Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States

Allison Callahan-Slaughter*

I. OVERVIEW

An enormous amount of data is exchanged between the United States and the European Union every day, amounting to billions of dollars every year.[1] Due to divergent data protection and privacy laws,

 J.D. candidate, 2017, Tulane University Law School; B.S. and B.A. 2012, Virginia Tech. I would like to thank NCS, for always supporting and believing in me, no matter the pursuit.

1. Gregory Shaffer, *Globalization and Social Protection: The Impact of the EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 39 (2000); *see also* Stephanie Schiedermair, *The New General Data Protection Regulation of the*

conflicts arise when data subject to more robust protection in the EU is transferred to the United States.[2] This dispute between the EU and United States over data and privacy protection has the potential to affect U.S. domestic policy.[3] By using its considerable market power as bargaining leverage, the EU has the capacity to facilitate change beyond its borders and strengthen other nations' data protection safeguards.[4] This Comment strives to find a balance between these differing approaches to privacy and data protection by focusing on developments in transnational data security following the invalidation of Safe Harbor, specifically, the recently accepted EU-U.S. Privacy Shield agreement and the EU General Data Protection Regulation.

Part II of this Comment details the different legal and historical approaches to privacy in both the United States and EU. Part III explains the impact of these divergent privacy approaches on the transnational transfer of data. Part IV looks forward to the future impact of the recent policy changes. Lastly, Part V presents closing remarks in the wake of recent global security concerns and their potential effect on privacy protections.

II. EXAMINATION OF THE DIFFERING APPROACHES TO PRIVACY BETWEEN THE EU AND THE UNITED STATES

A. European Union Protection of Data: The EU Data Protection Directive 95/46/EC

The European Union's approach to privacy is premised on the notion that individual privacy is a fundamental human right and should be afforded stringent protections.[5] The strong protections attached to individual privacy are not surprising considering most Europeans are but one or two generations removed from fascist or communist governments that strictly monitored citizens' personal lives.[6] With first-hand experience of the dangers of governmental intrusions, the EU provides sweeping safeguards for its citizens' individual privacy.[7]

European Union-Will it Widen the Gap Between Europe and the U.S.?, *in* PERSPECTIVES ON PRIVACY: INCREASING REGULATION IN THE USA, CANADA, AUSTRALIA AND EUROPEAN COUNTRIES 71 (Dieter Dörr & Russell L. Weaver eds., 2014).

2. Schiedermair, *supra* note 1, at 71.

3. Shaffer, *supra* note 1, at 39.

4. *Id.*

5. THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 250 (2014).

6. *Id.* at 250.

7. *Id.*

The current data policy, the EU Data Protection Directive (the Directive), unifies the privacy policies of individual EU Member States to ensure the unimpeded flow of data between countries.[8] In response to the need for unification due to the threat of transfer bans between Member States, the Organisation for Economic Co-operation and Development (OECD) issued a recommendation containing eight privacy principles: collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation, and accountability.[9] The EU Data Directive would eventually extract and incorporate all eight of the OECD Privacy Principles into its own standards, making the guidelines binding on all EU Member States.[10] Due to France's and Germany's political exploitation of their considerable market power, the Directive represents stricter privacy standards than those advocated by the less stringent countries of the EU, such as Italy.[11]

The Directive regulates the processing of all personal data of EU citizens.[12] Under the Directive, personal data represents "any information relating to an identified, or identifiable natural person (data subject)."[13] Data is considered personal when it enables anyone at all to link information to a specific person, even if the person or entity actually holding that data cannot make that link.[14] "Processing" is also broadly defined and involves any operation on personal data, manual or automated, including its collection, recording, organization, modification,

---

8. For example, Italy had less rigorous data protection laws while France was more protective. Prior to its enactment, there were differing standards within the EU, only unified under the broad privacy protection provided by the European Convention on Human Rights. Shaffer, *supra* note 1, at 10.

9. These Privacy Guidelines are credited with having an enormous impact on many legislative and self-regulatory adaptations and were extended to trans-border data flows. Org. for Econ. Cooperation & Dev. [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, at 14-15, C(80)58/FINAL (1985), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; *see also* Sunni Yuen, *Exporting Trust With Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 41, 61-62 (2008).

10. *See* Council Directive 95/46, art. 2, 1995 O.J. (L 381) 31, 38 (EC) [hereinafter Data Directive].

11. Shaffer, *supra* note 1, at 12.

12. Data Directive, *supra* note 10, art. 3.

13. The Directive balances privacy protections against the free flow of information by only applying to "personal data," allowing the collection and processing of information about corporate entities. *Id.* art. 2(a).

14. Examples include address, bank statements, and credit card numbers. *Id.* art. 2(a).

publication, or transmission.[15] Thus, from the Directive's view, data is considered "processed" the minute it is collected.

Except for in instances involving criminal law and national security, the Directive covers all processing of personal data without limitation by business or field of use, covering both public and private processing of data.[16] The Directive also highlights the need to protect personal data related to certain sensitive categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health, and sexual activity.[17] Member States reserve the right to exempt certain activities through their national legislation as long as the exemptions do not contravene the Directive's standards.[18]

The Directive mandates what steps must be taken prior to processing personal data and creates strict ex-ante controls on data controllers.[19] Data can only be gathered legally while complying with transparency, legitimate purpose, and proportionality requirements.[20] Under the transparency requirement, an individual has the right to be informed when his or her personal data is being processed and the controller must provide all information to ensure processing is fair.[21] Under the legitimate purpose requirement, personal data can only be processed for specified and legitimate purposes.[22] Finally, under the proportionality requirement, personal data may be processed only so far as it is adequate, relevant, and not excessive in relation to the purposes for which it is collected or further processed.[23] Data controllers are also required to inform the data subject of the controller's identity, the purposes of the processing, and other necessary information to ensure fair processing.[24] Individuals also have rights over the use of their information after it is processed through the Directive's ex-post controls.[25] The Directive guarantees individuals a permanent right of access to

---

15. *Id.* art. 2(b).

16 Unlike in the United States, where private data processing is primarily self-regulated. *Id.* art. 2.

17. *Id.*

18. *Id.* arts. 9, 13.

19. Shaffer, *supra* note 1, at 13.

20. *See* Data Directive, *supra* note 10, art. 7.

21. *Id.* arts. 10, 11.

22. *Id.* art. 6(1)(b).

23. Additionally, when the data involves any of the previously mentioned sensitive categories, further restrictions apply. *Id.* art. 6(1)(d).

24. *Id.* art. 10.

25. Shaffer, *supra* note 1, at 16.

obtain copies of the data about them, have it corrected, and receive confirmation of the purposes of its processing.[26]

Lastly, individuals are given substantial enforcement rights under the Directive.[27] To allow for effectual enforcement, Member States must designate a national data protection authority (DPA) tasked with monitoring the application of data protection law within their individual territories.[28] The States' significant powers include: investigative powers, such as access to data and powers of collection;[29] effective powers, such as ordering the blocking of data or imposing temporary bans on the processing or admonishing the controller;[30] legal proceedings power when national provisions have been violated;[31] and, jurisdictional powers to hear claims lodged by any person concerning protection of rights with regards to processing of personal data.[32] Member States are also expected to provide a judicial remedy for data privacy infringement, including a right to receive damages.[33]

B. U.S. Protection of Data: A Sectoral Approach

Unlike the overarching EU Directive, the U.S. data protection regime is ad hoc, decentralized, and narrowly tailored, placing its emphasis on market constraints rather than government intervention.[34] To some degree, this lack of an overarching governmental protection can be attributed to the U.S. public's historical disfavor of a centralized government and a preference for unrestricted flow of information.[35] The piecemeal regulation also showcases another important facet of U.S. regulation; reactive in nature, regulation tends to respond to privacy issues in the wake of highly publicized privacy breaches.[36]

The right to privacy in the United States centers on a limited amount of specific areas where protection is deemed necessary and is based on a patchwork of vehicles, namely the Constitution, federal and

---

26. Data Directive, *supra* note 10, art. 12.
27. Shaffer, *supra* note 1, at 16.
28. *Data Protection Bodies*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/bodies/index_en.htm (last visited Nov. 4, 2016).
29. Data Directive, *supra* note 10, art. 28(3).
30. *Id.*
31. *Id.*
32. *Id.* art. 28(4).
33. Data Directive, *supra* note 10, arts. 22-24.
34. Shaffer, *supra* note 1, at 22.
35. *Id.* at 22-23.
36. For example, the Fair Credit Reporting Act was passed in response to consumer complaints regarding credit reporting agencies. Yuen, *supra* note 9, at 53.

state legislation, and market self-regulation.[37] While the United States Constitution does not explicitly guarantee a general right to privacy, it provides limited protections for certain privacy rights in the First, Fourth, Fifth, and Fourteenth Amendments.[38] The United States Supreme Court first addressed the issue of informational privacy in *Whalen v. Roe*, recognizing an individual's right to have his personal information remain private.[39] In subsequent decisions, the Court has narrowly tailored the right to privacy, determining it only exists when a citizen has a "reasonable expectation of privacy" and, once information is disclosed to a third party, this expectation no longer exists.[40] Additionally, these constitutional protections only extend to unwarranted governmental invasions and do not extend to infringements by private actors.[41] Thus, under U.S. law, the private sector is subject to significantly less regulation over the use of personal information than the public sector.[42]

Federal U.S. privacy legislation has taken an industry-sectorial approach, with Congress enacting statutes in a piecemeal manner to target specific privacy concerns in governmental agencies, industries, or economic sectors.[43] The primary omnibus federal privacy regulation is the 1974 Privacy Act, setting standards for the collection, maintenance, and dissemination of personal data.[44] Only data processing conducted by the federal government is under the Act's purview, excluding state government and private sector processing.[45] The center of the Privacy Act's protection is its prohibition on the disclosure of personal information absent written consent of the individual subject.[46] However,

---

37. PAYTON AND CLAYPOOLE, *supra* note 5, at 248-49; *see also* Yuen, *supra* note 9, at 53.

38. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 220 (1999); *see also* Paul v. Davis, 424 U.S. 693, 712-13 (1976).

39. *See* Whalen v. Roe, 429 U.S. 589, 605-06 (1977) (concerning a New York law that created a central file of persons who obtained prescription drugs and individual's right to keep medical information private).

40. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (J. Harlan, concurring); *see also* Smith v. Maryland, 442 U.S. 735, 740-41 (1979).

41. For example, there is no constitutional protection available for the extensive profiling Facebook conducts on its users' personal data. *See* Cate, *supra* note 38, at 220.

42. Shaffer, *supra* note 1, at 28.

43. Examples of federal statutory protections include the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act. *Id.* at 22.

44. *See id.* at 23; Privacy Act of 1974, Pub. L. No. 93-579, § 2(b)(6), 88 Stat. 1896, 1896 (1974), reprinted in 5 U.S.C. § 552a note at 769 (1982).

45. Shaffer, *supra* note 1, at 23.

46. "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . ." Privacy Act of 1974 at 760.

this prohibition is subject to twelve statutory exceptions permitting non-consensual disclosure to U.S. government agencies.[47] In addition to the non-consensual disclosure prohibition, the Privacy Act also compels federal agencies to retain only information that is relevant and necessary,[48] to provide individuals with a right of access to review and have their records corrected,[49] and to establish safeguards to ensure information security.[50]

The effectiveness of the Privacy Act and other more targeted privacy legislation is limited by the absence of a centralized enforcement mechanism to ensure agency compliance.[51] In the United States, a mixture of federal agencies supervise privacy issues, including the Federal Trade Commission, the Office of Consumer Affairs, the Internal Revenue Service, and the Federal Reserve Board.[52] Because sector-specific data protection provisions differ in their protection strength and enforcement mechanisms, there is no uniform approach certifying data security across industry lines.[53]

States have been active in passing industry-specific privacy legislation in a similar fashion as those at the federal level.[54] Excluding issue-specific federal legislation, there is little uniformity in state law, resulting in fifty different jurisdictions with distinct regimes.[55] The industry gaps that are subsequently left in the U.S. regulatory scheme encourage industries to self-regulate.[56] Private sector regulation generally relies on industry norms and individual company policies.[57] The use of markets as a regulator for data security is, again, indicative of U.S. preference for a laissez-faire government, as well as demonstrating the power of the corporation.[58] Thus, a wide range of actors—including federal and state legislatures, agencies, courts, industries and individual companies, and market forces—are in charge of executing data protection standards and enforcement.

---

47. A significant exception in the form of the "routine use exception," permits federal agencies to transfer information between themselves for what they justify as a "routine use." *Id.*

48. *Id.* at 761.

49. *Id.* at 760.

50. *Id.* at 761.

51. Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet the Standard?*, 21 FORDHAM INT'L L. J. 932, 977 (1998).

52. *Id.*

53. Yuen, *supra* note 9, at 54.

54. *See* Murray, *supra* note 51, at 979-980.

55. *Id.* at 980.

56. Yuen, *supra* note 9, at 54.

57. Shaffer, *supra* note 1, at 27.

58. *See id.*

III. TRANSNATIONAL CONTEXT: MANAGING THE DATA TRANSFER CONFLICT BETWEEN THE UNITED STATES AND THE EU

A. Impact of the EU Directive on Transnational Data Transfers

Due to the transnational application of the EU Data Directive, the divergent approaches of the United States and the EU became problematic as data was transferred between the two.[59] Under the "adequacy principle" contained in Articles 25 and 26 of the Directive, European data may only be transferred to non-EU countries (third countries) that provide an "adequate level of data protection."[60] The key point of this provision is to ensure that personal data lawfully processed in the EU remains subject to safeguards when transferred to third countries.[61] When assessing the adequate level of protection, the European Commission takes into account all of the circumstances surrounding a data transfer to a third country.[62] Particular consideration is given to:

> the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measure which are complied with in that country.[63]

However, several exceptions exist to the adequacy requirement where personal data may still be transferred to a third country, including both consent and controller-enforced safeguards, such as contractual clauses or binding corporate rules.[64]

The extraterritorial impact of Article 25 illustrates the EU's exercise of coercive market power. In an attempt to encourage others to align themselves closer with EU data protections, third countries are essentially forced to either adopt similar data protection provisions or negotiate bilateral agreements.[65] By using adequacy decisions as a

---

59. Cate, *supra* note 38, at 226.

60. Data Directive, *supra* note 10, arts. 25, 26.

61. EUROPEAN COMM'N, FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES 3, http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf (last visited Nov. 4, 2016).

62. Data Directive, *supra* note 10, art. 25(2).

63. *Id.*

64. Data Directive, *supra* note 10, art. 26; *see also Data Transfers Outside the EU*, EUROPEAN COMM'N , http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm (last visited Nov. 4, 2016).

65. Countries that have adopted the EU Directive as their own data regulation to ensure compliance include Switzerland, Malaysia, and Canada. Yuen, *supra* note 9, at 64.

barrier to entry to the EU market, the EU privacy regime has succeeded in ratcheting up privacy protections in other countries.[66]

Furthermore, Article 29 of the Data Directive establishes the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the Article 29 Working Party.[67] The Working Party is responsible for examining and reporting on the adequacy of third country (non-EU country) protections and is made up of a representative from each EU Member State's Data Protection Authority (DPA), the European Data Protection Supervisor, and the European Commission's Data Protection Officer.[68] The Directive charges the Working Party with giving the Commission expert opinions on the level of protection in Member States and in third countries.[69] While these opinions are not binding on the Commission's decisions, they are relied on extensively.[70]

B. Safe Harbor

When the EU Data Directive was implemented, it was clear the United States would not meet the adequate protection requirement, potentially resulting in considerable losses to both countries, considering the size of the EU and U.S. markets.[71] To prevent this potential loss of billions of dollars and a possible trade war, the U.S. Department of Commerce and the European Commission initiated talks in 1998 to ensure the continuation of business.[72] The Safe Harbor Privacy Principles (Safe Harbor), accepted in July 2000, sought to balance the EU's interest in the Privacy Directive protection requirement without requiring a wholesale change to the United States' self-regulated ad hoc approach.[73]

Safe Harbor instituted a system of self-regulation and self-certification, whereby companies wishing to transfer data between the United States and EU voluntarily submitted themselves to regulation under the Department of Commerce.[74] In order to satisfy the EU's standards, the Department of Commerce required companies to comply

66. Data Directive, *supra* note 10, art. 26(1).

67. *Id.* art. 29.

68. *Article 29 Working Party*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Nov. 4, 2016).

69. Data Directive, *supra* note 10, art. 29.

70. *Id.* art. 30.

71. Specifically, EU concerns centered on the U.S. diverse regulatory scheme, lack of centralized enforcement, and extensive national security exceptions. *See* Cate, *supra* note 38, at 226-27.

72. Shaffer, *supra* note 1, at 44-45.

73. *See Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/ (last visited Nov. 4, 2016).

74. *Id.*

with the seven principles of European data protection. The seven principles are: (1) individual notice that data collection is occurring and for how long the data will be used; (2) individuals must be provided a choice to opt out of collection of data; (3) companies may only transfer data to other companies that comply with these rules; (4) companies must provide reasonable protection of the data; (5) data must be relevant for the purposes of the collection and use; (6) data subject must be able to access the information and correct inaccurate data; and (7) there must be a means for enforcement of these rules.[75]

According to the principles set out in the Safe Harbor agreement, an organization had to inform individuals about the purposes for which it collected and used their personal information.[76] Under the agreement, the legal basis for collection and using personal information was consent by giving the consumer "notice" of personal data practices and by allowing the consumer a "choice" respecting disclosures to third parties and uses of personal data that are incompatible with the original purpose of data collection.[77] A company was mandated to provide individuals the opportunity to choose whether their information could be disclosed to a third party or used for a purpose incompatible with the reason for its original collection.[78]

Companies also had to ensure that there were adequate protections in place for individuals' personal information.[79] To appease the European Commission's apprehension of non-legislative means to protect data, the Department of Commerce agreed to monitor the incorporation of Safe Harbor principles in companies' privacy policies rather than allowing market self-regulation.[80] Finally, under Safe Harbor, EU national DPAs reserved the right to suspend data transfers to Safe Harbor certified companies in special cases when either the government body in the United States has determined a company was in violation of the agreement or there was a substantial likelihood of the principles being violated.[81]

---

75. *Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor. (last visited Nov. 4, 2016).

76. *Id.*

77. *Id.*

78. *Id.*

79. *Id.*

80. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspectives of EU Citizens and Companies Established in the EU, at 9, COM (2013) 847 final (Nov. 27, 2013).

81. *Id.* at 4.

C. Impact of the Snowden Revelations: Schrems Decision and the Invalidation of Safe Harbor

The 2013 revelations by Edward Snowden regarding the expansive data surveillance activities of the NSA raised serious questions on surveillance and personal data protection, both in the United States and abroad.[82] Following the Snowden revelations, the EU Commission decided to review Safe Harbor and identified a number of shortcomings.[83] The Commission issued thirteen recommendations for the United States to follow in order to restore EU trust, focusing on transparency, redress, enforcement, and access to European data by U.S. authorities.[84] The Commission's report explicitly stated the need to address the "deep concerns about revelations of large-scale U.S. intelligence collection" and included a recommendation that the national security exception, which had been heavily exploited by the NSA, only be used to the extent that is strictly necessary or proportionate.[85]

On June 25, 2013, Max Schrems initiated a complaint with the Irish Data Protection Commissioner (Ireland's DPA), alleging that transfer of EU personal data to the United States was incompatible with EU law.[86] Specifically, Schrems alleged Facebook Ireland had mishandled his data even though it was self-certified under Safe Harbor.[87] Basing his complaint on the Edward Snowden revelations, Schrems argued that there was "no meaningful protection in U.S. law or practice" in this transnational transfer of data.[88] However, the Irish DPC found that, because the transfers were made under the European Commission approved Safe Harbor, the Irish Commissioner did not have authority to overrule.[89] Schrems appealed the DPA decision and initiated judicial review proceedings with the Irish High Court.[90]

A year after the initial complaint, the Irish High Court departed sharply from the Irish DPA, holding that Schrems did have legal standing

---

82. European Commission Press Release MEMO/15/6014, Q&A: Guidance on Transatlantic Data Transfers Following the Schrems Ruling 1 (Nov. 6, 2015), http://europa.eu/rapid/press-release_MEMO-15-6014_en.htm [hereinafter MEMO/15/6014].

83. *Id.*

84. *Id.*

85. European Commission Press Release IP/13/1166, European Commission Calls on the U.S. To Restore Trust in EU-U.S. Data Flows 1 (Nov. 27, 2013), http://europa.eu/rapid/press-release_IP-13-1166_en.htm [hereinafter IP/13/1166].

86. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-19.

87. *Id.*

88. *Id.* ¶ 29.

89. *Id.*

90. *Id.* ¶ 30.

under both domestic and EU law.[91] The court went further and stated that there was much to be said for the Snowden revelations, which demonstrated "significant over-reach" on the part of the NSA and other agencies, highlighting the need for an updated U.S.-EU data protection regime.[92] Following its decision, the Irish High Court referred the case to the Court of Justice of the European Union (CJEU)[93] to adjudicate whether Facebook's actions—in particular, its participation in the NSA's surveillance programs—were compatible with the Safe Harbor framework and whether Safe Harbor was functioning as intended.[94]

In its decision on October 6, 2015, the CJEU determined that the European Commission surpassed its authority in issuing the Safe Harbor adequacy decision in two ways.[95] First, highlighting the lack of safeguards attached to the national security exception, the Court found the Commission had failed to ensure an adequate level of safety for European data transfers to the United States.[96] The Court determined U.S. data protection law was inadequate under the Charter of Fundamental Human Rights of the EU due to both the indiscriminate bulk collection of Europeans' data by the NSA and the lack of judicial redress available for Europeans.[97] As it stood, Europeans did not possess the right to sue in U.S. court if their data was mishandled by U.S. federal agencies.[98] Second, the Commission overstepped its bounds in denying DPC's complete independence by enforcing the data protection regime following a claim by an individual.[99] Because these two issues could not be separated from the other provisions in the agreement, the CJEU ruled that there was no EU authorization for Safe Harbor and invalidated the entire agreement, effective immediately.[100]

---

91. *Id.* ¶ 34; *see* Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, 2014 E.C.R. 15 (determining that it is irrelevant whether a complainant was actually inconvenienced in order to establish an infringement of respect to private life).

92. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-19 ¶ 30.

93. Following a procedure where a court of an EU Member State (in this case, Ireland) may request from the CJEU a "preliminary ruling" on issues of EU law. Case 314/85, Foto-Frost v. Hauptzollamt Lübeck-Ost, 1987 E.C.R. ¶¶ 1, 16.

94. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-19 ¶ 36.

95. *Id.* ¶ 84-90.

96. *Id.* ¶ 90-91.

97. *Id.* ¶ 93-94.

98. *Id.* ¶ 95.

99. *Id.* ¶ 102-103.

100. *Id.* ¶ 105-106.

IV. LOOKING FORWARD: THE EU GENERAL DATA PROTECTION REGULATION AND THE EU-U.S. PRIVACY SHIELD AGREEMENT

A. EU General Data Protection Regulation

In 2012, the European Commission initiated discussions to reform the current EU Data Protective Directive in light of the technological advances that had taken place since its approval in 1995.[101] The Commission identified two key goals in developing a new data protection standard: strengthening user control over personal data and facilitating business.[102] Thus, the new General Data Protection Regulation (GDPR) aims to give data subjections broad rights of access and control over their own data that is collected, as well as to help businesses by creating a more unified data standard across the EU.[103] The EU Parliament approved GDPR on April 14, 2016, and it will enter into force in 2017.[104]

In an effort to increase user control of personal data, the GDPR extends the coverage of sensitive information provided for in the Directive to new categories of personal information, including genetic data, and allows individuals easier access to their personal data.[105] Additionally, unlike the Directive, to meet the consent category under the GDPR, the data controller must obtain written, explicit consent for the specified purpose; thus, implied consent is no longer recognized.[106] The GDPR also grants substantive rights to data subjects by establishing the "right to be forgotten" through the implementation of stronger rights to erase.[107]

The GDPR may cause conflict with data protection regimes in third countries due to new obligations for transnational transfer of European data and the extension of its territorial scope.[108] The GDPR adopts the Directive's "adequacy principle" prohibiting the transfer of data to third

---

101. European Commission Press Release IP/15/6321, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market 1 (Dec. 15, 2015), http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

102. *Id.* at 1-2.

103. A regulation has a general application and is binding in its entirety; while a directive gives Member States more opportunity to adopt their own specific rules in certain areas. By direct application in all Member States, a regulation provides a more overarching standard. *Id.* at 2.

104. 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/EEC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

105. *Id.* art. 9.

106. *Id.* art. 4(11); *contra* Data Directive, *supra* note 10, art. 2(h).

107. GDPR, *supra* note 104, art. 17.

108. *Id.* art. 3.

countries that do not have a sufficient level of data protection by European standards.[109] However, the GDPR goes further, clarifying the conditions under which data may be transferred.[110] First, transfers are permitted when the Commission certifies that a third country ensures an adequate level of protection.[111] Second, a controller or processor may transfer data if a legally binding and enforceable instrument establishes appropriate legal safeguards.[112] Finally, data may be transferred under certain specified conditions, such as where there is consent or public interest reasons.[113]

Unlike the current Directive, the new data regulation extends to all controllers processing EU personal data; it is irrelevant whether the processing of personal data takes place within the EU.[114] By widening the territorial scope of the application of the GDPR, the regulation could be taken to apply extraterritorially. An extraterritorial application would have a significant impact on transnational data flow across the globe. The GDPR could be considered a step towards an international standard due to the market power of the EU.

B. The EU-U.S. Privacy Shield

Following the CJEU's invalidation of Safe Harbor, companies were left scrambling to develop a new framework for transferring European data to the United States without violating EU laws.[115] The Article 29 Working Party gave EU and U.S. negotiators a three-month window to address their concerns and negotiate an updated agreement.[116] In the interim, the European Commission issued guidance on transatlantic data transfers, setting out alternative mechanisms for the transfer of European data to the United States.[117] The Working Party highlighted the CJEU's criticism of the lack of judicial redress for EU citizens, as well as for the U.S. mass surveillance programs, that together created "serious

---

109. *Id.* art. 45; *see also* Data Directive, *supra* note 10, art. 25.

110. GDPR, *supra* note 104, art. 45.

111. *Id.*

112. *Id.* art. 47.

113. *Id.* art. 46.

114. Under the Directive, controllers are only subject to regulation if they use equipment in the EU to process European data. *Id.* art. 44; *contra* Data Directive, *supra* note 10, art. 4.

115. *See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the United States of America Under Directive 95/46/EC Following the Judgment by the Court of Justice in Case C-362/14* (Schrems), at 2, COM (2015) 566 final (Nov. 6, 2015).

116. *Id.* at 4.

117. The Commission primarily relied on alternative mechanisms set forth in Article 26 of the Data Directive such as standard contractual clauses or binding corporate rules. *Id.*

questions . . . regarding the continuity of the level of data protection when data [is] transferred to the United States."[118]

On February 2, 2016, the European Commission and the United States announced their agreement for a new framework for transatlantic data flows: the EU-U.S. Privacy Shield.[119] Reflecting the requirements set forth in *Schrems*, EU-U.S. Privacy Shield "provide[s] stronger obligations on companies in the U.S. to protect the personal data of Europeans" and increases monitoring and enforcement.[120] Privacy Shield attempts to rectify Safe Harbors' shortcomings by placing safeguards on how U.S. authorities can access Europeans' data and creating a framework for resolving cases when Europeans challenge the use of their data as improper.[121]

Privacy Shield attempts to rectify one of Safe Harbor's main shortcomings in the protection of European data by limiting access for national security purposes.[122] At the European Commission's insistence, the United States, "[f]or the first time . . . has given the EU written assurance that law enforcement and national security data collection will be subject to clear limitations, safeguards, and oversight mechanisms."[123] Key limitations on intelligence operations specify that data collection be targeted, and also restricts the use of bulk data collection to six national security purposes: to detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to armed forces, or transnational criminal threats.[124] An annual joint review will regularly monitor the functioning of the agreement, including the issue of national security access.[125]

Privacy Shield also addresses the CJEU's concern over the lack of judicial redress available to Europeans whose data may be misused in the United States. The new agreement allows several redress possibilities for EU citizens.[126] Alternative dispute resolution is provided free of charge

---

118. Press Release, Article 29 Data Protection Working Party, The Court of Justice of the European Union Invalidates the EU Commission Safe Harbor Decision (Oct. 6, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf.

119. European Commission Press Release IP/16/216, EU Commission and United States Agree on a New Framework for Transatlantic Data Flows: EU-US Privacy Shield 1 (Feb. 2, 2016) [hereinafter IP/16/216].

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. DEPT. HOMELAND SEC., IA-1002, SAFEGUARDING PERSONAL INFORMATION COLLECTED FROM SIGNALS INTELLIGENCE ACTIVITIES 3 (2014).

125. IP/16/216, *supra* note 119, at 1.

126. *Id.* at 2.

and European DPAs can refer their citizens' complaints to the Department of Commerce and the Federal Trade Commission (FTC).[127] Disputes concerning national security will be handled by an ombudsperson in the United States, who will be independent of federal security agencies.[128]

Under Privacy Shield, U.S. companies that intend to transfer European data need to commit to strong obligations regarding their data processing and their guarantees of individual rights.[129] Monitored by the Department of Commerce, companies must publish their commitments, making them enforceable under the FTC.[130] Companies are also compliant with European DPA decisions.[131]

On April 13, 2016, the Working Party published an Opinion setting out their detailed analysis of the Privacy Shield's framework.[132] In this Opinion, the Working Party expressed concerns over both the commercial aspects of Privacy Shield, as well as the ability of U.S. authorities to access transferred data.[133] In particular, the Working Party pointed out the lack of certain key data protection principles in EU law, such as clear instructions that Privacy Shield principles apply from the moment the transfer takes place, not only from the time when it is considered "processed" by U.S. standards.[134] Additionally, Privacy Shield does not exclude massive and indiscriminate collection of European personal data by U.S. intelligence agencies.[135] The Working Party concluded the Opinion by urging the European Commission to resolve their concerns and strengthen data protections for Europeans in the Privacy Shield.[136] Despite the fairly critical Working Party Opinion, the European Commission formally approved Privacy Shield on July 12,

---

127. *Id.*
128. *Id.*
129. *Id.* at 1.
130. *Id.*
131. *Id.*
132. Article 29 Data Protection Working Party, WP238, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (April 13, 2016) [hereinafter Working Party Decision].
133. *Id.* at 12.
134. The U.S. interpretation on acquisition of data is that "processing" occurs when data is analyzed by a human being. Meanwhile, the EU position is that data is considered "processed" from the moment of collection. Thus, the differences regarding when privacy concerns arise and protections must be afforded may affect the CJEU's determination of the adequacy level of U.S. protections. Data Directive, *supra* note 10, art. 2(b); *see also*, Working Party Decision, *supra* note 132, at 12.
135. Working Party Decision, *supra* note 132, at 37-39.
136. *Id.* at 57.

2016, and it went into force immediately, with companies able to certify as of August 1, 2016.[137]

C. The Judicial Redress Act

European access to judicial redress became a key requirement of Privacy Shield after it was named as a principle reason for the invalidation of Safe Harbor.[138] European negotiators conditioned their Privacy Shield approval on the United States' adoption of the Judicial Redress Act, extending the U.S. Privacy Act of 1974 to European citizens.[139] For years, European privacy advocates complained that there was a lack of judicial redressability available to European citizens if their data was collected and misused by the U.S. government.[140] U.S. government agencies regularly use warrants to compel U.S. tech companies to turn over user data, including that of foreigners, but prior to the Judicial Redress Act only U.S. citizens relying on the Privacy Act could challenge those procedures.[141] The European Commission's negotiators demanded that the 1974 Privacy Act extend to European citizens, refusing to sign Privacy Shield until the necessary change was made.[142]

President Obama signed the Judicial Redress Act into law on February 24, 2016, and extended the Privacy Act to EU citizens.[143] The Judicial Redress Act gives EU citizens (and citizens of other countries or organizations designated in the future by the Department of Justice) the ability to seek remedies under the Privacy Act for the mishandling of personal information in criminal or terror investigations.[144] However, in response to Senate Republican concerns that the United States was giving up too much to EU counterparts, an amendment was incorporated,

---

137. European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016) http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

138. Mark MacCarthy, *Senate Should Pass the Judicial Redress Act Now*, HILL (Nov. 3, 2015, 11:00 AM), http://thehill.com/blogs/congress-blog/foreign-policy/258852-senate-should-pass-the-judicial-redress-act-now.

139. *Id.*

140. European Commission Memorandum MEMO/13/1059, Restoring Trust in EU-US Data Flows-Frequently Asked Questions 9 (Nov. 27, 2013).

141. As a contrast, American citizens retain the right to sue if their data is misused under EU law. IP/16/216, *supra* note 119.

142. MacCarthy, *supra* note 138.

143. *Remarks by the President at the Signing of the Judicial Redress Act Bill*, WHITE HOUSE (Feb. 24, 2016, 4:39 PM), https://www.whitehouse.gov/the-press-office/2016/02/24/remarks-president-signing-judicial-redress-act-bill.

144. Judicial Redress Act of 2015 § 2, 5 U.S.C. § 552a note (2016).

centering on commercial data and national security interests.[145] With the inclusion of the amendment, Privacy Act benefits are only extended to countries when the Attorney General determines those countries permit commercial data transfers with the United States and do not materially impede national security interests.[146]

V. CONCLUSION

Despite the passage of the Judicial Redress Act, the Privacy Shield may still fail to meet the CJEU's demands under *Schrems*. While invalidating Safe Harbor, the CJEU raised serious concerns over the current U.S. ad hoc regulatory scheme and the EU preference for all-encompassing protections.[147] There is also a lower threshold for the collection of foreigners' data within the United States.[148] The 1974 Privacy Act is generally less protective than European legislation is on the same issues, and it contains many exceptions, particularly for law enforcement agencies and the CIA.[149]

Because the rights of U.S. citizens under the Privacy Act are minimal in comparison to those of Europeans, the substantive rights required by *Schrems* may be too lofty for the Privacy Act to meet. Max Schrems, whose actions led to the invalidation of Safe Harbor, has criticized Privacy Shield as an attempt to "put a lot of lipstick on the same old data-suckling pig."[150] Because the agreement does not address the "core concerns and fundamental flaws of U.S. surveillance law and the lack of privacy protections under U.S. law," the CJEU could potentially end up striking down the Privacy Shield agreement for the

---

145. Katie Bo Williams, *Last-Minute Change to Privacy Bill Adds Tension to US-EU Talks*, HILL (Jan. 28, 2016, 4:35 PM), http://thehill.com/policy/cybersecurity/267401-last-minute-change-to-privacy-bill-adds-tension-to-us-eu-negotiations; *see also* Lisa Brownlee, *Judicial Redress Act 'National Security Interests' Amendment Could Affect US-EU Negotiations*, FORBES (Jan. 28, 2016, 4:55 AM), http://www.forbes.com/sites/lisabrownlee/2016/01/28/posted-judicial-redress-act-national-security-interests-amendment/#30e85c82155d.

146. Judicial Redress Act § 2(d)(1).

147. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-30-32 ¶¶ 84-91.

148. Procedures targeting and minimizing data collection apply only to U.S. citizens and the First and Fourth Amendment protections don't apply to nonresidents outside the country. *Report on the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection* 17 (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

149. Privacy Act of 1974, Pub. L. No. 93-579, § 2(b)(6), 88 Stat. 1896, 1896 (1974), reprinted in 5 U.S.C. § 552a note at 763 (1982).

150. Natasha Lomas, *Draft Text of EU-US Privacy Shield Deal Fails To Impress the Man Who Slayed Safe Harbor*, TECH CRUNCH (Feb. 29, 2016), http://techcrunch.com/2016/02/29/lipstick-on-a-pig/.

same reasons it struck down Safe Harbor: a lack of adequate protection of European data.[151]

However, recent global terrorism events may influence the CJEU's eventual ruling on the Privacy Shield adequacy decision. Although, generally, Europeans have not given national security exceptions favorable interpretations in the past. During Safe Harbor negotiations, the European Commission tried to limit the scope of the national security exception in the transatlantic flow of data, pointing out that the exception must be narrowly tailored, as well as necessary and proportionate.[152] However, even with the Commission's influence, Safe Harbor was still invalidated by the CJEU, in large part, because of concerns centering on the United States' extensive reliance on national security exemptions.[153] A more recent example is EU concern about the inclusion of the national security amendment in the Judicial Redress Act.[154] By only extending judicial redress to nations that do not impede U.S. national security interests, the CJEU could consider the exception too expansive to satisfy *Schrems*.

However, while the EU has been notoriously protective of individual privacy, with recent terrorist attacks throughout Europe, we may start to see a loosening of their strict privacy regulations in the name of national security. In response to a string of attacks originating at the Charlie Hedbo offices in 2015, France's Constitutional Council approved a sweeping surveillance law later that year.[155] The bill allows the government to monitor phone calls and emails of suspected terrorists without prior authorization from a judge.[156] It also calls for Internet service providers to install so-called "black boxes" that sweep up and analyze metadata, and forces providers to make the data available to intelligence organizations.[157]

More recently, the string of terrorist attacks across Germany in the summer of 2016 has rekindled concerns about Germany's and the EU's

---

151. *Id.*

152. *See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 16, COM (2013) 847 final (Nov. 27 2013).

153. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-30-32 ¶¶ 84-91.

154. Williams, *supra* note 145.

155. Alyssa J. Rubin, *Lawmakers in France Move To Vastly Expand Surveillance*, N.Y. TIMES (May 5, 2015), http://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html?_r=0.

156. Conseil constitutionnel [CC] (Constitutional Court) decision No. 2016-536QPC, Feb. 19, 2016 (Fr.).

157. Rubin, *supra* note 155.

ability to cope with the growing migrant problems, prompting a serious conversation on possible changes to both German and EU privacy law.[158] Based on national security concerns, German officials have called for relaxing privacy laws to make it easier for authorities to observe online data like email, WhatsApp, and Skype messages.[159] Historically, France and Germany have been more protective of individual privacy rights than other EU Member States. This relaxing of domestic privacy rights in the name of national security may be indicative of a larger trend occurring. Ultimately, the CJEU has the final say and, when the Court reviews the Privacy Shield adequacy decision, it is possible that these developments could cause the court to be more forgiving of national security exceptions than it has been in the past.

158. *German Officials Vow Tighter Security, Migrant Controls After Recent Attacks*, CHI. TRIB. (July 26, 2016, 10:20 AM), http://www.chicagotribune.com/news/nationworld/ct-germany-attacks-20160726-story.html.

159. *Id.*