Maryland Journal of International Law

Volume 36 | Issue 1 Article 6

Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems: Where Do We Go From Here?

Dillon Swensen

Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems: Where Do We Go From Here?

DILLON SWENSEN†

I. INTRODUCTION

In *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (*Schrems II*)[1], the European Court of Justice (ECJ) ruled that the EU-U.S. Privacy Shield Framework (the Framework), which permitted the transfers of EU citizens' personal data to the United States, was invalid.[2] Finding that United States law was insufficient to adequately protect the fundamental privacy rights of its citizens[3] and provide rights "essentially equivalent" to those that European citizens had in their home countries, the ECJ struck down the Framework and also called into question the adequacy of EU-U.S. data transfers based on the primary alternative data transfer mechanism: the Standard Contractual Clauses (SCCs).[4] The *Schrems II* decision upheld the principles of the prior *Schrems I* decision, which

† J.D. Candidate (2022), University of Maryland Francis King Carey School of Law. The author thanks Alison DeMarco, Edward Bellows, Erick Marquina, and the Executive Board of the Maryland Journal of International Law for their feedback, edits, and comments. He also thanks Professor Markus Rauschecker for his guidance and advice throughout the writing process. The author dedicates this article to his mother, Susan Swensen for her love and moral support.

1. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 EU:C:2020:559 (July 16, 2020) [hereinafter "*Schrems II*"].

2. *See infra* Part III.5.

3. In large part, these findings were based on the existence of mass surveillance programs such as PRISM, which the court did not believe were sufficiently accountable. *See infra* Part II.B, III.B.5

4. The Standard Contractual Clauses are boilerplate language inserted into contracts between data providers, designed to create binding obligations on data providers to protect privacy. *See infra* Part II.C, Part III.4–5.

created the essential equivalence standard used by the ECJ in *Schrems II*.[5] Thus, when viewed in light of the fundamental importance of data privacy as enshrined in EU law, this ruling was perhaps inevitable.[6]

In the wake of the *Schrems II* ruling, it is evident that any future Framework would likely be equally invalid absent a substantial overhaul of U.S. privacy law.[7] This poses a nearly impossible barrier to any future attempt to build a new version of the Framework that could survive judicial review by the ECJ.[8] There will be no easy options available for businesses seeking to ensure compliance with EU data protections and avoid strict fines.[9] With the validity of many transatlantic SCCs called into question and conflicting statements as to their validity from the U.S. Government and various European authorities, it is unclear what path remains for companies seeking to comply with EU law and engage in international electronic data commerce.[10] It may be that the only viable long-term solution is for the U.S. to pass legislation to bring its data privacy laws up to the essential adequacy standard.[11] Given the potential for large fines for companies that fail to comply with EU law, the safest option for any company is to keep EU citizens' data within Europe.[12] However, this may not be economically feasible.[13] The ECJ has created an extremely uncertain business environment for multinational corporations seeking to do business in Europe, a fact made clear by the comments from European Data Authorities seeking to make sense of the ECJ's ruling.[14]

This note was written during a time of remarkable uncertainty for the future of transatlantic data transfer.[15] While there is a significant body of scholarship analyzing the *Schrems I* decision,[16] the *Schrems II* decision to date has been discussed primarily by journalists and the reactions of government bodies.[17] Accordingly, the intent of this note is to provide an early assessment of the impact of the *Schrems II*

5. *See infra* Part II.B.
6. *See infra* Part IV.A.
7. *See infra* Part IV.B.
8. *See infra* Part IV.B.
9. *See infra* Part IV.C.
10. *See infra* Part IV.C.
11. *See infra* Part IV.B.
12. *See infra* Part IV.C.
13. *See infra* Part IV.C.
14. *See infra* Part IV.C.
15. The research in this note is current as of December 21, 2020.
16. *See e.g.*, *infra* notes 25, 30, 42.
17. *See e.g.*, *infra* notes 153, 165, 168, 171.

decision.[18] More specifically, this note will provide an overview of the legal and procedural background that informs the *Schrems II* decision and will review the decision itself within the context of the prior litigation on this topic.[19] Next, this note will analyze the revolutionary nature of the *Schrems II* opinion, discussing the role of the ECJ as a safeguard for the fundamental rights of its citizens unbeholden to corporate or political interests.[20] Because the ECJ's concerns with Privacy Shield go beyond the document itself and take issue with the foundations of the United States' constitution and security apparatus, this note will also discuss the degree to which competing values and partisan deadlock within the United States make a replacement Framework impossible, despite proclamations by the Department of Commerce to the contrary.[21] Finally, this note will provide a brief analysis of the legal uncertainty that predominates after the *Schrems II* ruling, with a particular focus on the conflicting statements of the various national and regional European Data Protection Authorities and the implications of these statements for companies seeking to engage in EU-U.S. data transfers.[22]

II. LEGAL BACKGROUND

A. Commission Decision 2000/520 and the Development of Safe Harbor

Under the EU Data Protection Directive (95/46/EC) ("the Directive"), EU member states were only allowed to permit the transfer of personal data to countries outside the EU if, and only if, said outside county "ensure[d] an adequate level of protection" for the data.[23] Article 25(6) of the Directive provided that the European Commission may make a finding that a [non-EU] country ensures an adequate level of protection either (1) "by reason of its domestic law"

18. While this paper does discuss the impact of the *Schrems II* decision on corporations to some degree, detailed information on specific corporate responses largely falls outside of its scope. For an example of a corporate response, consider: Rian van der Merwe, *Postmark's Response to the Schrems II Judgment*, POSTMARK (Dec. 8, 2020), https://postmarkapp.com/blog/postmarks-response-to-the-schrems-ii-judgment-privacy-shield-invalidation.

19. *See infra* Part II, III.

20. *See infra* Part IV.

21. *See infra* Part IV.B.

22. *See infra* Part IV.

23. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the free movement of such data, 1995 O.J. (L 281) art. 25(1) [hereinafter EU Data Protection Directive 95/46].

or (2) "the international commitments it has entered into."[24] Without such a finding, the personal data of EU citizens could not be transmitted out of the EU.[25]

In order to ensure that EU-U.S. data transfers were legally permissible, the European Commission and the U.S. Department of Commerce negotiated the Safe Harbor Privacy Principles.[26] Under the Safe Harbor Principles, companies were required to certify compliance with the principles and publicize their adherence to the framework.[27] This requirement that companies publicize their adherence ensured that domestic U.S. regulatory agencies such as the FTC and state attorney generals could bring claims against companies who breached these public commitments on the basis of "unfair or deceptive" trade practices.[28]

A mere five days after the issuance of the Safe Harbor Principles, the EU Commission found that the Safe Harbor Principles provided "an adequate level of protection for personal data" transferred from the EU to organizations in the United States.[29] The Commission's finding of adequacy was based on the Safe Harbor's inclusion of dispute resolution provisions and the commitment of the FTC to regulate violations of the Safe Harbor Principles.[30] This enforcement provision was not entirely toothless either—over the next few years, the FTC brought cases against companies including Google, Facebook, and MySpace for violations of the Safe Harbor Principles.[31] These enforcement actions were not based on the Safe Harbor Principles themselves, but rather on the violation of the public commitments, which the FTC contended amounted to deceptive practices under U.S.

24. *Id.* at art. 25(6).

25. *Id.* at art. 25(1).

26. Gabe Maldoff & Omer Tene, *"Essential Equivalence" and European Adequacy After Schrems: The Canadian Example*, 34 WIS. INT'L L.J. 211, 223 (2016).

27. *Id.*

28. *Id.* at 222–24.

29. Commission Decision 2000/520, art. 1, 2000 O.J. (L 215) 1 (EC).

30. *Id.*

31. Holly Kathleen Hall, *Restoring Dignity and Harmony to United States–European Union Data Protection Regulation*, 23 COMM. L. & POL'Y 125, 129 (2018); Maldoff, *supra* note 26, at 224; MySpace LLC, Docket No. C-4369 (Sept. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf; Facebook, Inc. Docket No. C-4365 (Nov. 11, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf; Google, Inc., Docket No. C-4336 (Nov. 10, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf .

law.[32]

Notably, the Safe Harbor Principles contained a carve-out allowing states unlimited access to data for national security purposes.[33] Some have suggested that this lack of limitations was because, at the time, few if any policymakers were aware of the scope of warrantless government surveillance.[34]

B. The Schrems I Decision and the End of Safe Harbor

In 2013, Edward Snowden, a former NSA contractor, leaked information to the Guardian and the Washington Post detailing the extensive data collection efforts of U.S. surveillance agencies.[35] One of the most notable of these efforts was PRISM, a government program which gave the NSA direct access to major U.S. internet service providers, including Facebook and Google.[36] When contacted for comment, these providers denied the allegations.[37] Later revelations from Snowden expanded upon this picture of a vast and unaccountable surveillance architecture, including the capacity of the NSA to gather information directly from fiberoptic cables (a process known as upstream data collection).[38]

Shortly thereafter, Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner alleging that the Safe Harbor framework, as implemented, was incompatible with EU law.[39] Schrems had previously worked as a privacy advocate filing complaints against Facebook to challenge the website's privacy policies, but in the aftermath of the Snowden revelations, Schrems filed yet another complaint, inquiring whether Facebook was voluntarily forwarding his personal data to the NSA.[40] However, these

32. Maldoff, *supra* note 26, at 224.

33. *Id.*

34. *Id.* at 227.

35. Maldoff, *supra* note 26, at 225 (citing Glenn Greenwald, et al., *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance).

36. Maldoff, *supra* note 26, at 226 (citing Dominic Rush & James Ball, *PRISM Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers*, THE GUARDIAN (June 6, 2013, 19:48), http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining).

37. Dominic Rush & James Ball, *PRISM Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining.

38. Maldoff, *supra* note 26, at 226.

39. *Id.* at 228–30.

40. *Id.*

complaints were dismissed as "frivolous and vexatious" by the Commissioner.[41] Schrems sought judicial review of this decision from the Irish High Court.[42] Although the High Court expressed concern with the protections granted to EU citizens under the law, it did not have the authority to make a ruling on a matter of EU law.[43] Irish privacy laws were preempted by the adequacy finding of the European Commission.[44] Accordingly, the High Court referred the matter to the ECJ.[45]

This referral led to the famous *Schrems I* decision, where the ECJ held that Decision 2000/520 was invalid and the "adequate level of protection" standard under the Directive could only be satisfied by a level of protection of its citizens' fundamental privacy rights that was "essentially equivalent" to the level of protection guaranteed within the EU.[46] Decision 2000/520, the Court held, could not be valid because it did not account for domestic U.S. surveillance laws in its finding of adequacy.[47] Although national security was a "legitimate objective" which could potentially justify an intrusion on the data privacy rights of EU citizens, neither the Safe Harbor Framework nor any other domestic law or international commitment of the U.S. placed any limitations on this surveillance.[48] Because Decision 2000/520 did not account for this lack of limitations, the Court struck down the Decision, invalidating the Safe Harbor framework as a mechanism for data transfer.[49]

C. The Privacy Shield Framework and the Development of the GDPR

The reaction by various American-based tech businesses operating in the EU was perhaps predictable.[50] Even as soon as the

41. Schrems v. Data Prot. Comm'r [2014] IEHC 310 (Ir.), ¶ 32.

42. Schrems v. Data Prot. Comm'r [2014] IEHC 310 (Ir.).

43. Dr. Nora Ni Loidean, *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, 19 J. INTERNET L. 1, 9–10 (2016) (citing Foto-Frost v. Hauptzollamt Lübeck-Ost, Case C-314/85, ECR 4199 (1987)).

44. Maldoff, *supra* note 26, at 229.

45. Hall, *supra* note 31, at 132.

46. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EU:C:2015:650 (Oct. 6, 2015) ("*Schrems I*") at 73.

47. *Id.* at 98.

48. *Id.* at 88.

49. Maldoff, *supra* note 26, at 230.

50. *See, e.g.*, Ben Kepes, *How Tech Vendors Are Reacting to the Safe Harbor Ruling*, NETWORKWORLD (Oct. 19, 2015), *www.networkworld.com/article/2991752/how-tech-vendors-are-reacting-to-the-safe-harbor-ruling.html*;
Safe Harbour: Tech Firms Shudder As Watchdogs Meet, BBC (Feb. 2, 2016),

Advocate General gave his preliminary, non-binding opinion, tech executives stepped forward to criticize the direction of the ECJ.[51] Google and other companies were forced to scramble to determine alternative measures, with Google announcing to its cloud platform users that it would adopt a contractual clause based protection until a new Safe Harbor agreement could be ratified.[52]

The European Commission and the U.S. Department of Commerce moved quickly, and within four months of the *Schrems I* decision, the European Commission and the U.S. Department of Commerce announced a replacement framework, the "EU-U.S. Privacy Shield."[53] Broadly speaking, the Privacy Shield agreement did not differ much from Safe Harbor, although it did grant EU citizens additional rights to access their private data and made clear that data subjects had legal claims against data owners who failed to meet the requirements of Privacy Shield (although there was no clear enforcement mechanism in U.S. courts).[54] Of particular note, the Privacy Shield agreement created a "Privacy Shield Ombudsperson" vested with the authority to investigate complaints made by EU residents.[55] This was combined with assurances from "high level US officials" who provided assurances of the limitations on U.S. surveillance, although it was unclear if these assurances merely repeated existing, post USA Freedom Act policy.[56]

Bearing in mind the requirements of *Schrems I*, the Commission

https://www.bbc.com/news/technology-35460131.

51. See Sam Schechner & Natalia Drozdiak, *U.S.–EU Data-Transfer Pact Should Be Invalidated, Says Advocate General*, WALL STREET J. (Sept. 23, 2015, 12:09 PM), https://www.wsj.com/articles/u-s-eu-data-transfer-pact-should-be-invalidated-says-advocate-general-1442998520.

52. Hall, *supra* note 31, at 135.

53. Maldoff, *supra* note 26, at 236; Press Release, Eur. Comm'n, EU Comm'n and U.S. Agree on New Framework for Transatlantic Data Flows: EU–U.S. Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.html.

54. *See* Owen, *Comparison Safe Harbor vs. the EU–US Privacy Shield*, OTAVA (Apr. 11, 2019), https://www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/ (noting that little had changed between Privacy Shield and Safe Harbor besides the fact that companies could not transfer data on to a third party without consent). *But see* David Zetoony, *A Side-by-Side Comparison of "Privacy Shield" and the "Safe Harbor"* (July 16, 2019), https://iapp.org/media/pdf/resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf (identifying several major changes including increased rights of data subjects to access their private data and expanded legal recourse for said subjects).

55. Commission Implementing Decision 216/1250 of July 12, 2016, 2016 O.J. (L 207) 71.

56. Maldoff, *supra* note 26, at 238–39 (noting that the United States had passed further legislation, including the USA Freedom Act, which limited NSA bulk metadata collection and introduced new reporting requirements related to government data collection).

Implementing Decision 2016/1250 formally approved the Privacy Shield Agreement after "[careful analysis of] U.S. law and practice, including [the United States'] official representations and commitments."[57] The Commission noted that the Fourth Amendment would indirectly protect EU citizens because their data would be stored in the hands of U.S. corporations who could avail themselves of Fourth Amendment protections.[58] Although these protections did not apply directly to EU citizens, the Commission noted that EU citizens could avail themselves of certain statutory protections, such as the Freedom of Information Act and the Administrative Procedure Act.[59] The Commission concluded that, based on this law and the assurances of the U.S. government, the U.S. would limit its "interference" into the "fundamental rights" of citizens whose personal data was transferred out of the EU to "what was strictly necessary."[60] Finally, the Commission committed to a regular review of the adequacy finding, mindful that the level of protection provided by the U.S. could change.[61]

On April 27, 2016 the European Parliament and Council of the European Union repealed the EU Data Protection Directive (95/46/EC) and replaced it with the General Data Protection Regulation ("GDPR").[62] The GDPR still invested the European Commission with the power to determine whether nonmember countries offered adequate levels of data protection.[63] However, the GDPR affirmed the "essential equivalence" standard of *Schrems I*.[64] Of particular note was the requirement that EU citizens needed to be granted "effective and enforceable rights" and "effective administrative and judicial redress" by the legal system of a nonmember state in order for a finding of adequacy to be made by the Commission.[65] Given the Commissioner's finding of inadequacy, the GDPR provided that the controllers or

57. *See* Commission Implementing Decision 216/1250 of July 12, 2016, 2016 O.J. (L 207) 12.

58. *Id.* at 126–27.

59. *Id.* at 130–34.

60. *Id.* at 135.

61. *Id.* at 145–46.

62. *Schrems II*, 2020 EU:C:2020:559 at 71 (explaining that for the purposes of the ECJ's analysis, the GDPR did not represent a fundamental shift in the law with regard to transfers of personal data to nonmember states); *see also infra* Part III.B.

63. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, 2016 O.J. (L 119) 103 [hereinafter "GDPR"].

64. *Id.* at 104.

65. *Id.*

processors of its citizens' personal data should compensate for inadequate data protection through one of two measures: standard contractual clauses (SCCs) or binding corporate rules (BCRs) judged by the Commission to offer adequate safeguards for data protection.[66]

The European Commission created SCCs in its 2010 SCC Decision, which laid out a series of binding contractual clauses,[67] which, when implemented without modification into the contract between a EU-based data controller or processor and a non-EU-based data controller or processor, were found to provide adequate data protection.[68] Although it was obvious that such SCCs were not capable of binding the authorities of the non-EU country where the non-EU data controller or data processor resided, because the authorities of that country were not parties to the contract, the Commission stated that they were nevertheless sufficient to meet the data protection standards of the EU.[69]

BCRs[70] were a similar type of data protection safeguard for companies seeking to engage in data transfers.[71] Unlike the SCCs, BCRs were custom procedures developed and implemented by the data controller themselves and then approved by the data protection authorities and the European Data Protection Board.[72] These BCRs were held to be adequate protection for data so long as (1) they were made legally binding, (2) were enforceable against and enforced by every interested party involved in the data transfer, and (3) provided a clear system for EU citizens to vindicate their data rights if necessary.[73]

66. *Id.* at 108.

67. For an example of the SCCs, please see: Annex, 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, 2016 O.J. (L 39) (Feb. 5, 2010).

68. *Schrems II*, 2020 EU:C:2020:559 at 124.

69. *Id.* at 125.

70. For an example of Binding Corporate Rules, please see: *Privacy Rules for Customer, Supplier and Business Partner Data*, KONINKLIJKE PHILIPS ELECTRONICS N.V. (2012), https://www.philips.com/c-dam/corporate/about-philips/investor-relations/General-Business-Philips-PrivacyRulesCSBData.pdf.

71. *Binding Corporate Rules (BCR)*, EUROPEAN COMMISSION (May 25, 2018), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en; *Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR*, EUR. COMM'N (Apr. 11, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

72. *Binding Corporate Rules (BCR)*, *supra* note 71.

73. *International Personal Data Transfers: Binding Corporate Rules (BCRs) Under the GDPR*, I-SCOOP (last visited Dec. 18, 2020), https://www.i-scoop.eu/gdpr/binding-corporate-rules-bcrs-gdpr/.

If these criteria were met, then the data controlling companies did not need to rely on SCCs or Safe Harbor.[74] The use of BCRs was essentially limited to large companies that could afford to implement them.[75]

Despite the difficulties of using BCRs, in the aftermath of *Schrems I*, the ECJ had identified these two tools as a stopgap measure that could be used until a new Safe Harbor provision was created.[76] Accordingly, in the aftermath of the *Schrems I* decision, many companies, including Facebook, came to rely on the SCCs to ensure their compliance with the law.[77]

III. DATA PROTECTION COMMISSIONER V. FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

A. Procedural Background

After the October 2015 *Schrems I* decision and Facebook's adoption of the standard data protection clauses set out in the SCC Decision, in December 2015 Schrems reformulated his Complaint to the Data Protection Commissioner.[78] Schrems argued that because United States law required Facebook to make personal data transferred to it available to American security agencies such as the NSA and FBI, the SCC decision was insufficient to ensure the essentially equivalent protections required under the *Schrems I* decision.[79] In a draft decision, the Commissioner agreed, stating that the SCCs were by their very

74. *Id.*

75. Nigel Cory, et al. *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, INFO. TECH. & INNOVATION FOUND. (ITIF) (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic (noting that even for such companies, BCRs were not a panacea, being vulnerable to many of the same risks as SCCs). However, the difficulty in implementing BCRs means that in 2018, only 132 companies had ever obtained an approved BCR. Alexandra Ross & Volha Samsiuk, *BCRs: 'Best Case Route' or 'Better Call Reinforcements'?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/bcrs-best-case-route-or-better-call-reinforcements/.

76. *Commission Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14*, at 5, EUR. COMM'N, COM (2015) 566 final (Nov. 11, 2015).

77. Natasha Lomas, *Facebook Told it May Have to Suspend EU Data Transfers After Schrems II Ruling*, TECHCRUNCH (TC) (Sept. 9, 2020, 5:20 PM), https://techcrunch.com/2020/09/09/facebook-told-it-may-have-to-suspend-eu-data-transfers-after-schrems-ii-ruling/.

78. *Schrems II*, 2020 EU:C:2020:559 at 53–55.

79. *Id.*

nature incapable of binding the United States authorities.[80] Given that Schrems' new complaint raised the issue of the validity of the SCC decision, the Commissioner brought the action before the Irish High Court, which in turn referred the question to the ECJ.[81]

Before referring the matter to the ECJ however, the Irish High Court undertook an expansive examination of the facts at issue.[82] The High Court did not confine itself to an assessment of the question of the validity of Facebook's SCC, but conducted a broad review of the United States governments' intelligence activities and other grounds for holding data transfers between the United States and European Union to be invalid.[83] In particular, the High Court focused on § 702 of FISA an Executive Order 12333.[84]

The High Court identified that the Attorney General of the United States and the Director of National Intelligence had the authority under § 702 of FISA[85] to approve surveillance of individuals other than United States citizens who were located outside of the United States, an authority which provided the basis for the PRISM and UPSTREAM programs.[86] Under PRISM, the Court found that internet service providers were required to supply the NSA with all communications to and from a selected individual.[87] Under UPSTREAM, the court found that the telecommunications providers were required to allow the NSA to copy internet traffic in order to acquire communications to and from non-U.S. citizens.[88] Executive Order 12333 provided even more expansive surveillance authority by authorizing the NSA to access data transmitted to the United States via underwater cables in the Atlantic.[89]

A primary concern of the High Court was the lack of significant protections for non-U.S. citizens.[90] Under U.S. law, the High Court found that intelligence activities conducted against non-U.S. citizens are limited only insomuch as they must be "as tailored as feasible."[91]

80. *Id.* at 55–56.
81. *Id.* at 57–58.
82. *Id.* at 59.
83. *Id*. at 60–61.
84. *Id.*
85. 50 U.S.C. § 1881a (2020).
86. *Schrems II*, 2020 EU:C:2020:559 at 61.
87. *Id.*
88. *Id.* at 62.
89. *Id.* at 63
90. *Id.* at 64.
91. *Id.*

Furthermore, EU citizens lacked the judicial remedies available to U.S. citizens, since they did not fall under the Fourth Amendment protections.[92] Even if such protections had been available to EU citizens, the High Court noted that the NSA's transatlantic cable surveillance under E.O. 12333 was not subject to any judicial oversight.[93] In attempting to defend the SCCs, Facebook argued that the Privacy Shield Framework, which the Commission had found to provide adequate data protections for the data of EU citizens, was binding on U.S. authorities such that even if the SCCs did not prevent mass surveillance of EU citizens, the Privacy Shield Framework would.[94] However, the High Court expressed doubt, noting that the Privacy Shield ombudsperson did not have sufficient judicial oversight powers to "afford EU citizens a level of protection essentially equivalent to that guaranteed by [EU law]."[95]

Accordingly, the Irish High Court stayed the proceedings and referred a series of eleven questions to the ECJ.[96] The ECJ reduced these questions to a set of five core questions, which were:

> (1) Does the processing of data for national security purposes by a non-EU country remove that data from the protections of the GDPR?[97]
>
> (2) What level of protection does the GDPR require? [98]
>
> (3) If a data transfer does not comply with the protections required by the GDPR, does that data transfer have to be shut down?[99]
>
> (4) Does the SCC decision ensure an adequate level of data protection?[100]
>
> (5) Does the United States, by virtue of its laws and international commitments, ensure an adequate level of

92. *Id.* at 65.
93. *Id.*
94. *Id.* at 66.
95. *Id.* at 65.
96. *Id.* at 68.
97. *Id.* at 68, 80.
98. *Id.* at 68, 90.
99. *Id.* at 68, 106.
100. *Id.* at 68, 122.

data protection?[101]

B. The Case

Prior to addressing these questions, the ECJ first needed to address a series of admissibility challenges brought by Facebook Ireland and the German and UK Governments.[102] Facebook Ireland's objection was that the referral from the Irish High Court was based on Directive 95/46, which after the referral had been repealed in favor of the GDPR.[103] Accordingly, Facebook Ireland argued the entire case was inadmissible.[104] However, the ECJ rejected this line of reasoning, holding that for purposes of the case, the relevant portions of Directive 95/46 were effectively identical to those in the GDPR.[105] The Court further stated that it had a duty not merely to answer the Irish High Court's questions themselves, but to interpret all provisions of EU law which the Irish High Court would need in order to decide the case, whether explicitly mentioned in the referral questions or not.[106]

The German government and the UK government objected on the grounds that the record of the case had not been sufficiently developed.[107] In response, the ECJ pointed to precedent which indicated that national courts referring matters to the ECJ enjoy a "presumption of relevance" and acknowledged that sufficient facts had been presented by the Irish High Court to make a ruling on each question.[108] It was clear from the factual record that Facebook Ireland did transfer data and that those transfers were made pursuant to the standard data protection clauses in the SCC decision.[109]

1. The First Question

After determining that the questions referred by the Irish High Court were admissible, the ECJ proceeded to assess whether the GDPR applied to data processed by third party countries acting in their

101. *Id.* at 68, 150. A complete listing of all questions can be found within the text of the decision. *Id.* at 68.

102. *Id.* at 69.

103. *Id.* at 70.

104. *Id.*

105. *Id.* at 71.

106. *Id.* (citing Case C-897/PPU, Ruska Federacija, 2020 EU:C:2020:262 at 43 (Apr. 2, 2020)).

107. *Id.* at 72. The German Government emphasized that it was unclear whether Schrems had consented to the data transfers at issue, and the UK Government emphasized that since it was unclear what data had been transferred, the entire case was purely a hypothetical one. *Id.*

108. *Id.* at 73-74.

109. *Id.*

national security capacity.[110] The ECJ confirmed that it did.[111] Because the GDPR expressly required the Commission, when making adequacy decisions, to assess "relevant legislation . . . concerning public security, defen[s]e, national security and criminal law and the access of public authorities to personal data. . .", the court held that the GDPR still applied, even in cases where state security was implicated or where data was processed by state security apparatuses.[112]

2. The Second, Third, and Sixth Questions

In response to the Irish High Court's inquiries regarding the level of data protection required under the GDPR, the ECJ affirmed that an "adequate level of protection" meant "a level of protection of fundamental rights and freedoms that is essentially equivalent to that . . . under the European Union by virtue of the regulation[.]"[113] In the absence of a finding by the European data authorities that a third party country provided an "adequate level of protection" i.e. the essential equivalence standard established in *Schrems I*, the controller or processer had to take "appropriate safeguards[.]"[114] In order to take "appropriate safeguards," the controller or processor must be capable of ensuring that their data protections provide the same protection in the third party country as in the European Union.[115] To determine what level of protection was adequate, the ECJ assessed (1) the contractual clauses (such as SCCs) binding the data controllers and processors in the EU and outside of the EU, (2) the degree of access that third party non-EU countries' public authorities had to the data, (3) the legal system of the third party country and (4) the specific remedies that legal system provided to EU citizens.[116]

3. The Eighth Question

Next, the court sought to identify the proper remedy in the event that there was not a finding of essential equivalence.[117] The Irish High Court questioned whether Article 58(2)(f) of the GDPR required the suspension of a data transfer to a third country if that third country offered insufficient protections to EU citizen's personal data.[118]

110. *Id.* at 80.
111. *Id.* at 86.
112. *Id.* at 86-89.
113. *Id.* at 94.
114. *Id.* at 95.
115. *Id.* at 96, 104.
116. *Id.* at 105.
117. *Id*. at 106.
118. *Id*.

Although the ECJ recognized that individual supervisory authorities had the discretion to determine what action was appropriate under particular factual circumstances, supervisory authorities were nonetheless required to "suspend or prohibit" transfers to non-EU countries where either SCCs were not or could not be complied with, or where "EU law cannot be ensured by other means."[119] Although the court appeared to give some leeway to these supervisory authorities to craft individual remedies, the ruling was nevertheless definitive in its statement that data transfers that were not adequately protected by SCCs or other law needed to be terminated.[120]

4. The Seventh and Eleventh Questions

Having resolved that where data transfers performed under SCCs did not provide adequate data protection, those data transfers must be terminated, the Court next turned to whether the SCC decision itself could ensure an adequate level of protection at all.[121] It was undisputed that SCCs did not and could not bind third party countries, who theoretically were free to process data in ways that denied EU citizens an adequate level of protection under EU law.[122] Here, the Court stated that while SCCs drawn up by the Commission theoretically could provide an essentially equivalent level of protection, it was the obligation of the controller or processor to provide adequate safeguards, including "effective legal remedies" and "enforceable . . . rights."[123]

The Court, however, acknowledged that such adequate safeguards might well be beyond the power of data controllers to provide, since after all, public authorities were free to circumvent or ignore those protections.[124] Therefore, the Court suggested that it may be necessary to "supplement" SCCs if said protections were circumvented or ignored by public authorities in a non-EU country.[125] However, the Court did not explain what these supplementary measures might entail.[126] The Court limited its analysis to concluding that in the absence of effective supplementary measures, data transfers

119. *Id.* at 113.
120. *Id.* at 121.
121. *Id.* at 123.
122. *Id.* at 125.
123. *Id.* at 131–32.
124. *Id.* at 132.
125. *Id.* at 133.
126. *Id.*

would need to be terminated.[127] Each data controller established in the EU seeking to transfer data out of the EU had an obligation, the Court ruled, to verify the level of protection it could provide.[128]

5. The Fourth, Fifth, Ninth, and Tenth Questions

Lastly, the Court considered whether the Privacy Shield Decision's finding that the United States provided an adequate level of protection was binding on the supervisory authority of member states.[129] Although Advocate General Øe had written a preliminary opinion suggesting that the Court could rule without actually addressing the United States or Privacy Shield, the Court declined to follow this guidance.[130] Because the controversy at issue was over the validity of SCCs, Øe's opinion had sidestepped the issue of Privacy Shield entirely, perhaps out of a desire to avoid invalidating the entire Privacy Shield Framework with potentially significant ramifications.[131] However, the ECJ noted that Facebook Ireland had claimed in the proceedings below that Privacy Shield was binding on data authorities in Europe and therefore, those data authorities did not have the authority to prohibit data transfers to the United States.[132]

Although the Court found that the Privacy Shield Decision was binding, it nevertheless reviewed the Privacy Shield Decision to determine whether it was valid.[133] The Court found that the Privacy Shield Decision was questionable in light of Section 702 of the FISA and E.O. 12333.[134] Because Section 702 of the FISA did not provide any limitations on the U.S. Government's power to implement surveillance programs targeted at non-U.S. persons, the Privacy Shield Decision, in order to be valid, would have to create an enforceable right to legal redress for EU citizens under surveillance.[135] For the ECJ, the existence of an effective legal redress in the U.S. was of "particular importance" in guaranteeing essential equivalence, and it was

127. *Id.* at 135 (noting, for example, where the laws of a third-party country rendered SCCs inadequate and there was nothing that supplementary measures could do, the data transfer could not go through).

128. *Id.* at 142.

129. *Id.* at 150.

130. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland, Ltd., ECLI:EU:C:2019:1145, Opinion of Advocate General Saugmandsgaard Øe.

131. *Id.* at 6, 171–73.

132. *Schrems II*, 2020 EU:C:2020:559 at 153, 156.

133. *Id.* at 160.

134. *Id.* at 178.

135. *Id.* at 181–82.

impossible to guarantee essential equivalence without it.[136] The ECJ's concerns went to the heart of the U.S. legal system. In particular, the ECJ raised concerns that without effective legislation permitting EU citizens to access data relating to themselves and obtain the "rectification or erasure" of that data when held by a third party, adequacy standards could not be met.[137] The Court particularly emphasized the threat posed by E.O. 12333, which authorized broad reaching surveillance with no hope of effective redress by EU citizens.[138]

The Privacy Shield Ombudsperson under the Privacy Shield Framework did nothing to allay the concerns of the ECJ.[139] The Privacy Shield Ombudsperson, the ECJ found, reported to the Secretary of State and thus was not independent from the U.S. Executive, even if they were ostensibly independent from the intelligence community.[140] Furthermore, the Ombudsperson did not provide any real legal remedy to EU citizens.[141] In light of these facts, the ECJ ruled that the Privacy Shield Decision was invalid just as it had previously struck down Safe Harbor.[142]

VI. ANALYSIS

Having struck down the Privacy Shield Decision, the ECJ has once again left U.S. based data controlling companies doing business within the EU in a state of uncertainty. This section argues that although companies and academics on the U.S. side of the Atlantic expressed a degree of shock and consternation in response to the ECJ decision,[143] when viewed in the context of historical trends in EU regulation, the ECJ was simply following the logical and inevitable outcome of EU laws.[144] Furthermore, when reviewing the history of

136. *Id.* at 189.

137. *Id.* at 187.

138. *See, e.g.*, *id.* at 183.

139. *Id.* at 190.

140. *Id.* at 195.

141. *Id.* at 196.

142. *Id.* at 201.

143. *See, e.g.*, Stewart Baker, *The Cyberlaw Podcast: Trumping Schrems II*, LAWFARE (Nov. 3, 2020, 11:05 AM), https://www.lawfareblog.com/cyberlaw-podcast-trumping-schrems-ii (criticizing the Schrems II decision as "hypocritical European imperialism"); Multi-Association Letter Responding to Schrems II, U.S. CHAMBER OF COM. (July 17, 2020), https://www.uschamber.com/sites/default/files/multi-association_letter_responding_to_schrems_ii_july_17_2020.pdf (expressing concern over the effects of the ECJ's decision to strike down Privacy Shield).

144. *See Infra* Part IV.A.

how the U.S. and the EU view data privacy, it becomes clear that there is a fundamental incompatibility in outlook; one which has hamstrung the past two attempts to reconcile EU and U.S. privacy law, first through Safe Harbor and later the Privacy Shield Decision.[145] Mechanisms such as the Privacy Shield's Ombudsman fail to address the fundamental differences in the two privacy regimes.[146] If the U.S. wants to maintain electronic data trade with the EU, without adopting laws analogous to the GDPR as California has, Japan provides an imitable model for future data privacy laws.[147] However, this represents a long-term solution.[148] In the short term, this section argues that there is no clear path forward; the confusing and highly varied responses of the U.S. government and various European data protection agencies indicate a lack of easy short-term answers for companies seeking to maintain data transfers across the Atlantic.[149]

A. The Schrems II *Decision was not Extraordinary but Inevitable*

On a fundamental level, the *Schrems II* decision follows the principles outlined by the ECJ in *Schrems I* and the principles outlined in the GDPR. *Schrems I* created the essential equivalence standard and the fundamental framework that underpinned the ECJ's understanding of essential equivalence.[150] Much of the ECJ's opinion was merely an affirmance of these principles.[151] Therefore, the decision of the ECJ in *Schrems II* should be seen as the predictable and logical outcome. After all, Privacy Shield did not represent a major deviation from Safe Harbor in terms of the protections it offered.[152] The underlying EU laws had not fundamentally changed in the interim between *Schrems I* and *Schrems II*, and the court utilized the same analytical framework—essential equivalence—that it had utilized in *Schrems I*.[153] Thus, in the absence of any substantive change in the law or in the EU-U.S. agreement, it is hard to imagine a different result. Despite the consternation that the decision has generated among some parties in

145. *See Infra* Part IV.B.

146. *Id.*

147. *Id.*

148. *Id.*

149. *See Infra* Part IV.C.

150. Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN L.J. 881, 899–900 (2017) (predicting in essence the process of comparison of U.S. domestic law and EU law that the ECJ would undertake).

151. *See supra* Part III.

152. *See supra* Part II.

153. *See supra* Part III.B.2.

United States,[154] the *Schrems II* decision fits within a historical trend of European data protection, a trend which reflects the importance of data privacy to EU citizens.[155]

However, in the field of data privacy, the European regulatory regime has historically been tempered by pragmatism: all parties recognize that some mechanism for the legal transfer of personal data is necessary, and that as valuable as the European data market is, it would be extremely harmful to Europe to have to close its borders to international, and specifically American, tech companies.[156] Thus, after the collapse of Safe Harbor, both sides rushed to create a new agreement as quickly as possible.[157] Privacy Shield was not merely a benefit to American companies; numerous European firms relied on it as well.[158] Even now, the European Union and the U.S. government have expressed mutual willingness to negotiate a new agreement.[159]

By contrast, the highest court in Europe appears to be acting out of a different and more fundamental set of values—not the pragmatism of the negotiators who have now drafted two sets of privacy frameworks in the past decade, only for each to be struck down in turn—but rather out of a concern for data privacy as a fundamental value enshrined in EU law.[160] The *Schrems II* decision could have been much more cautious—indeed, the ECJ perhaps could have avoided making a concrete ruling on the validity of the Privacy Shield Framework, as shown by the Opinion of Advocate General Øe.[161] The

154. This regulatory project has often been described in various hostile terms by U.S. commenters – as "hypocritical European imperialism" or the like. *See, e.g.*, Baker, *supra* note 143; *Multi-Association Letter Responding to* Schrems II, *supra* note 143.

155. European citizens remain highly concerned with the sharing of their personal data: 41% do not want to share "any personal data" with private companies. *Your Rights Matter; Data Protection and Privacy*, EUR. UNION AGENCY FOR FUNDAMENTAL RTS. (FRA) (2020), https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

156. EU-U.S. data transfers facilitate a transatlantic trade worth $7.1 trillion. *EU-US Privacy Shield for Data Struck Down by Court*, BBC (July 16, 2020), https://www.bbc.com/news/technology-53418898.

157. Zoya Sheftalovich, *5 Takeaways from the Privacy Shield*, POLITICO (Feb. 29, 2016), http://www.politico.eu/article/privacy-shield-agreement-takeaways-text-released/ ("[T]he Council's biggest concern is how quickly the new arrangement can be up and running.").

158. Cory, *supra* note 75.

159. Press Release, U.S. Department of Com., Com. Secretary Wilbur L. Ross at the U.S.-Ireland Economic Forum Virtual Meeting (Oct. 22, 2020) (on file with U.S. Department of Com.).

160. Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection Regulation?*, 114 AJIL UNBOUND 5, 7 (2020) ("[T]he [ECJ] has . . . strongly emphasized the right to data protection over countervailing interests, such as security and the free flow of information.").

161. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland, Ltd.,

Advocate General's Opinion completely avoided ruling on the Privacy Shield framework and instead focused on the SCC actually used by Facebook.[162] Ostensibly, only the SCC was actually at issue in this case, although the Irish High Court framed the issue more broadly.[163] In answering all the questions at issue, the ECJ left itself no choice but to strike down the Privacy Shield Framework.[164]

This decision, although widely accepted by the European Data Protection Authorities,[165] has also led to some concern. In an interview commenting on the ECJ's ruling, Stefan Brink, the Baden-Württemberg State Commissioner for Data Protection acknowledged that if European nations were required to prevent personal data transfers to the U.S., there would be significant economic harm to the EU as well as the U.S.[166] However, even in *Schrems I*, the ECJ clearly indicated that its considerations were not based on economics or pragmatism.[167] The ECJ, following its own fundamental rights law, established a stringent standard and it expected the Commissioner to uphold that standard.[168] U.S. companies are already experiencing the ramifications of such a standard. In September 2020, the Irish Data Commissioner reportedly instructed Facebook to stop data transfers to the U.S.[169]

B. The Incompatibility of the EU and U.S. Conceptions of Data Privacy

The ECJ likely had no choice but to open Europe up to this uncertainty and potential harm. At its core, the *Schrems II* decision necessarily accepts the GDPR and European privacy law as it has been

ECLI:EU:C:2019:1145, Opinion of Advocate General Saugmandsgaard Øe at 171–73.

162. *Id.* at 174–79.

163. *Schrems II*, 2020 EU:C:2020:559 at 68.

164. *See Data Prot. Comm'r*, ECLI:EU:C:2019:1145, at 186, 308 (refusing to rule on the issue of whether Privacy Shield provided essential equivalence, while acknowledging that if the court did, it was probable that the finding of adequacy would be overturned).

165. *See infra* Part IV.C.

166. *Der EuGH könnte seinen Hebel überschätzen* [translated as *"The ECJ Could Overestimate its Leverage"*], FRANKFURTER ALLGEMEINE (July 20, 2020), https://zeitung.faz.net/faz/politik/2020-07-20/22ea53d809ccc61cfe25da3e213e61e6/?GEPC=s3.

167. *See Schrems I*, 2015 EU:C:2015:650 at 32, 39.

168. *See id.* at 72–74.

169. Adrian Weckler, *Irish Data Regulator Orders Facebook to Stop Sending Personal Data to the US*, INDEPENDENT.IE (Sept. 9, 2020 at 10:36 PM), https://www.independent.ie/business/technology/irish-data-regulator-orders-facebook-to-stop-sending-personal-data-to-the-us-39518775.html.

established.[170] The real evaluative work of the decision is in its assessment of U.S. privacy law, an assessment which it is admittedly difficult for a foreign body to perform.[171]The ECJ's opinion of U.S. law may seem extreme; certainly, there has been no shortage of negative commentary on the ECJ from U.S. observers.[172] And certainly, the current situation has created difficulties for companies seeking to comply with EU data law and avoid what can be extremely steep fines.[173] However, the root of this decision comes from the fundamentally and potentially irreconcilable views of the right to privacy under U.S. and EU law.[174]

Under EU Law, the right to privacy is fundamental and generally cannot be contracted away.[175] The fundamental importance of privacy is enshrined in both the EU Data Protection Directive (95/46/EC) and in its successor, the GDPR.[176] EU policymakers traditionally favor comprehensive legislation establishing private and public principles for data privacy which are then enforced by data protection authorities.[177] For the EU "privacy is not only an individual right but also a social value."[178] Data protection itself is a fundamental right.[179] Although the EU recognizes that data protection interests must be balanced against competing national security, human rights, and other policy interests,[180] there is an understanding within the EU that because of the fundamental nature of the right to data protection, it has a non-negotiable character.[181] It is from this non-negotiable character that the concept of essential equivalence springs – the EU (and thus the ECJ) cannot abrogate its conception of data privacy for trade purposes.[182]

In comparison, the U.S. data privacy law is relatively restricted. The origins of data privacy in the United States arise out of a common law tradition which did not meaningfully recognize privacy as a

170. *Schrems II*, 2020 EU:C:2020:559 at 3–34.

171. *Kuner*, *supra* note 150, at 900.

172. Multi-Association Letter Responding to Schrems II, *supra* note 143.

173. GDPR, Art. 83 at 1–5.

174. *See infra* text accompanying notes 187–91.

175. EU Data Prot. Directive 95/46 at 10.

176. GDPR at 3–16.

177. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 22–24 (2012).

178. *Data Protection*, EUROPEAN DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection_en (last visited Dec. 19, 2020).

179. *Id.*

180. *Id.*

181. Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J.L. & TECH. 661, 668 (2020).

182. *Id*. at 670–71.

right.[183] The protection of privacy largely emerged out of the Fourth Amendment over a series of Supreme Court rulings.[184] This right was always somewhat circumscribed: for example, in *NASA v. Nelson*, the Supreme Court has suggested that there might be no right to informational privacy.[185] Further, the constitutional right to privacy within the U.S. context applies primarily to state actions, and purely private conduct is not protected.[186] Data protection in the U.S. has always relied upon a patchwork of federal and state laws, largely designed to protect not consumer data generally, but rather certain types of particularly sensitive data.[187]

Schrems I and *Schrems II* must be viewed in the context of these two very different privacy regimes. America has taken a less strict approach towards data protection, and one which, especially in the context of national security, does not meet the EU standards.[188] The sprawling nature of U.S. surveillance, combined with the lack of recourse for European data subjects, will likely make it impossible for a new EU-U.S. Privacy Framework to replace the Privacy Shield Framework.[189] The absence of limitations on the power of the United States surveillance apparatus to surveil "non-U.S. persons" was a critical consideration of the ECJ and is one which cannot be addressed without a change to U.S. law.[190] The ECJ was unable to identify any U.S. legislation that would provide effective judicial review of U.S.

183. Stephen Mulligan & Chris Linebaugh, *Data Protection Law: An Overview*, CONG. RSCH. SERV. 3 (Mar. 25, 2019) (noting that "solitude was readily available in colonial America" and that there were common law protections against eavesdropping and trespass, but no protection of an individual right to privacy as such).

184. *See, e.g.*, Katz v. United States, 389 U.S. 347, 350 (1967) (ruling that the Fourth Amendment does not create a general right to privacy); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that an individual retains some expectation of privacy with regard to cell phone site location information).

185. NASA v. Nelson, 562 U.S. 134, 159 (2011).

186. *Id.* at 158.

187. Stephen Mulligan & Chris Linebaugh, *Data Protection Law: An Overview*, CONG. RSCH. SERV. 3 (Mar. 25, 2019).

188. This is not to say, of course, that the EU does not restrict data privacy on the basis of national security concerns; quite the contrary. GDPR at 16.

189. *See Schrems II*, 2020 EU:C:2020:559 at 178. Although negotiations are underway to replace the Privacy Shield Framework, these negotiations have been hampered by the recent inauguration of President Biden due to changeover in personnel. Vincent Manancourt & Mark Scott, *Joe Biden Win Kicks US-EU Privacy Deal into the Long Grass*, POLITICO (Nov. 10, 2020) https://www.politico.eu/article/joe-biden-win-kicks-us-eu-privacy-deal-into-long-grass/. Also, President Biden and President Trump's stances on privacy and national security are not significantly different – a reflection perhaps of the gulf in policy between Europe and America on this issue. *Id.*

190. *Schrems II*, 2020 EU:C:2020:559 at 178–85.

surveillance and bulk data collection.[191] Therefore, in order to provide essential equivalence between U.S. and EU data protection laws, the United States would likely need to pass federal data privacy legislation. At the bare minimum, this law would need to provide enhanced protections for EU data subjects and effective redress for those data subjects under U.S. law.[192]

In order to move past *Schrems II* and create a privacy regime that is acceptable to the ECJ, one possible solution may be to look to foreign models which have been accepted as essentially equivalent.[193] Motivated by potential economic benefits, Japan has recently reformed its own data privacy laws, creating a two track model which ensures the protection of EU citizens' personal data at a higher level than its own domestic personal data.[194] The Japanese Constitution, like the U.S. Constitution, only implicitly recognizes the right to privacy.[195] Although Japan has not historically been deeply concerned with data privacy for its own citizens, the potential loss of access to European markets motivated a bilateral agreement.[196] In the future, Japan's two track approach may not be an isolated example: South Korea and India are seeking similar agreements which would allow them to maintain data trade with Europe.[197] However, there are significant downsides to such an approach: if the U.S. were to follow a similar path, it might take several years of negotiations, and a deal modelled on the Japanese would not provide protection for U.S. data subjects.[198]

A more sensible approach might be for the United States to move towards a data privacy regime more closely aligned with the European model.[199] The CCPA replicates various provisions of the GDPR, albeit

191. *Id.* at 187–90.

192. *Id.* at 189.

193. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information, 2019 O.J. (L 76) 1 at 4.

194. Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J.L. & TECH. 661, 689 (2020).

195. *Id.* at 669 (citing NIHONKOKU KENPŌ [KENPŌ] [CONSTITUTION], art. 13 (Japan)) ("All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.").

196. *Id.* at 667 (explaining that Japan's decision was motivated by a desire to retain access to EU markets and strengthen its own economy).

197. *Id.* at 672–73.

198. *Id.* at 671.

199. Dimitri Sirota, *California's new data privacy law brings U.S. closer to GDPR*, TECHCRUNCH (Nov. 14, 2020), https://techcrunch.com/2019/11/14/californias-new-data-

with a limited scope.[200] However, at the national level, there are few signs of any push towards a federal privacy bill.[201] There have only been infrequent debates in the Senate on this issue to date, and the current proposals fall significantly short of the GDPR.[202] Thus, U.S. based multinational companies attempting to comply with EU data law will not be able to rely in the short term on a legislative remedy from the U.S.

C. Reactions to the Schrems II Decision – Where do we go from here?

Schrems II did not provide substantial clarity on what affirmative steps companies could take to ensure compliance with the essential equivalence standard.[203] Thus, interpreting what measures are necessary has fallen to the European Data Protection Authorities, who themselves have offered a wide range of conflicting and often unclear advice.[204] Generally, the European Data Protection Authorities have expressed the need for some action or reassessment of current data privacy safeguards.[205] However, these responses still raise serious questions for companies seeking to comply with the new system as to what, if any, action is necessary.[206] Certain authorities, such as the

privacy-law-brings-u-s-closer-to-gdpr/.

200. Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKER HOSTETLER, LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

201. Emily Birnbaum, *Senators Inch Forward on Federal Privacy Bill*, THE HILL (Dec. 4, 2019), https://thehill.com/policy/technology/473071-senators-inch-forward-on-federal-privacy-bill.

202. Christian Fjeld, *Congressional Privacy Action – Part 1: The Senate*, NAT'L L. REV. (Jan. 28, 2020), https://www.natlawreview.com/article/congressional-privacy-action-part-1-senate; Mila Japser, *Senate Still Divided on Comprehensive Data Privacy Legislation*, NEXTGOV (Sept. 23, 2020), https://www.nextgov.com/analytics-data/2020/09/senate-still-divided-comprehensive-data-privacy-legislation/168725/ (explaining that only one of the proposed bills includes a private right of action, and the other proposed bill could actually substantially reduce data privacy protections by preempting stricter state laws).

203. *Schrems II*, 2020 EU:C:2020:559 at 168–202.

204. *See Data Transfers After Schrems II – the Response of Authorities*, PINSENT MASONS (Jan. 6 2021, 11:10 AM), https://www.pinsentmasons.com/out-law/guides/schrems-ii-the-response; *Responses to the Decision in Case C-311/18* (Schrems II), PAUL HASTINGS, www.paulhastings.com/docs/default-source/pdfs/2020_responses-to-privacy-shield.pdf?sfvrsn=d1e7daaa_28 (last accessed Dec. 19, 2020). Many of these agencies have provided what amount to neutral statements, merely summarizing the ruling of the ECJ without offering substantial commentary or clarification with regard to the ruling.

205. *Europe: Data Protection Authorities React to Schrems II Judgment*, ONETRUST DATA GUIDANCE (Oct. 2, 2020), https://www.dataguidance.com/news/europe-data-protection-authorities-react-schrems-ii.

206. *Id*; *see also Data Transfers After Schrems II – the Response of Authorities*, *supra* note 204; *Responses to the Decision in Case C-311/18 (Schrems II)*, *supra* note 204.

Baden-Württemberg State Commissioner for Data Protection, have taken a hard line stance, stating that a data controller relying on an SCC in the U.S. would certainly not be in compliance.[207] Similarly, the Berlin Commissioner ordered that personal data stored in the U.S. needed to be transferred to Europe.[208] As noted above, in the aftermath of the decision, Facebook was instructed by the Irish Data Commissioner to stop sending information to the U.S.[209]

More recently, in response to the *Schrems II* decision, the European Data Protection Board has issued recommendations for companies seeking to remain in compliance with EU data protection law.[210] These recommendations include advising data exporters to know what data is being transferred, rely on SCCs, BCRs, or some equivalent, and ensure that supplementary measures are taken to bring the level of data protection up to the EU standard.[211] While little guidance is given on what the supplementary measures should entail, they may have a "contractual, technical or organizational" nature, and may consist of encrypting all sensitive personal data belonging to EU data subjects.[212]

The advice to adopt supplementary measures, however, comes with the caveat that "[y]ou may . . . find that no supplementary measure can ensure an essentially equivalent level of protection[.]"[213] In such a case, the transfer must be suspended or terminated.[214] Taken in concert with regional and national data protection authorities comments indicating that data transfers to the United States cannot meet the essential equivalence standard, the safest step for a company operating in Europe would be to keep all data in Europe.[215]

207. *Europe: Data Protection Authorities React to Schrems II Judgment*, *supra* note 205.

208. *Id.*

209. Weckler, *supra* note 169.

210. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, EUR. DATA PROT. BD. 2–3 (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

211. *Id.* at 2.

212. *Id.* at 15.

213. *Id.* at 3.

214. *Id.* At every stage of the process, the burden is on the company to ensure that BCRs and SCCs are sufficient.

215. Private data protection associations have already launched a lawsuit against Amazon for exporting data out of Europe. *See, e.g.*, *EU Announces Lawsuit Against Amazon for Unlawful Data Transfers to the US*, DATAGUIDANCE (Oct. 9, 2020), https://www.dataguidance.com/news/eu-eugd-announces-lawsuit-against-amazon-unlawful-data.

The U.S. State Department[216] and Secretary of Commerce[217] have already expressed dissatisfaction with the *Schrems II* ruling, while offering little advice to companies seeking to comply. Remarks by the Secretary of Commerce reflected a commitment to finding an "enduring solution" but continue to be relatively short on specifics.[218] A recent white paper drafted at the behest of the State Department, and referenced in Ross' remarks, seeks to allay concerns that businesses may have regarding the *Schrems II* opinion. [219] The white paper focuses on the fact that "the overwhelming majority of companies" including those involved in the transmittal of "ordinary commercial information like employee, customer, or sales records" should have no reason to believe that U.S. intelligence agencies would seek to collect that data.[220] The paper goes on to critique strongly the ECJ's findings that U.S. data protections were inadequate, arguing, *inter alia*, that the FISC does have adequate oversight over U.S. surveillance agencies bulk data collection under FISA.[221] However, the white paper falls flat in arguing that there is an adequate remedy for EU data subjects under U.S. law, relying in particular on *Wikimedia Foundation v. National Security Agency*.[222] As the paper itself admits, certain data subjects may lack standing to sue.[223]

The upshot of these varying remarks is that it remains unclear what, if anything, U.S. based companies can do to comply with European data protection law. In light of U.S. surveillance, true compliance (absent government action) may be impossible, necessitating a system where no European data subjects' data is transferred outside of Europe.[224] However, this will have a vast and disproportionate effect on small and medium sized businesses.[225] Even for larger companies, data balkanization through banning data

216. Press Statement, Michael R. Pompeo, Sec'y of State, European Ct. of Justice Invalidates EU-U.S. Privacy Shield (July 17, 2020) (on file with the U.S. Dep't of State).

217. Press Release, U.S. Dep't of Com., U.S. Sec'y of Com. Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020) (on file with the U.S. Dep't of Com.).

218. Press Release, U.S. Dep't of Com., Com. Sec'y Wilbur L. Ross at the U.S.-Ireland Economic Forum Virtual Meeting (Oct. 22, 2020) (on file with U.S. Dep't of Com.).

219. Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After *Schrems II*, DEP'T OF COM., DEP'T OF JUST., OFF. OF THE DIR. OF NAT'L INTEL. 1–2 (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

220. *Id.* at 2.

221. *Id.* at 7.

222. *Id.* at 13.

223. *Id.*

224. *See supra* note 215.

225. *See supra* note 75.

transfers is not a realistic short-term solution.[226] Sufficient encryption of data combined with SCCs and the rigorous processes recommended by the EDPB appears to be the only sufficient short term answer.[227]

V. CONCLUSION

If *Schrems I* set the standard by which all future European adequacy decisions would be judged, *Schrems II* serves as a warning: essential equivalence cannot be met by minor revisions to a treaty. Given the substantial difference between European and American conceptions of privacy, substantive legislation, either modeled on the Japanese example or perhaps a nationwide version of the CCPA seems to be the only possible long-term solution, and even this would not be accomplished without years of negotiation and compromise. If the U.S. and EU were to simply renew Privacy Shield with cosmetic changes, the ECJ would likely strike it down. And yet, the longer it takes to construct such a solution, the more uncertainty will be generated by conflicting statements on both sides of the Atlantic, and the more harm that will be done to transatlantic data trade, and thus the global economy. There are no easy answers: indeed, the ECJ provided no answers at all.

226. For example, abolishing the transatlantic data trade would have massive deleterious effects on the medical and biomedical research industries, potentially causing substantial harms to people around the world. *See id*.

227. *See supra* note 210.