NOTES

Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems: Shattering the International Privacy Framework

I. OVERVIEW

Maximillian Schrems is an Austrian privacy advocate who filed a complaint regarding Facebook Ireland's transfer of personal data in 2015.[1] Facebook Ireland is a subsidiary of Facebook, Inc.[2] Facebook Ireland had been transferring the personal data of its users to the servers of Facebook Inc. in the United States.[3] Facebook Ireland users cannot create a Facebook account without agreeing to this transfer of their personal data from Facebook Ireland to Facebook, Inc.: it is a condition of the use of the service.[4] This is a typical practice for Facebook, generally accepted under the E.U.-U.S. Privacy Shield framework as well as the Standard Contractual Clauses, or SCCs, agreed to between the two entities.[5] Schrems argued that while the practice of transferring personal data did not violate the E.U.-U.S. Privacy Shield or SCCs, it violated E.U. law.[6] Schrems claimed that because Facebook, Inc. in the United States does not protect personal data to the extent required by E.U. law, it was a violation of E.U. citizen's privacy rights for Facebook Ireland to share their personal data with the U.S.-based Facebook, Inc.[7]

Specifically, in the United States, Facebook's data is open to government institutions such as the Federal Bureau of Investigation, while

1. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 50 (July 16, 2020).
2. *Id.* at ¶ 51.
3. *Id.*
4. *Id.*
5. *Id.* at ¶ 52.
6. *Id.* at ¶¶ 54-55.
7. *Id.*

in the E.U. these types of government entities do not have access to personal data collected by companies like Facebook Ireland.[8] Schrems first filed this complaint with the Irish Data Protection Commissioner.[9] The Commissioner filed the complaint against Facebook with the Irish High Court, who then referred the case to The Court of Justice of the European Union (CJEU).[10] The Irish High Court referred questions of the legitimacy of the E.U.-U.S. Privacy Shield, as well as questions about the legitimacy of SCCs in ensuring adequate data protection for E.U. citizens.[11] A preliminary decision on these questions was rendered in 2020.[12] The Court of Justice of the European Union *held* that the E.U.-U.S. Privacy Shield was invalid, because U.S. law does not give enough protection to satisfy E.U. law, and while SCCs themselves may still be used, organizations are responsible for implementing additional measures to protect personal data and cannot rely on SCCs alone. Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems*, http://curia.europa.eu/, (July 16, 2020).

II. BACKGROUND

Directive 95/46/EC, which went into effect in 1995, governed how personal data of E.U. citizens could be processed and transferred.[13] In 2018, the E.U. General Data Protection Regulation, or GDPR, replaced Directive 95/46/EC.[14] The GDPR and Directive 95/46/EC give the same general instructions and measures, but the GDPR is a more comprehensive piece of legislation, which applies to all companies that are involved in personal data transfers.[15] Under the GDPR, "personal data" includes any information that relates to a living individual.[16] This can include anything from tax ID numbers to a first and last name.[17]

---

8. *Id.*
9. *Id.*
10. *Id.* at ¶ 57.
11. *Id.* at ¶ 68.
12. *Id.* at ¶¶ 77-202.
13. Council Directive 95/46, 1995 O.J. (L 281) 1 (EC).
14. *European Union – Data Privacy and Protection*, INT'L TRADE ADMIN., https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection#:~:text=The%20EU%2DU.S.%20Privacy%20Shield%20Framework%20was%20designed%20by%20the,United%20States%20in%20support%20of (last visited December 18, 2020) [https://perma.cc/9SWN-6KX5] [hereinafter, EU Data Privacy and Protection].
15. EU Data Privacy and Protection, *supra* note 14; Council Directive 95/46, *supra* note 13.
16. EU Data Privacy and Protection, *supra* note 14.
17. *Id.*

Under the GDPR, personal data transferred outside the E.U. can only be exported if it is adequately protected.[18] Some countries have sought to have their framework approved by the European Commission. This way, companies can follow their own country's framework for data protection with pre-approved assurance that they are compliant with E.U. law. [19] The United States has not sought that approval by the European Commission.[20] Consequently, companies in the United States must take additional measures to ensure that they comply with E.U. privacy laws.[21]

Historically, U.S. companies could choose to show that their privacy protection was adequate in one of three ways: by joining the E.U.-U.S. Privacy Shield Program, providing safeguards agreed to in SCCs, or referring to a GDPR derogation.[22] Many companies chose to use the Privacy Shield Program, which was designed jointly by the European Commission and the U.S. Department of Commerce, because it provided a clear framework to ensure compliance with both United States and E.U. privacy laws when collecting and transferring personal data.[23] The Privacy Shield Program contains principles on data that can be collected, liability for data protection, access, and verification requirements that companies must follow.[24] When a U.S. company commits to compliance with these principles, the commitment is enforceable under U.S. law, even if some of the principles require higher levels of protection than those required by other U.S. privacy laws.[25]

The purpose of this framework was to ensure that companies based in the United States, but collecting data of E.U. citizens, adequately protected E.U. users' data according to E.U. standards, and vice versa.[26] Companies can also use SCCs to either supplement the protections required by the Privacy Shield Program, or to completely bring the companies into compliance with the required privacy protections.[27] SCCs are clauses agreed to by both parties, often included as part of the companies' contracts or business plans as a whole, that describe the

18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Privacy Shield Program Overview*, INT'L TRADE ADMIN., https://www.privacyshield.gov/Program-Overview (last visited December 18, 2020) [https://perma.cc/F62N-X8LS].
24. *Id.*
25. *Id.*
26. *Id.*
27. EU Data Privacy and Protection, *supra* note 14.

measures that will be taken to protect the personal data of the companies' users.[28]

In the United States, the Foreign Intelligence Surveillance Act allows the United States to gather foreign intelligence information and conduct surveillance on individuals who are not United States citizens to protect against acts such as terrorism.[29] The Act is strengthened by Executive Order 12333, signed by President Reagan in 1981, which authorizes the National Security Association to procure information and surveillance of U.S. and foreign citizens via electronic communications.[30] Some of the provisions in the Foreign Intelligence Surveillance Act and Executive Order 12333 are in direct conflict with the personal data protections outlined in the Privacy Shield Program.[31] This conflict is what led to the noted case, which raised the question of whether the Privacy Shield Program could truly grant E.U. individuals the rights required to protect their personal data.[32]

III. COURT'S DECISION

In the noted case, the Court of Justice of the European Union decided that the Privacy Shield Program could not grant the necessary protection required by E.U. law.[33] Facebook was required to stop sending E.U. citizens' data to the United States.[34] SCCs are still valid under the noted case, though they are no longer sufficient on their own to satisfy the required privacy safeguards.[35] Now, on a case-by-case basis, parties must assess the privacy laws in the countries of each entity, and the safeguards implemented by the SCC proposed in that specific situation, and determine whether additional safeguards are required to create an adequate

28. Haley Evans, *What Does Schrems II Mean for the U.K.?*, LAWFARE (July 29, 2020), https://www.lawfareblog.com/what-does-schrems-ii-mean-uk [https://perma.cc/WK4A-K3ZQ].

29. 50 U.S.C. § 1802.

30. 50 U.S.C. § 1802; Exec. Order No. 12333, 3 C.F.R. § 200 (1981).

31. 50 U.S.C. § 1802; Exec. Order No. 12333; *Privacy Shield Program Overview*, *supra* note 23.

32. 50 U.S.C. § 1802; Exec. Order No. 12333; *Privacy Shield Program Overview*, *supra* note 23; Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 52 (July 16, 2020).

33. Case C-311/18, Data Prot. Comm'r, at ¶ 181; *Schrems II Landmark Ruling: A DetailedAnalysis*, NORTON ROSE FULBRIGHT (July 2020), https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis.

34. *Max Schrems v. Data Protection Commissioner (CJEU – "Safe Harbor")*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/intl/schrems/ (last visited Dec. 18, 2020) [https://perma.cc/M58J-YDH5].

35. *Schrems II Landmark Ruling: A Detailed Analysis*, *supra* note 33.

protection of personal data.[36] The most relevant focus in the court's decision was surveillance laws.[37] When public authorities can access the data of the importing entity, additional safeguards may be required to ensure that E.U. citizens' data is not accessible to these foreign public authorities.[38] However, the validity of SCCs are only half of the equation considered by the CJEU in the noted case.[39]

Unlike the SCCs, which were held to still have a place in E.U. privacy law, the E.U.-U.S. Privacy Shield was considered to be entirely invalid by the CJEU.[40] In the United States, surveillance programs are not limited to what is strictly necessary, which is the threshold required in the E.U. to access personal data.[41] Further, E.U. citizens do not have an actionable judicial recourse when their rights are violated by U.S. surveillance, which is in violation of E.U. Charter Article 47.[42] United States citizens are protected by the Fourth Amendment of the Constitution, and may seek recourse under the Fourth Amendment if their privacy rights are violated.[43] E.U. citizens, as foreign nationals, do not have this same legal recourse if their privacy rights are violated in the United States.[44]

In the United States, public entities like the Federal Bureau of Investigation can access personal data stored by companies like Facebook.[45] This access conflicts with E.U data protection laws, because similar public entities in the E.U. do not have comparable overriding access to citizens' personal data.[46] Even when a company like Facebook

---

36. *Id.*

37. *Id.*

38. *Id*; Marios Christodoulou, *Cyprus: Case C-311/18 Data Protection Commissioner V Facebook Ireland and Maximillian Schrems: Landmark CJEU Decision Invalidates EU – U.S. Privacy Shield*, MONDAQ (Aug. 20, 2020), https://www.mondaq.com/cyprus/privacy-protection/977936/case-c-31118-data-protection-commissioner-v-facebook-ireland-and-maximillian-schrems-landmark-cjeu-decision-invalidates-eu-us-privacy-shield, [https://perma.cc/9X6A-PSBF] [hereinafter, *Cyprus*].

39. *Cyprus*, *supra* note 38.

40. *Id.*

41. 50 U.S.C. § 1802; Exec. Order No. 12333; Caitlin Fennessy, *The Schrems II Decision: EU-US Data Transfers in Question*, IAPP (July 16, 2020), https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/; Charter of Fundamental Rights of the European Union, art. 52, Dec. 14, 2007, 2007 O.J. (C 303).

42. 50 U.S.C. § 1802; Exec. Order No. 12333; Fennessy, *supra* note 41; Charter of Fundamental Rights of the European Union, art. 47, Dec. 14, 2007, 2007 O.J. (C 303).

43. U.S. CONST. amend. IV.

44. *Id.*; U.S. CONST. art. III, § 1.

45. 50 U.S.C. § 1802; Fennessy, *supra* note 41; Exec. Order No. 12333; Charter of Fundamental Rights of the European Union, art. 47, Dec. 14, 2007, 2007 O.J. (C 303).

46. 50 U.S.C. § 1802; Exec. Order No. 12333; Fennessy, *supra* note 41; Charter of Fundamental Rights of the European Union, art. 47, Dec. 14, 2007, 2007 O.J. (C 303).

complies with the E.U.-U.S. Privacy Shield Program, they cannot adequately protect the data of E.U. citizens because of this extended access by public entities.[47] In the noted case, the CJEU determined that this completely invalidates the Privacy Shield Program, which is not binding on U.S. authorities and therefore cannot protect E.U. citizens to the extent required by the Charter.[48]

The Advocate General stated in his Opinion that any guarantees made through SCCs or the Privacy Shield Program must be protected on a basis essentially equivalent to the protection afforded within the European Union to be considered an adequate protection.[49] This decision applies to the transfer of personal data of E.U. citizens to any third country, though in this particular case it is the laws and protections afforded by the United States that were being questioned.[50] It is for this reason that SCCs were deemed valid but not sufficient on their own, while the Privacy Shield Program was deemed ineffective entirely.[51] The CJEU noted the factors that should be taken into consideration for purposes of determining protection adequacy for personal data include the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer in the third country, as well as the access by public authorities of the third country.[52] Therefore, even in agreements where both the controller and the recipient of the transfer have contracted to protect the personal information of E.U. citizens, the transfer will be in violation of the GDPR and thus incompatible with E.U. law if the access of public authorities in the recipient country go beyond that which may be allowed in the European Union.[53]

The CJEU also ruled on whether transfers of personal data must be suspended or prohibited where a third country does not comply with the protection of data required by E.U. law.[54] In the European Union, there are supervisory authorities that monitor application of the GDPR and ensure its enforcement both within the E.U. and in data transfers to other countries.[55] These supervisory authorities have investigative powers and

47. 50 U.S.C. § 1802; Exec. Order No. 12333; *Cyprus*, *supra* note 38.

48. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 185 (July 16, 2020).

49. *Id.* at ¶ 96.

50. *Id.* at ¶ 1.

51. *Id.* at ¶¶ 146-48.

52. *Id.* at ¶ 104; General Data Protection Regulation, art. 46, 2016 O.J. (L 119) 1, 2.

53. General Data Protection Regulation, art. 46, 2016 O.J. (L 119) 1, 2; Case C-311/18, Data Prot. Comm'r at ¶ 105.

54. Case C-311/18, Data Prot. Comm'r at ¶ 106.

55. *Id.* at ¶ 107; General Data Protection Regulation, art. 57, 2016 O.J. (L 119) 1.

must take appropriate action where their investigation leads to a finding of a violation under the GDPR.[56] The Advocate General stated affirmatively that when a supervisory authority finds a breach of the GDPR, where personal data is not adequately protected, the supervisory authority is required to suspend or prohibit the transfer of that data where necessary.[57] In the noted case, because the personal data must be transferred to the United States as a condition of using Facebook Ireland, and the United States public authorities have access to this personal data, Facebook is in violation of the GDPR of the European Union.[58] Therefore, the transfer of this personal data must necessarily be suspended until the fundamental right of privacy protected in the E.U. can be adequately protected while the data is in the United States.[59]

Likewise, though SCCs are not invalid, an SCC between Facebook Ireland and Facebook, Inc. would not adequately protect E.U. citizen's personal data, and therefore an SCC could not be relied on as satisfying the privacy requirements of the GDPR in and of itself.[60] Overall, the transfer of personal data to the United States for commercial purposes is in conflict with the GDPR and therefore in conflict with the fundamental rights of the E.U. and cannot be remedied by SCCs or the Privacy Shield Program alone because the issue lies in the accessibility of this personal data to public authorities, not the privacy of the data within the receiving company itself.[61]

IV. ANALYSIS

This case was certainly a landmark decision, which resulted in the upheaval of privacy and data protection systems that have been in place for years.[62] Companies have relied on SCCs and the Privacy Protection Program in the United States, assuming that compliance with these safeguards guaranteed compliance under the GDPR.[63] The invalidation of the E.U.-U.S. Privacy Shield program will result in a scrambling by many

56. Case C-311/18, Data Prot. Comm'r at ¶¶ 111-13; General Data Protection Regulation, art. 57, 2016 O.J. (L 119) 1.

57. Case C-311/18, Data Prot. Comm'r at ¶ 113.

58. *Id.* at ¶¶ 122-25.

59. *Id.* at ¶¶ 122-25; General Data Protection Regulation, art. 57, 2016 O.J. (L 119) 1.

60. Case C-311/18, Data Prot. Comm'r at ¶¶ 122-25; General Data Protection Regulation, art. 57, 2016 O.J. (L 119) 1.

61. Case C-311/18, Data Prot. Comm'r at ¶ 125; General Data Protection Regulation, art. 57, 2016 O.J. (L 119) 1.

62. Fennessy, *supra* note 41.

63. *Id.*

businesses to find new ways to ensure their data collection and transfer systems comply with E.U. law.[64] Further, the decision has opened questions as to whether there are actions U.S. companies can take that would completely satisfy E.U. requirements, as companies cannot limit the access that public authorities have to personal data under the Foreign Intelligence Surveillance Act.[65]

On the one hand, the CJEU has received praise for its continued protection of personal data in the European Union.[66] The Privacy Shield Protection Program has been critiqued by the European Data Protection Supervisor (EDPS) for several years, as it did not protect the "actionable rights" guaranteed in the European Union.[67] The EDPS has also pushed for several years for clarification on the duties of supervisory authorities to stop the transfer of data that does not conform with E.U. mandated protections when these authorities encounter them.[68] The noted case provides the requested clarity on the duties of supervisory authorities, explaining that they are required to suspend or prohibit the transfer of personal data in cases where an investigation has led to a finding of non-compliance with E.U. law.[69]

On the other hand, however, this decision will require many companies to change their current data sharing plans to comply with E.U. law.[70] Where before companies could rely on SCCs or the Privacy Shield alone, they are now left with only one other option: relying on derogations.[71] Derogations are exceptions to the requirements for personal data transfers.[72] Derogations include aspects such as consent, necessity, and compelling legitimate interests as valid exceptions for companies transferring personal data that is not adequately protected under the

64. *Id.*

65. *Id.*; 50 U.S.C. § 1802

66. 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/7TH4-V5DV].

67. *Id.*

68. *Id.*

69. *Id.*

70. Brandon Moseberry & Florian Tannen, *What 'Schrems II' Means for Companies That Rely on Derogations*, IAPP (July 24, 2020), https://iapp.org/news/a/what-schrems-ii-means-for-companies-that-rely-on-derogations/, [hereinafter, Moseberry].

71. *Id.*

72. General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1.

GDPR.[73] However, these derogations are narrowly tailored and are not meant to be used as a daily loophole to the GDPR.[74] Companies in the United States will need to find new ways to comply with the laws of the E.U., whether it is by enhanced SCCs or other new safeguards to protect E.U. citizens' personal data.[75] Some companies, such as those involved with healthcare or financial services who are subject to more extensive government oversight, may have trouble complying with the GDPR at all, regardless of their use of SCCs or derogations, because public authority access will still be so vast that it may conflict with the GDPR.[76] In fact, it is possible that currently most companies that engage in personal data between the U.S. and E.U. cannot adequately comply with the GDPR in light of the noted decision.[77]

The U.S. Department of Commerce Secretary Wilbur Ross expressed his disappointment in the invalidation shortly after the decision was rendered and voiced his hope that further collaboration could lead to a more uniform solution to privacy and personal data protection between the U.S. and E.U.[78] In the meantime, U. S. companies are looking to SCCs and derogations, such as consent, to conform with E.U. law.[79]

The derogation of consent, which seems to be a viable option for companies to use in this interim of uncertainty as to the compliance of E.U. privacy laws, is very narrowly tailored.[80] The consent must be explicit, and the subject of the data transfer must have been informed of any possible risks of such transfers.[81] The derogation of necessity, which will likely also

---

73. Moseberry, *supra* note 70; General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1.

74. Moseberry, *supra* note 70; General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1.

75. Moseberry, *supra* note 70; General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1; Kaylee Cox Bankston, et al, *Schrems II Decision: Immediate Considerations for U.S. Businesses*, JD SUPRA (July 17, 2020), https://www.jdsupra.com/legalnews/schrems-ii-decision-immediate-33271/, [https://perma.cc/4PS8-8BDY].

76. Bankston, *supra* note 75; *see* General Data Protection Regulation, art. 49-51, 2016 O.J. (L 119); Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 89 (July 16, 2020).

77. Bankston, *supra* note 75; *see* General Data Protection Regulation, art. 49-51, 2016 O.J. (L 119); Case C-311/18, Data Prot. Comm'r at ¶ 89.

78. *Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*, U.S. DEPT. OF COM. OFF. OF PUB. AFF. (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and [https://perma.cc/8A3H-VAYE] [hereinafter Wilbur Ross Statement].

79. Fennessy, *supra* note 41.

80. Bankston, *supra* note 75; *see* General Data Protection Regulation, art. 49-51, 2016 O.J. (L 119); Moseberry, *supra* note 70.

81. General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1.

be relied on heavily in the wake of the CJEU's decision, requires that the transfer of data is necessary for performance of a contract between the data subject and the controller, the transfer is necessary for the conclusion of the contract in the interest of the data subject, the transfer is necessary for important reasons of public interest, or the transfer is necessary to protect the interests of the data subject in either legal claims or where the subject is incapable of giving consent.[82] These narrowly tailored derogations do not lend themselves to the typical business practices of companies such as Facebook, where there is no necessity to protect the interests of the data subject and consent would be a requirement of using the service at all, since Facebook Ireland is a subsidiary of Facebook, Inc. and the Facebook, Inc. servers are located in the United States.[83]

The decision by the CJEU was rendered in July of 2020.[84] Since then, the implications of this confusing decision have been anti-climactic in light of the potential confusion that could have been caused for U.S. companies.[85] The oversight regulatory bodies that were determined to have a duty to suspend or prohibit the transfer of data in occurrences of non-compliance with the GDPR have taken very little action against U.S. companies so far.[86] It is unclear whether this is a result of the newness of this decision, and regulators will soon begin issuing more suspensions, or not.[87] Regardless, many U.S. companies are left in a "limbo" for the time being.[88] They have been told that their current system is no longer enough, but have not yet been given clear guidance on how to remedy the situation, whether that be through enhanced SCCs, derogations, or through other measures not yet established between the E.U. and United States.[89] Businesses that transfer personal data between the E.U. and the United States may not find a clear solution for months or even years.[90]

---

82. *Id*; Bankston, *supra* note 75.

83. General Data Protection Regulation, art. 49, 2016 O.J. (L 119) 1; Bankston, *supra* note 75; European Data Protection Supervisor Press Release, *supra* note 66; Evans, *supra* note 28.

84. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, (July 16, 2020).

85. *See Id*; Dan Cooper et al., *Life After Schrems II: Practical Recommendations in an Uncertain Time*, COVINGTON & BURLING (Sept. 4, 2020), https://www.insideprivacy.com/cross-border-transfers/life-after-schrems-ii-practical-recommendations-in-an-uncertain-time/ [https://perma.cc/S3W5-VE4K].

86. Cooper, *supra* note 85; *see* case C-311/18, Data Prot. Comm'r.

87. Cooper, *supra* note 85.

88. *Id.*

89. *Id.*

90. *Id.*

V. CONCLUSION

The noted decision was groundbreaking, in that it requires the restructuring of personal data protection guarantees for many companies operating in the United States.[91] At the time of the noted decision, there were more than 5,300 Privacy Shield Program participants who now need to restructure their privacy safeguards.[92] However, the decision was made before any adequate remedy or replacement program was prepared, and very little guidance has been offered thus far on how businesses can protect the data of their E.U. citizen users adequately under the GDPR.[93] Both U.S. and E.U. officials have expressed interest in preparing a new program to uniformly protect users' personal data, but in the meantime businesses must rely on strengthening their SCCs and using derogations to ensure compliance.[94] Regardless of future remedies, it is clear from this decision that there is a problematic misalignment between E.U. privacy law and United States public authority access to the personal data of foreign citizens.[95]

Julia Hamilton*

91. *Id.*; *See* case C-311/18, Data Prot. Comm'r.
92. Wilbur Ross Statement, *supra* note 78.
93. *See* case C-311/18, Data Prot. Comm'r; Wilbur Ross Statement, *supra* note 78.
94. Fennessy, *supra* note 41.
95. *See* case C-311/18, Data Prot. Comm'r.

* © 2021 Julia Hamilton, J.D. Candidate Tulane University School of Law 2022. B.B.A. Texas A&M University 2017.