2007 when the PCLOB lacked a quorum to operate, due to an insufficient number of Senate-confirmed board members," which is indicative of how partisan conflict can lead to inaction in Congress).
313. *See id.*
314. *See id.*
315. *See id.* (noting that the FISC already oversees Section 702 programs and that the judges often review agency decisions in their non-FISC capacities).
316. 5 U.S.C. § 552.
317. *See* Propp & Swire, *supra* note 297.
318. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 115 (July 16, 2020).
319. *See* Propp & Swire, *supra* note 297.
320. *See id.*
321. *See id.*
322. *See id.*

Act[323] (APA). Finally, standing for the individual is established in this context because the "case or controversy" is the review of the agency action and whether the agency has complied with the statutory duties on behalf of the complaining individual.[324]

III. A HYBRID SOLUTION INVOLVING PUBLIC AND PRIVATE LAW

In an ideal world, the best solution to the current uncertainty surrounding EU-U.S. cross-border data transfers might center on a new international agreement—a "Privacy Shield 2.0"—that includes updates to EU data protection mandates and addresses the CJEU's objections to U.S. surveillance law. Absent that highly unlikely scenario, companies and entities continue to assess the adequacy of the various proposals discussed in Part II to determine which, if any, can be utilized to satisfy the strict conditions required by the EU.[325]

This part argues that the most effective solution for addressing the different deficiencies articulated in *Schrems II* is to adopt a hybrid of multiple private-law solutions discussed in Part II.B, along with manageable public-law updates discussed in Part II.C. Part III.A addresses why some of the solutions from Part II are insufficient on their own. Part III.B explains why the combination of encryption and updated SCCs can mitigate the risk of the U.S. public authorities improperly obtaining EU subjects' data. Then, Part III.C endorses parts of Professors Propp and Swire's proposal to afford individuals an avenue to independent redress as the best solution, not only to fix the redress deficiency but also to meaningfully strengthen oversight of U.S. surveillance authorities—thereby helping to establish essentially equivalent protection.

A. The Ineffectiveness of Some Proposed Recommendations

Article 49 derogations emerged in the immediate aftermath of *Schrems II* as a possible solution to the problem of inadequacy, perhaps in part due to the CJEU's acknowledgment that the article could suffice.[326] However, in the EDPB's recommendations to exporters about supplemental measures, the board confirmed that the derogations under Article 49, including consent, have "an exceptional nature"[327] and "must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive."[328] Therefore, in light of the EDPB's subsequent guidance, which reiterates the "strict conditions" transfers must meet under any of the

323. 5 U.S.C. § 706(2)(A) (requiring that an agency decision is not "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law").

324. *See* Propp & Swire, *supra* note 297.

325. *See* Zwillinger et al., *supra* note 168 (discussing the work done on behalf of clients to continue business operations without a solid government solution).

326. *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 202 (July 16, 2020).

327. EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 25.

328. EUROPEAN DATA PROT. BD., *supra* note 78.

Article 49 derogations, it is unlikely to be the mechanism on which most companies and transfers can rely for adequacy.[329]

The same EDPB recommendations emphasize technical measures, but they are unlikely to provide the solution without more.[330] Not only are the outlined parameters for considering encryption to be adequate protection very strict,[331] there is also no redress for the data subjects in the United States if public authorities do access personal data despite the state-of-the-art technical measures the exporters and importers employ.[332] The importer and exporter may then be exposed to liability for failing to create adequate protections. Considering the uncertainty in the space, companies should conduct thorough assessments of the law and of the practices of public authorities toward their particular transfers and then combine technical measures with additional private-law options.[333]

Many of the suggested contractual promises to inform the exporter and data subject of public authority access are promising, but in the context of U.S. importers, however, these recommended provisions may be impractical—particularly for those electronic communications service providers that are subject to FISA Section 702, which prohibits disclosure of any production orders they may receive for the data.[334] In that circumstance, the importer may be able to specify which parts of the exporter's inquiry they are legally prohibited from disclosing.[335] But ultimately, if the legislation in the third-party country prevents such disclosure (as FISA Section 702 does in the United States),[336] then the importer will be unable to comply with the above contractual commitments and will thus fail to provide essentially equivalent protection.[337]

The contractual measures that impose an obligation to fight orders from public authorities to provide data would only be effective according to the EDPB's recommendation if the public authority's access to the data is suspended while the challenge takes place.[338] Additionally, the importer would have to be permitted to document the actions it takes to demonstrate to the exporter that it has fulfilled its commitment.[339] This is likely implausible given FISA's current disclosure restrictions.[340]

Of course, a provider making promises related to Section 702 of FISA may still ultimately be compelled to provide U.S. intelligence authorities with the information because this order is likely legal in the United States.[341] In such

329. EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 26.
330. *See supra* text accompanying notes 213–20.
331. *See* Christakis, *supra* note 181.
332. *See supra* text accompanying note 294.
333. *See generally* EUROPEAN DATA PROT. BD., *supra* note 66.
334. *See supra* note 104 and accompanying text.
335. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 106(5).
336. *See* 50 U.S.C. § 1881a.
337. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 110.
338. *See id.* ¶ 119.
339. *See id.*
340. *See supra* note 104 and accompanying text.
341. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 119.

a scenario, the U.S.-based importer should inform the exporter of its inability to further comply with the terms; this notification will permit the exporter to cease further data transfers and terminate the contract.[342] This scenario is already protected under the existing SCCs and does not require supplemental terms.[343]

Importantly, the fact that such an exit strategy is provided for in the existing SCCs suggests that exporters and importers need not guarantee absolute security.[344] By providing an "out" for when parties cannot comply, the SCCs—the validity of which was affirmed by the court in *Schrems II*—imply a certain tolerance of risk, so long as transfers can be suspended once compliance is no longer feasible.[345] So, while the EDPB's recommendations suggest a primarily rights-based approach, there are elements of it that utilize a risk-based approach where the risk is properly assessed by the data exporter and importer on a case-by-case basis,[346] which could be consistent with GDPR compliance.[347]

B. Solving Proportionality with Private Covenants

The most effective and immediate way for companies to continue to transfer data from the EU to the United States is to adopt measures the companies themselves can take to mitigate the risk of sacrificing the data protections required under the GDPR. A combination of state-of-the-art encryption and enhanced supplemental contractual clauses can provide an adequate level of protection for EU data subjects that is "essentially equivalent" to that of the EU.[348]

As discussed in Part II.B.1, technical enhancements can provide the required level of legal protection under certain circumstances.[349] The final direction from the EDPB explains that if data is encrypted prior to being transferred and the U.S. importer does not have the decryption key, then the encryption is considered an effective supplementary measure.[350] In that scenario, even if public authorities obtain the data in transit or from the importer directly under Section 702, the data will be useless because the agency will not be able to match it to an EU data subject.[351] So, even if the public authority technically obtains encrypted or pseudonymized data, the EDPB will still characterize the EU data as subject to protection so long as the public authority lacks the capacity to decrypt the data or reidentify the

342. *See id.* ¶ 114.
343. *See* SCC Decision, *supra* note 67, cl. 5(a); *see also supra* notes 279–81 and accompanying text.
344. *See supra* note 269 and accompanying text.
345. *See supra* note 269 and accompanying text.
346. *See supra* note 181 and accompanying text.
347. *See supra* notes 279–81 and accompanying text.
348. EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 77.
349. *See supra* Part II.B.1.
350. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶¶ 79–92.
351. *See supra* notes 196–97 and accompanying text.

subject.[352] At a minimum, companies should endeavor to adopt any and all encryption methods that satisfy these criteria.[353]

However, technical measures alone will not be enough in some cases.[354] For example, whenever the importer requires *decrypted* data for processing, that data may be vulnerable under Section 702, or it could be intercepted in transit via EO 12333.[355] Therefore, additional binding protections should be addressed in contracts prior to transfers.[356] Such clauses should first clearly articulate the encryption tools employed to prevent or minimize actual access, as discussed above.[357] But these clauses should also include transparency measures and an obligation to take specific actions that are consistent with what is permissible under U.S. surveillance law.[358]

These enhanced supplemental contractual clauses should begin with those that the EDPB has recommended.[359] They should clearly identify how the importers and the data may be subject to the different aspects of U.S. surveillance law.[360] For example, Section 702 of FISA only applies to electronic communications service providers, so if the importer falls outside of that definition, the reach of Section 702 need not impact the assessment of the transfer.[361]

More critically, the parties can include provisions that obligate the importers to take legal action (in addition to the technical encryption) to prevent public authority access whenever possible.[362] These could include guaranteeing good faith efforts to challenge any orders consistent with U.S. law.[363]

The problem, however, is that under some of the U.S. laws, such as Section 702, when an importer receives an order from the U.S. public authority requesting the data, the importer is prohibited from disclosing that fact to others, including the data subjects or the exporters.[364] This may be overcome with a "canary" provision, whereby the importer sets a regular and frequent notification confirming that it has not received any request.[365] Should that notification fail to reach the exporter according to schedule, that exporter will be free to suspend data transfers and notify the data subjects if it believes the public authorities have accessed that data.[366] This "negative notification"

352. *See supra* notes 205–16 and accompanying text.
353. *See supra* notes 205–16 and accompanying text.
354. *See supra* notes 214–20 and accompanying text.
355. *See supra* notes 201–04 and accompanying text.
356. *See supra* Part II.B.4.
357. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶ 103.
358. *See supra* Parts II.B.4.a–b.
359. *See* EUROPEAN DATA PROT. BD., *supra* note 66, ¶¶ 103–27.
360. *See supra* note 264 and accompanying text.
361. *See supra* notes 274–75 and accompanying text.
362. *See supra* Part II.B.4.b.
363. *See supra* note 289 and accompanying text.
364. *See* 50 U.S.C. § 1881a.
365. *See supra* notes 282–85 and accompanying text.
366. *See supra* notes 282–85 and accompanying text.

does not actually disclose that an order has been received; thus, it should be permissible and not in conflict with Section 702's prohibitions.[367]

These additional obligations recommended by the EDPB, when combined, can effectively mitigate the risk of overbroad U.S. public authority access to EU subjects' data, and they should be adopted immediately.[368] Indeed they are also consistent with the CJEU's rationale in *Schrems II*, which articulated that private parties can take supplemental measures to achieve essentially equivalent protections for EU data subjects.[369] Technical protections, along with contractual obligations, can clear this legal hurdle and provide practical protections for EU data subjects. They do not, however, remedy the lack of judicial redress that was the primary deficiency in *Schrems II*.[370] An effective remedy would require some level of congressional involvement.[371]

C. Enabling Individual Redress While Strengthening Oversight

Despite the EDPB's recommendations and private parties' best efforts, private law cannot solve the standing problem for subjects who wish to seek redress from the U.S. judicial system.[372] Therefore, Congress should adopt the main components of Professors Propp and Swire's proposal[373] for two reasons: (1) the proposal is a reasonable and logical adjustment that remedies a consistent deficiency with regard to redress, and (2) the proposal is an opportunity to actually strengthen effective oversight of surveillance programs in the United States. Such a result not only benefits the pragmatic needs of entities that wish to engage in cross-border data transfers between the EU and United States but also strengthens the state of American democracy.[374]

Professors Propp and Swire propose two potential groups that could be appropriate for the task: fact-finder PCLOs and the PCLOB.[375] While PCLOs may be most readily equipped to assume factual inquiry duties because of their current role and work at the agencies,[376] the PCLOB's separation from the intelligence agencies makes it more likely to qualify as an independent and effective fact-finder consistent with the CJEU's assessment of the requirements under the Charter.[377] Ultimately, enabling

367. *See supra* note 285 and accompanying text.
368. *See supra* Part III.B.
369. *See supra* note 157 and accompanying text.
370. *See supra* notes 140–47 and accompanying text.
371. *See infra* Part III.C.
372. *See supra* note 109 and accompanying text.
373. *See supra* Part II.C.2. (outlining the proposal to strengthen and expand the powers and duties of existing oversight agents to permit an avenue of redress for non-U.S. persons).
374. More transparent and effective oversight of the intelligence authorities is an opportunity to rebuild trust since the Snowden revelations. *See supra* note 106 and accompanying text.
375. *See supra* Part II.C.2.
376. *See supra* text accompanying notes 304–06.
377. *See* Docksey, *supra* note 307 (noting that the PCLOs are structured more like internal data protection officers or chief privacy officers who are found within companies, rather than

the PCLOB to assume the fact-finding role is the superior choice because the board's entire mission can be focused on oversight, and it does not suffer from conflicting interests by being a part of the intelligence agency it is meant to monitor.[378] Therefore, to simply, yet effectively, remedy the redress problem, Congress must take moderate statutory action to update the scope of the PCLOB's role, duties, and resources.[379]

Neither of these bodies would sufficiently address the redress problem on its own, however, as both are still within the executive branch.[380] Professors Propp and Swire's proposal effectively addresses this issue by subjecting to review by an Article III judge the results of any fact-finding done as part of agency decision-making; this judicial review is similar to that of any administrative agency decision-making review.[381] While the proposed review would be a new task for the FISC, judges on this court are better suited for it than traditional Article III judges because of their expertise in U.S. surveillance law and demonstrated record of effective oversight of Section 702.[382]

Professors Propp and Swire realize that, due to the classified nature of the administrative finding, there may not be an effective way for the complainant to determine whether an appeal to the judiciary is warranted.[383] Therefore, an automatic appeal to the FISC could work to ensure effective judicial oversight.[384] The natural concern, then, would be overburdening the FISC by permitting a flood of complaints.[385] However, that need not be the case if Congress considers an effective balance when it makes its statutory updates.[386] Also, Professors Propp and Swire highlight that this is not a new problem; based on prior international agreements with Europe like the Privacy Shield and the Terrorist Finance Tracking Program, the "actual number of complaints would likely be manageable."[387]

The other benefit of this proposed remedy to redress is seen during the appeal to the FISC. The USA FREEDOM Act of 2015[388] established a role

independent supervisory authorities like DPAs and therefore could not alone satisfy independent oversight or judicial redress).

378. *See id.*

379. *See supra* text accompanying notes 310–12.

380. *See* Propp & Swire, *supra* note 297. The PCLOB, though an independent agency, is still within the executive branch and ultimately suffers from the same deficiencies as the ombudsperson under the Privacy Shield. *See supra* text accompanying notes 298–302.

381. *See supra* notes 313–15 and accompanying text.

382. *See* Peter Swire, *The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Peter Swire* 3–15 (Georgia Tech Scheller Coll. of Bus. Research Paper, Paper No. 18-2, 2016), https://ssrn.com/abstract=3097444 [https://perma.cc/B2NW-NJT4] (stating that, after a review of declassified FISC decisions that emerged in the wake of the Snowden revelations, the "FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance").

383. *See* Propp & Swire, *supra* note 297.

384. *See id.*

385. *See id.*

386. *See id.*

387. *Id.*

388. Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in scattered sections of the U.S.C.).

for amici curiae who can brief the FISC on "legal arguments that advance the protection of individual privacy and civil liberties."[389] In this capacity, the amici would also advance the interests of the complainant, allowing the FISC judge to receive complete adversarial briefings, thus further enhancing the judicial oversight.[390]

Finally, the proposed expansion of redress should be made available to U.S. persons in addition to those making complaints from the EU.[391] The Snowden revelations showed that these surveillance programs also impacted U.S. persons.[392] While reform has taken place since the public learned of the mass collection programs in 2013, there is value in allowing a limited avenue of redress for U.S. persons to ensure that oversight keeps the intelligence community in check.[393] This would not upend the standing requirements, but it would merely empower stronger and more effective independent oversight of the intelligence community, both at the agencies and in the judiciary.[394] This proposal for redress seems to require the implementation of more government action, but it might provide the meaningful adjustment that institutes an opportunity for independent redress that, according to the CJEU, was critically missing from the Privacy Shield.[395]

CONCLUSION

In *Schrems II*, the CJEU confirmed that it will protect the fundamental privacy and data protection rights of EU subjects when subjects' data is transferred out of the EU. That position conflicts with the current scope of data collection conducted in accordance with U.S. surveillance law. To resolve this conflict, private entities should do everything they can to reasonably protect EU personal data that is imported into the United States. In addition, the U.S. government must also make minor adjustments to improve and expand the independent oversight of the intelligence community.

Private actors should adopt supplemental measures recommended by the EDPB, such as technical encryption and supplemental contract terms that provide more assurances about the steps they take to protect data from U.S. intelligence. These measures are consistent with the CJEU's assertion that supplemental measures may achieve essentially equivalent protection. However, if with the assurances, U.S. public authorities still access that data, the CJEU has been clear that there needs to be some properly independent avenue of redress for the data subject. Expanding the purview of the FISC and empowering the PCLOB to perform independent factual investigations

389. Propp & Swire, *supra* note 297.
390. *See id.*
391. *See id.*
392. *See supra* note 106 and accompanying text.
393. *See supra* text accompanying note 374.
394. *See* Propp & Swire, *supra* note 297.
395. *See supra* notes 140–48 and accompanying text.

are reasonable and manageable solutions that can enhance data protection and oversight without opening the entire judiciary to a flood of claims.