NAVIGATING THE ATLANTIC: UNDERSTANDING EU DATA PRIVACY COMPLIANCE AMIDST A SEA OF UNCERTAINTY

GRIFFIN DRAKE*

TABLE OF CONTENTS

*. J.D. candidate, University of Southern California Gould School of Law, 2018. I am forever grateful to my best friend and fiancée, Venessa Simpson, for the endless love and support she has provided me throughout college and law school, and to my mom and dad, the most loving, caring, and supportive parents there are; you three are my inspiration and make me want me to be a better person each and every day. Many thanks also to Professor Valerie Barreiro for your guidance and feedback during the note-writing process and to Jonathan Frimpong, Emily Arndt, and James Salzmann for your invaluable and much-needed feedback and editing expertise.

INTRODUCTION

United States government surveillance has reached a point where the government "c[an] construct a complete electronic narrative of an individual's life: their friends, lovers, joys, sorrows."[1] In June 2013, Edward Snowden released thousands of confidential documents from the National Security Agency ("NSA") regarding classified government surveillance programs.[2] The documents brought to light the fact that that the NSA was spying on individuals, including foreign citizens, and deliberately misleading Congress about these activities.[3] According to Snowden, the spying was so extensive that the spying measures, including a program known as "PRISM," involved the improper mass collection of data from citizens worldwide through NSA interactions with telecom giants like Google, Microsoft, and Facebook, and by tapping into global fiber optic cables.[4]

These revelations sent shockwaves around the globe, and the backlash was swift and unforgiving. One thing became clear to Americans and the rest of the world: the NSA and the U.S. government had prioritized the massive collection of private information over and above the personal privacy rights of the global population.[5] The concept of throwing civil liberties to the wayside through grossly intrusive surveillance pushed Snowden to step forward and reveal what he had seen all too closely.[6] He no longer wanted to "live in a world 'where everything that I say, everything that I do,

1. Luke Harding, *How Edward Snowden Went from Loyal NSA Contractor to Whistleblower*, GUARDIAN (Feb. 1, 2014, 6:00 A.M.), https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

2. *Id*.

3. *Id.*

4. *Id*.

5. *See* Schrems v. Data Protection Commissioner, ELECTRONIC PRIVACY INFO. CTR. [hereinafter Schrems], https://epic.org/privacy/intl/schrems (last visited Nov. 15, 2017).

6. *See* Harding, *supra* note 1.

everyone I talk to, every expression of love or friendship is recorded.'"[7]

Across the Atlantic, the priorities of European Union member nations stand in stark contrast to those of the United States. The EU takes a much stronger stance on privacy and data protection and restricts how companies transfer data to non-EU nations. In the EU's Data Protection Directive (the "Directive"), the right to privacy is described as a "fundamental right[] and freedom[]."[8] This sentiment is echoed in other landmark EU documents such as the Convention for the Protection of Human Rights and Fundamental Freedoms.[9]

Despite the very different treatment of the right to privacy in the U.S. and EU, we live in an era of lightning-quick information transfers and an interconnected global economy in which the sharing of private data (including names, IP addresses, health care information, and so forth) across borders is essential to companies conducting business worldwide.[10] The current state of the world necessitates that data flow seamlessly from country to country.[11] This reality led to the EU's Safe Harbor Decision ("Safe Harbor"), allowing American companies to self-certify their compliance with certain heightened privacy restrictions when handling the private information of EU citizens and thus facilitating the transfer of information from the EU to the U.S.[12] However, the Safe Harbor was invalidated in *Schrems v. Data Protection Commissioner* ("*Schrems I*").[13] This left American companies to rely on other EU-approved data transfer mechanisms—namely, Model Clauses,[14] Binding Corporate Rules ("BCRs"), or specific statutory derogations. In need of a replacement for the

7. *Id*.

8. Directive 95/46, 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, art. 1, 1995 O.J. (L 281) 31, 38 (EC) [hereinafter Directive 95/46/EC]. The Directive has since been replaced by the General Data Protection Regulation ("GDPR"). *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation]. The GDPR will be addressed in depth in Part III of this Note.

9. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, 230.

10. *See* McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 422 (2016).

11. *See id*.

12. *See* Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, art. 1, 2000 O.J. (L 215) 7, 8 [hereinafter Safe Harbor].

13. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.

14. The EU Model Clauses are also referred to as Standard Contractual Clauses. For convenience, the term "Model Clauses" will be used throughout this Note.

Safe Harbor, the EU and the United States agreed on a new deal known as the "Privacy Shield," despite heavy criticism.[15] An additional layer of complexity exists due to the fact that the Directive, which long governed the handling of private information in the EU, is now being replaced with the significantly stronger General Data Protection Regulation ("GDPR").

This Note will argue that in light of the pending commencement of the GDPR, American companies relying on the Privacy Shield are exposed to potential risk, as it fails to satisfy the "essentially equivalent protection" standard set forth in *Schrems I,* and that alternative data protection mechanisms, such as Model Clauses or BCRs, have serious drawbacks and face similar questions regarding their validity.[16] Subsequently, I will discuss some of the potential alternative mechanisms that companies can use to best mitigate exposure to the risks inherent in transatlantic data transfers.

Part I of this Note will describe the background that has led to the current uncertainty in the validity of the various data protection mechanisms. This Part will discuss the key principles behind data privacy protections, the *Schrems I* case and the subsequent invalidation of the Safe Harbor, the buildup to the Privacy Shield, and the other possible transfer mechanisms. Part II will discuss the fundamental differences between the United States' and the European Union's approaches to protecting individuals' private information. This section will highlight the irreconcilable differences between U.S. surveillance policies and the EU's view of the fundamental right to privacy. Part III will discuss the pending implementation of the GDPR and the relevant changes this directive will have to the current transatlantic data transfer legal regime. Part IV will outline the shortcomings inherent in the Privacy Shield, Model Clauses, and BCRs individually. Part V will conclude this Note by briefly discussing potential alternatives that companies can use to attempt to weather the shaky data privacy landscape that exists today. The proposed alternatives include obtaining consent, using codes of conduct and certification, and layering transfer mechanisms.

I. BACKGROUND

A. KEY PRINCIPLES OF PRIVACY REGULATIONS

With the ability of companies to transfer swaths of consumers' personal data globally at the click of a button, the United States and the European

15. *See* Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision (2016) [hereinafter Opinion 01/2016], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

16. *Schrems*, ECLI:EU:C:2015:650, ¶¶ 73–74, 96.

Union have been forced to adapt privacy regulations to meet this rapidly changing reality. In doing so, certain fundamental principles have arisen and been used to shape modern data privacy laws. In 1973, the U.S. Department of Health, Education, and Welfare developed a committee to review the use of automated data systems that maintained personal information.[17] This committee laid out five principles for data protection, known as the "Fair Information Practices" ("FIPs").[18] These principles were incorporated, though not by name, in the Privacy Act of 1974.[19] The Privacy Act of 1974 also established the Privacy Protection Study Commission, which in 1977 refined the FIPs into eight clear principles.[20] The principles are: Openness, Individual Access, Individual Participation, Collection Limitation, Use Limitation, Disclosure Limitation, Information Management, and Accountability.[21] These principles, however, apply only to the *public* sector and were not formally referenced by Congress until 2002.[22]

In the EU in the 1970s, many laws were already consistent with the principles described in the FIPs.[23] In 1980, the Organization for Economic Co-operation and Development ("OECD") developed a set of privacy guidelines with its own eight principles for data protection.[24] These principles include: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.[25] These principles clearly bear a strong resemblance to the FIPs with one major difference—they are broadly intended to apply across both the public *and* private sectors. In 1995, the EU took the principles a step further and adopted the Directive to protect

17. U.S. DEP'T. OF HEALTH, EDUC., & WELFARE, NO. (OS) 73–94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41 (1973).

18. *See id*.

19. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)).

20. Robert Gellman, Fair Information Practices: A Basic History 5 (Apr. 10, 2017) (unpublished manuscript) (https://bobgellman.com/rg-docs/rg-FIPshistory.pdf).

21. Gellman, *supra* note 20, at 5.

22. *Id*. at 10. *See also* 6 U.S.C. § 142. For further discussion, see *infra* Part II.

23. Gellman, *supra* note 20, at 6.

24. ORG. FOR ECON. CO-OPERATION & DEV., *Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980), *reprinted in* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 11 (2002).

25. *Id.* at 14–16. As further proof of the enduring nature of these principles, the OECD reviewed the principles in 2013 in light of the changes over the past thirty years, choosing to maintain the eight principles in their original form. ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 14–15 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

individuals and their private data.[26] These principles were also included in the GDPR, along with a few additional principles.[27] All in all, the principles created in 1973 and revised over time often serve as the foundation for data privacy regulations today.

B. *SCHREMS I* AND THE INVALIDATION OF THE SAFE HARBOR

While transferring data around the world is a practical necessity for large companies, governments in the EU and the United States recognize that due to how quickly and easily personal data is being transferred, this data must be protected. Acknowledging these two conflicting important interests, the EU and the United States struck a deal. In 2000, the European Commission passed a decision known as the Safe Harbor, determining that the United States, in conjunction with the terms of the agreement, provided adequate privacy protection.[28] The Safe Harbor decision allowed U.S. companies to self-certify that they will abide by EU data protection standards when transferring data across the Atlantic.[29] This option was attractive to companies because it was relatively easy to institute and it efficiently lowered transaction costs compared to Model Clauses or BCRs—so much so that over five thousand companies chose to self-certify.[30] Self-certification involved companies (1) outlining specific information about the company and the company's use of personal data obtained from EU citizens on an online form and (2) paying a processing fee of $200.[31] This option was considered to fall into the category of an "adequacy decision" by the Commission in accordance with Article 25 of the Directive.[32] It is important to note, though, that this decision did not allow free rein for all U.S. companies to freely exchange information across the Atlantic. Instead, this

26. *See* Directive 95/46/EC, *supra* note 8, art. 1, at 38 ("In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.").

27. *See* General Data Protection Regulation, *supra* note 8, art. 5, at 35–36.

28. *See* Safe Harbor, *supra* note 12, art. 1, at 8 (describing how companies that self-certify can comply with the Safe Harbor requirements).

29. *See* Kelli Clark, *The EU Safe Harbor Agreement Is Dead, Here's What to Do About It*, FORBES (Oct. 27, 2015, 3:30 P.M.), http://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/#29a319fc7171.

30. *See id*.

31. *See* U.S. DEP'T OF COMMERCE, U.S.-EU SAFE HARBOR FRAMEWORK: GUIDE TO SELF-CERTIFICATION 4–10 (2013), https://build.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf. *See also Safe Harbor Fees*, EXPORT.GOV, https://2016.export.gov/safeharbor/eg_main_020436.asp (last visited Oct. 15, 2017) ("An organization that is self-certifying its compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework for the first time on or after March 1, 2009 must remit a one-time processing fee of $200.00.")

32. *See* Directive 95/46/EC, *supra* note 8, art. 25, at 45–46.

method of achieving adequate protections only applied to the companies that self-certified and complied with the requisite standards.

While this solution worked for over a decade, the revelations published by Edward Snowden served as evidence that the Safe Harbor was built on false assurances. The Safe Harbor met its ultimate demise in *Schrems I*, in which Maximillian Schrems, an Austrian privacy activist, complained to the Data Protection Commissioner that Facebook, a Safe Harbor-certified company incorporated in Ireland, was transferring personal data into the United States where "the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities."[33] In his original case, Schrems cited Facebook's voluntary participation in the aforementioned NSA PRISM program, which gave the U.S. government access to substantial amounts of private personal information.[34] The claim was that "there was 'no meaningful protection in US law or practice' regarding data transferred that was subject to US state surveillance."[35]

The Irish High Court agreed with Schrems, stating that "[t]here is, perhaps, much to be said" for the Snowden revelations exposing "gaping holes in contemporary US data protection."[36] Accordingly, the Irish High Court, in line with EU law, referred the matter to the Court of Justice of the European Union ("CJEU") to adjudicate the validity of the adequacy decision regarding the United States.[37]

The CJEU agreed with the Irish High Court and took a large step by fully invalidating the Safe Harbor.[38] The standard as stated by the court vastly elevated the requirements for all future transfer mechanisms by stating that privacy protection measures in non-EU member nations need to be "essentially equivalent to that guaranteed in the EU legal order."[39] Thus, the CJEU found that U.S. privacy law was incompatible with the EU charter.[40]

33. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 28, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN. *See also* Schrems, *supra* note 5.

34. *See* Schrems v. Data Protection Comm'n [2014] IR 75, ¶ 29 (H. Ct.) (Ir.).

35. Nora Ni Loidean, *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, 19 No. 8 J. INTERNET L. 1, 1, 9 (2016) (quoting *Schrems*, IR 75, ¶ 29).

36. *Schrems*, IR 75, ¶ 69.

37. *See id.* ¶ 71.

38. *See* Case C-362/14, *Schrems*, ¶ 107.

39. *Id.* ¶ 96.

40. *Id.* ¶ 86.

C. THE ROAD TO THE PRIVACY SHIELD

With roughly five thousand companies relying on an invalidated measure, uncertainty as to what steps to take was apparent and widespread. But just as economic necessity drove the United States and the EU into the eventually invalidated Safe Harbor, it likewise drove them to craft a new, seemingly more robust agreement.[41] In coming to this agreement, the two parties faced incredible time constraints and deadlines from the Article 29 Working Party, the group designated to represent the EU member nations' data protection authorities. The agreement that was developed, known as the Privacy Shield, was fully approved and placed into effect in July 2016, despite facing some bumps in the road,[42] and was intended to guarantee that the United States will provide the necessary "essentially equivalent" protections to individuals as those individuals would receive under the Directive.[43] The goal was that the Privacy Shield would fix the weaknesses inherent in the Safe Harbor as identified by the CJEU while providing a useful means to maintain the free flow of information.[44]

The dilemma faced by both the EU and the United States was that data necessarily needs to flow between them to maintain everyday business functions, while at the same time there must be protections in place to ensure the proper handling of the data being transferred.[45] The Privacy Shield was agreed upon because of this dilemma, and it has been described by some as a much stronger version of the invalidated Safe Harbor.[46] The Privacy Shield now includes stronger obligations regarding how companies handle data, increases transparency regarding how data is used, safeguards against U.S. government access, and provides new protections and remedies for individuals and a joint review mechanism.[47]

The agreement, though, was created in line with the Directive (and the *Schrems I* decision, which was made based on the Directive). Come 2018, the Directive will be replaced by the GDPR.[48] The GDPR was developed to

41. *See* Clark, *supra* note 29.

42. *See* Opinion 01/2016, *supra* note 15.

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

44. *Id*.

45. Loidean, *supra* note 35, at 7–12.

46. *See* European Commission Press Release IP/16/2461, *supra* note 43.

47. *Id*.

48. European Commission Statement 16/1403, Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection (Apr. 14, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm.

modernize the protections given by the EU to individuals while greatly strengthening individual's rights.[49] The GDPR is intended to protect personal data in a manner significantly stronger than under the Directive.[50] Further, the new, stronger protections of the GDPR may lead to the invalidation or revision of the Privacy Shield, which was hurriedly designed to comply with the CJEU court decision and the Directive. Even today, there are already complaints about the adequacy of the Privacy Shield's ability to adequately protect EU citizens' data, similar to those raised against the Safe Harbor.[51] These complaints have been exacerbated by an executive order issued by President Trump, excluding non-U.S. citizens from the protections of the Privacy Act of 1974.[52]

D. OTHER AVAILABLE TRANSFER MECHANISMS

So, what options does a U.S. company have for transferring personal data? The Directive outlines acceptable methods for such transfers, including an adequacy decision by the Commission, a Commission-approved transfer mechanism, or a statutory derogation.[53] A brief overview of these transfer mechanisms follows here, but they are discussed in more depth in Parts II, III, and IV.

An "adequacy decision" is a determination by the Commission that a non-EU member country "ensures an adequate level of protection."[54] The Safe Harbor and the Privacy Shield were considered adequacy decisions in the sense that they developed certain rules and regulations that would strengthen the United States' privacy protections to an "adequate" level. The Privacy Shield remains approved, meaning that a company can legally rely on it to transfer data. However, this mechanism could place a company in a position where if the Privacy Shield is invalidated or undergoes substantial revision, the company will need to undertake costly measures to ensure that its data transfers comply with the applicable laws and regulations in order to avoid hefty fines for non-compliance.[55]

49. European Commission Memorandum 15/6385, Questions and Answers—Data Protection Reform (Dec. 21, 2015), http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.

50. European Commission Press Release IP/16/2461, *supra* note 43.

51. *See* Schrems, *supra* note 5; Tomaso Falchetta, *New 'Shield', Old Problems*, PRIVACY INT'L (July 7, 2016), https://www.privacyinternational.org/node/889.

52. *See* Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017). *See also infra* Part IV.A.

53. Schrems, *supra* note 5.

54. *Id*.

55. *See* General Data Protection Regulation, *supra* note 8, art. 83, at 82–83. Fines can total up to €20,000,000 or up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. *Id.* at 83.

A second option is either of the two European Commission-approved transfer mechanisms: Model Clauses or BCRs.[56] BCRs are company-developed rules governing the protection of private data that must undergo a rigorous, multi-step approval process by EU data authorities; they may be used to ensure that all transfers within a single group or company provide adequate protection as described in Article 26(2) of the Directive.[57] It is worth noting, though, that BCRs only legitimize data transfers made within a single overarching group.[58] A major benefit of BCRs is that unlike Model Clauses, there is no need to sign new contracts with each transaction.[59] This allows a company to have a clear internal procedure for handling private data and can lead to particular efficiencies.[60] Any company that is sharing or transferring data outside of its broader corporate entity structure, however, will still need to use a different method to validate those transfers, making this option less attractive to companies that exchange information externally.

This leads some companies to turn to Model Clauses, sets of contract clauses that, as determined by the European Commission, provide adequate safeguards to data privacy.[61] These have become an option oft-recommended by privacy experts and lawyers[62] due to the relative ease of implementation and their long-standing legal validity in the EU.[63] In order to receive the immunity given to companies using Model Clauses, the Clauses must be included in agreements verbatim, leading to the benefit of needing no prior authorization from country-specific data authorities.[64] Model Clauses also have the distinct advantage of covering a wide range of data transfers.

56. Francoise Gilbert, *EU General Data Protection Regulation: What Impact for Businesses Established Outside the European Union*, 19 No. 11 J. INTERNET L., May 2016, at 3, 4–6.

57. *Overview on Binding Corporate Rules*, DIRECTORATE GENERAL FOR JUST. & CONSUMERS, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last visited Nov. 16, 2017).

58. *Id*.

59. *Id*.

60. *Id*.

61. *Id.*

62. *See* Melinda L. McLellan & William W. Hellmuth, *Safe Harbor is Dead, Long Live Standard Contractual Clauses?*, DATA PRIVACY MONITOR (Oct. 22, 2015), https://www.dataprivacymonitor.com/enforcement/safe-harbor-is-dead-long-live-standard-contractual-clauses (summarizing best practices for the usage of Model Clauses following the invalidation of the Safe Harbor Framework by the CJEU).

63. *See id. See also Model Contracts for the Transfer of Personal Data to Third Countries*, DIRECTORATE GENERAL FOR JUST. & CONSUMERS, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited Nov. 16, 2017).

64. DATA PROT. UNIT, DIRECTORATE GEN. FOR JUSTICE AND CONSUMERS, FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES 26–28 (2009), http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf.

Specifically, Model Clauses, like BCRs, can be used for intra-company transfers; they can be used for U.S.-EU transfers, like the Privacy Shield; and they have the additional benefit of being available for transfers between the EU and entities in any other jurisdiction, unlike the other two options.[65] This added flexibility, combined with the lower transactions costs associated with implementing these clauses, can be especially appealing to large, multinational companies that transfer data to different jurisdictions and between different entities. Model Clauses, though, are not without flaws, many of which will be discussed in Part IV.

Lastly, the data transfer itself may qualify for a statutory derogation.[66] Derogations may include a data transfer necessary to protect the vital interests of the data subject or a data transfer after the subject has given unambiguous consent, amongst other options.[67] Due to the highly specific and less common nature of many of the derogations, only consent will be discussed in this Note.

II. THE FUNDAMENTAL DIFFERENCES BETWEEN U.S. AND EU DATA PRIVACY POLICIES

Data protection as a concept is itself a novel and rapidly changing field, due in large part to the fact that commercialized Internet is only a few decades old.[68] Despite the relative infancy of this field, developments in how data is used and managed electronically evolve rapidly, and legislators fight a constant battle to keep pace with these changes. In light of the practical realities that attach to this field, the EU and the United States have taken substantially different views on what measures should be taken to protect the data filling the technological universe. The EU has widely confirmed the belief that citizens have a "fundamental right[]" to data protection.[69] The United States, however, does not explicitly share the view that data privacy protection is a fundamental right of all persons.[70]

A. EU PRIVACY POLICIES

The notion that "[e]veryone has the right to the protection of personal

65. McLellan & Hellmuth, *supra* note 62.

66. PRACTICAL LAW INTELLECTUAL PROP. & TECH., EXPERT Q&A: EU-US PERSONAL INFORMATION DATA TRANSFERS (2016), Westlaw W-000-8901.

67. *Id.*; DATA PROT. UNIT, *supra* note 64, at 48.

68. Cunningham, *supra* note 10, at 422.

69. Directive 95/46/EC, *supra* note 8, art. 1, at 38.

70. *See generally* Cunningham, *supra* note 10, at 422 ("Unlike in Europe, U.S. law does not recognize a fundamental right to privacy."); Loidean, *supra* note 35, at 8 (stating that the United States has a framework that has "rejected the fundamental rights approach to information privacy").

data concerning him or her" is stated plainly in the Charter of Fundamental Rights of the European Union, a document designed to lay out the basic rights of European citizens and provide guidelines relating to these rights.[71] As mentioned earlier, this EU-recognized right is reiterated in the Directive with its specifically stated purpose "to ensure that 'member states [] protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'"[72]

One explanation put forward by some commentators regarding the EU stance that data protection is a fundamental right stems from the 1940s.[73] During the Second World War, the Nazis appropriated European census records, using these records to expedite deportations to concentration camps and to strengthen Germany's hold over Europe.[74] I argue that this experience, in part, prompted the EU to take a stronger stance on privacy protections, whereas the United States, a country that has not experienced such a scarring example of what can happen when private information falls into the wrong hands, is less inclined to push for stronger protections.

Another explanation can be seen by the early adoption of the FIPs by many EU nations and the EU as a whole.[75] By adopting these principles and incorporating them into early data privacy rules and regulations, the EU set a precedential course that influenced all future privacy-related decisions. This created a multi-generational awareness of, and belief in, the importance of protecting individuals' privacy.

The focal point of the EU privacy regime has historically been the Directive. The Directive is an omnibus legislation protecting personal data, as opposed to a fragmented, country-by-country approach. The Directive has been hailed by commentators as "the most influential national data protection law."[76] Additionally, the drafters of the Directive took an important step in Article 28, making the Directive applicable in countries outside of the EU.[77] Specifically, transfers of data outside of the EU require

71. Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391, 397. *Cf.* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 466 (2016) (discussing how in the United States this right is never explicitly stated in the Constitution, and it is only implied to be relevant in certain specific areas).

72. Jörg Rehder & Erika C. Collins, *The Legal Transfer of Employment-Related Data to Outside the European Union: Is It Even Still Possible?*, 39 INT'L LAW. 129, 130 (2005) (quoting Directive 95/46/EC, *supra* note 8, art. 1, at 38).

73. Cunningham, *supra* note 10, at 426–27.

74. *Id*.

75. *See* Gellman, *supra* note 20, at 6–10.

76. Cunningham, *supra* note 10, at 427.

77. Directive 95/46/EC, *supra* note 8, art. 28, at 47–48.

contracts or other legal acts explicitly governed by EU or member-nation law.[78]

Internationally, the trend has been to follow the EU in creating legislation that applies to all data processing inside and outside of the country, largely mirroring the strict protections laid out in the Directive.[79] The thought is that if foreign countries cannot process information about EU residents, private interests will lose out on a major global market, and thus, countries will have an overwhelming incentive to come into compliance. However, despite a global trend of compliance, two powerful nations have remained defiant in the face of such measures—China and the United States.[80]

Although at first glance it may appear that the EU has come up with a comprehensive and invaluable solution to the data privacy issue, it remains, like most legislation, imperfect. One flaw is apparent simply from the name of the document: it is a directive. As such, member nations maintain some control in dictating their own privacy laws, which has led to fragmentation in the interpretations of the principles laid out in the Directive.[81] This materially limits one of the major strengths of the Directive: its being a single document utilized by all member nations.

This, however, will change with the commencement of the GDPR.[82] The key again comes in the name of the document: here it is "regulation." As a regulation, member nations no longer have the ability to interpret the document to create their individual data policies.[83] Regulations, therefore, carry with them an increased level of strength that does not exist in the Directive. All things considered, the general idea is to centralize power regarding data privacy and eliminate the sometimes patchwork effects of the Directive. This will be discussed in more detail in Part III.

B. U.S. PRIVACY POLICIES

In describing the United States' approach to data privacy policy, it may be useful to imagine a scheme opposite to that of the EU. The United States

78. *See id*. art. 25, at 45–46.

79. Cunningham, *supra* note 10, at 426–27.

80. *See id.* at 426–27 ("The Directive set the international standard for data privacy and security regulation and facilitated a trend among technologically advanced countries toward adopting nationalized data privacy laws.").

81. *See generally* Rehder & Collins, *supra* note 72, at 132.

82. Manu J. Sebastian, *The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises?*, 31 SYRACUSE J. SCI & TECH. L. 216, 225–26 (2015).

83. *See id*.

government does not recognize a fundamental right to privacy.[84] Additionally, the United States "uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation."[85] U.S. privacy laws are often responses to particular events and are tailored to particular industries and types of data, similar to a firefighter running around putting out individual fires one at a time.[86] This has led to not only inefficiently overlapping polices but also notable gaps in the U.S. privacy framework.[87] These gaps in protection have been used as an explanation as to why the United States failed to satisfy an adequacy decision by the EU before the initiation of the Safe Harbor.[88]

As discussed in Part I, the United States produced the FIPs in 1973 as an early step in privacy protection. Here, however, the United States went in a different direction than the EU, which is one possible explanation for the very different positions that each holds today. The United States did not explicitly create broad legislation with the FIPs in mind;[89] instead, it opted for various acts and statutes determined by the needs of certain industries and agencies which interpreted and revised the FIPs in various ways.[90] Further, early laws incorporating the FIPs were applicable only to public sector entities, applying only in specific circumstances to the private sector.[91] I argue that because of the lack of a longstanding and broad commitment to the protection of individuals' private information, U.S. citizens do not have their EU peers' deep-rooted, multi-generational awareness of and belief in the importance of protecting individuals' privacy. This leads to less political pressure on the U.S. government to enact strong privacy policies, perpetuating a cycle of citizens accustomed to weaker protections.

Another explanation for why the United States would take an approach to privacy substantially different from that of the vast majority of developed nations is similar to one rationale behind the EU policy—namely, a massive tragedy. As one commentator described, "[t]he attacks of September 11,

84. *See* Cunningham, *supra* note 10, at 422; Fairclough, *supra* note 71, at 464–66; Loidean, *supra* note 35, at 8.

85. W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 No. 11 J. INTERNET L. 1, 1, 9 (2016). *See also* Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at the Amsterdam Privacy Conference, Transatlantic Privacy After *Schrems*: Time for an Honest Conversation (Oct. 23, 2015), 2015 WL 9684096.

86. *See* Cunningham, *supra* note 10, at 422–26.

87. *See id*.

88. MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 3, 7 (2016).

89. Gellman, *supra* note 20, at 10.

90. Fairclough, *supra* note 71, at 463–66, 476.

91. Gellman, *supra* note 20, at 19–20.

2001, 'have further weakened Washington's will to protect data. [In fact, t]hrough new laws and new offices, Washington now has more unfettered access to citizens' data than ever before.'"[92] Another author, in 2002, went so far as to predict that "[c]ommunications technology is necessarily intrusive and, spurred on by international efforts to ferret out terrorism as a result of the September 11, 2001, attacks on the United States, will become even more so."[93] In summation, the September 11 tragedy planted an unshakable image in the minds of U.S. citizens as a whole, leading to an increase in concern and vigilance regarding terror threats. Whether this sentiment remains as vibrant today is beyond the scope of this Note, but terror threats are ever-present,[94] suggesting this rationale is unlikely to fade. Evidence of an ongoing desire to manage the danger includes the U.S. government's covert surveillance tactics, as exposed by the documents leaked by Edward Snowden.[95]

An additional rationale for the U.S. stance on privacy regulation results from a desire to maintain a free market economy with limited government regulation. The idea is that the government should limit regulations on businesses and allow the market to police itself. For instance, the Clinton administration advocated for industry-specific self-regulation, as opposed to government regulation.[96] That is not to say that the Clinton administration was opposed to privacy regulations, but this advocacy was a clear endorsement of a fragmented system of dealing with privacy issues. Additionally, one commentator described the Safe Harbor as being a "minimalist solution" in order to avoid a trade war "that was supposed to evolve into something stronger. It transpired, however, that the United States never intended to follow through on commitments to strengthen it."[97] While these anecdotes are far from dispositive, they do point to the endurance of an American philosophy holding that the government should not over-regulate markets.

This rationale, though, is at least debatable. For instance, President

92. *See generally* Rehder & Collins, *supra* note 72, at 131 (quoting David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL STREET J., Oct. 10, 2003, at A1).

93. Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 392 (2002).

94. *See generally* Uri Friedman, *Is Terrorism Getting Worse?*, ATLANTIC (July 14, 2016), https://www.theatlantic.com/international/archive/2016/07/terrorism-isis-global-america/490352 (explaining the rise of terrorist attacks in the period from Operation Iraqi Freedom to the present).

95. Harding, *supra* note 6, at 4–6.

96. *See* Cunningham, *supra* note 10, at 423.

97. Voss, *supra* note 85, at 10 (quoting Simon Davies, *Privacy Opportunities and Challenges with Europe's New Data Protection Regime*, *in* PRIVACY IN THE MODERN AGE 55, 57 (Marc Rotenberg et al. eds., 2015)).

Obama released a report in January 2017 calling for increased privacy regulations and re-emphasizing the right to be protected from governmental intrusion.[98] The Obama administration itself, though, was heavily criticized upon the exposure of the PRISM program undertaken by the NSA.[99] Furthermore, the views expressed in this report may not be shared by the new administration, which removed the report from the White House website the day after President Trump's inauguration and issued an executive order cutting back privacy protections for non-citizens just days after his inauguration.[100]

It would be remiss to paint a picture of the United States as being completely indifferent to individuals' privacy rights. For instance, the First, Third, Fourth, Fifth and Fourteenth Amendments collectively provide the implicit foundation for many of the laws and regulations regarding privacy in the United States.[101] There are also numerous federal laws, including the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and many others, that address the protection of private information.[102] Additionally, the Federal Trade Commission has broad powers to take enforcement actions regarding "unfair or deceptive acts or practices in or affecting commerce."[103] On top of this, individual states have passed their own regulations, with California's regarded as amongst the most comprehensive.[104] These different protective measures are likely in place because the U.S. government places at least some value on protecting individuals' privacy.

The issue, however, is that a system like this is inherently flawed. Using a patchwork structure necessarily leaves gaps.[105] In addition to gaps, individual state and federal laws are often inconsistent with one another.[106] Unfortunately, the United States has consistently rejected both omnibus

98. WHITE HOUSE, PRIVACY IN OUR DIGITAL LIVES: PROTECTING INDIVIDUALS AND PROMOTING INNOVATION, 3–9, 12–14 (2017).

99. Kate Kaye, *New Privacy Report Already Removed from White House Site*, AD AGE (Jan. 20, 2017), http://adage.com/article/privacy-and-regulation/privacy-report-removed-white-house-site/307632.

100. *See* Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017).

101. Cunningham, *supra* note 10, at 422.

102. *Id*. at 423–24. *See* Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (1999) (codified as amended at scattered sections of 12 U.S.C. (2012)); Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended at scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.); Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114-2 (1970) (codified at 15 U.S.C. 1681).

103. Brill, *supra* note 85, at 1 (quoting 15 U.S.C. § 45(a)).

104. Loidean, *supra* note 35, at 8.

105. *Id*.

106. *See* Cunningham, *supra* note 10, at 423.

legislation and the fundamental-rights approach to data protection.[107] There is no more clear depiction of this than the egregious surveillance tactics used by the U.S. government and revealed in the Snowden leak. Just as September 11 dramatically changed the landscape of data privacy protection in the United States, the Snowden documents dramatically altered the state of EU-U.S. privacy relations.

III. HOW THE GDPR AFFECTS THE CURRENT AND FUTURE DATA PROTECTION LANDSCAPE

The Directive has stood as the basis for EU data privacy law since 1995. The Directive provides the structure and legal guidelines with which the Safe Harbor, the Privacy Shield, the Model Clauses, and other transfer mechanisms seek to comply. The Directive, however, is nearing extinction. On April 14, 2016, the European Parliament approved the GDPR; it takes effect on May 25, 2018, at which point companies will need to be in compliance with the new, stronger regulation.[108] This section of this Note will focus on how the GDPR differs from the Directive and what that means in terms of compliance and the potential transfer mechanisms.

A. WHAT'S NEW IN THE GDPR?

The GDPR sets out to tackle the same goal as the Directive—protecting the fundamental rights and freedoms of the EU citizenry with regard to the handling of personal data.[109] The goal is to do this while also facilitating efficiencies within the European economy and helping to promote economic and social progress.[110] These goals, however, are pursued slightly differently in the GDPR than in the Directive.

First, as mentioned earlier, a relevant distinction between the GDPR and the Directive is identifiable by looking at the titles of the two enactments. The GDPR is a "regulation," whereas the Directive is a "directive." This matters because a directive gives only guidance to member nations, allowing each member nation to interpret the directive and achieve its purposes in whatever way they deem appropriate.[111] A regulation, however, is applicable to each member nation and does not have to be enacted into each individual country's legal framework.[112]

107. Loidean, *supra* note 35, at 8.
108. EU GDPR PORTAL, http://www.eugdpr.org (last visited Nov. 16, 2017).
109. General Data Protection Regulation, *supra* note 8, at 1.
110. *Id*.
111. Gilbert, *supra* note 56, at 4.
112. *Id*.

The impact of this should not be understated. A major issue with the current system is that companies must deal with greatly differing regulations in each nation in which they maintain data. This, in large part, will be eliminated. The EU stated in a press release that the estimated savings from creating a "one-stop-shop" will be in the neighborhood of €2.3 billion per year.[113] Nevertheless, while the GDPR will remove a substantial amount of the difficulty that has arisen from potentially having to comply with twenty-eight different member-state data protection laws, companies must be aware that there are still some areas in which member nations have discretion.[114] An example can be seen in Article 6(1)(e), regarding one way in which a company can legally process personal data.[115] This provision allows processing when "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[116] All in all, though, one of the most consequential differences of the GDPR will be the decrease in administrative costs faced by companies who no longer have to negotiate, communicate, and work with data protection authorities from many different nations.

A second difference between the GDPR and the Directive is the strengthened focus on individuals' rights vis-à-vis the way the world transfers, accesses, and uses data. In 2017, personal data is being transferred at speeds and in volumes that were unthinkable not long ago, and consumers recognize a need for strong protection. As stated by the EU, "[n]ine out of ten Europeans have expressed concern about mobile apps collecting their data without their consent."[117]

The specific individual rights highlighted in the GDPR are the right to be informed, the right of access, the right of rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights related to automated decision-making and profiling.[118] These rights focus on two overarching goals of the GDPR. First, the GDPR

113. European Commission Statement 16/1403, *supra* note 48.

114. Gilbert, *supra* note 56, at 4.

115. *Lawful Processing*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider (last visited Nov. 16, 2017).

116. General Data Protection Regulation, *supra* note 8, at 9.

117. European Commission Memorandum 15/6385, *supra* note 49. There is a growing concern over data privacy associated with in-home connected devices and apps, such as Amazon's Alexa, and health-tracking devices, like Fitbit. For further discussion, see Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 78–81 (2016); Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and* Kyllo*: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 760–62 (2015).

118. *Individuals' Rights*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights (last visited Nov. 16, 2017).

increases the availability and clarity of the information provided to individuals whose data is being processed. Second, it grants citizens more control over the data they provide and also gives the citizens easier access to legal remedies for breaches. While not all of these rights are completely new or different than rights discussed in the Directive, in general they are written in a way that strengthens the rights of the citizen.[119]

Third, the definition and application of "consent" have been adjusted to further protect individuals. Consent needs to be clear, unambiguous, specific, informed, and freely given.[120] Further, the language in the GDPR seems to have noticeably narrowed the possibility of a type of implied consent arguably possible under the Directive.[121] The GDPR also has another important new feature regarding consent. Individuals are now allowed to withdraw consent at any time, and this withdrawal must be as easy to execute as the original consent.[122] This further emphasizes the strong weight the EU has placed on strengthening the role of the individual in the handling of one's private information.

Fourth, the enforceability of the GDPR and the accountability of companies have been enhanced by new procedures, which companies must follow in order to ensure that data is appropriately protected and processed. The accountability principle accompanies transparency in an attempt to strengthen citizens' trust in how their data is handled.[123] One way of accomplishing corporate accountability is by mandating "[d]ata protection by design" and "[d]ata protection by default."[124] These concepts, in short, mean that projects being designed or undertaken by companies must consider appropriate data protection mechanisms from inception and throughout their duration.[125] This includes safeguards such as minimizing the processing of personal data, anonymizing data as soon as possible, and building services and applications with "state-of-the-art" data protection.[126] Accountability is also addressed in a few other ways. First, there are stricter regulations governing how companies record what data they are processing

119. European Commission Memorandum 15/6385, *supra* note 49.

120. General Data Protection Regulation, *supra* note 8, arts. 4, 7, at 34, 37. Consent is further discussed throughout the GDPR. *See id.*, *passim*.

121. *See* Gilbert, *supra* note 56, at 6–7. *But see* Cunningham, *supra* note 10, at 437–38.

122. Sebastian, *supra* note 82, at 233.

123. European Commission Memorandum 15/6385, *supra* note 49.

124. *Id*. *See also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (2011), https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

125. Sebastian, *supra* note 82, at 230.

126. General Data Protection Regulation, *supra* note 8, art. 25, at 48.

and for what purpose.[127] Second, extensive privacy impact assessments are necessary to comply with the requirement that companies maintain effective procedures to protect personal data.[128] These assessments analyze the risks to individuals, determine the necessity and proportionality of the processing in relation to the purpose, and give a description of the processing operations and the legitimate interests pursued by the data controller.[129] Lastly, data protection authorities will be able to fine companies up to 4 percent of their global annual revenue for violations of the rules.[130]

Certainly there are other differences between the two enactments, but I have highlighted the most relevant to the issue at hand. Altogether, the key differences between the GDPR and the Directive are that the GDPR (1) takes a stronger stance on the accountability and enforcement of the principles that underlie the regulation and (2) gives individuals access to more information and a larger role to play in the data processing process. Each of these goals is championed by the EU and appears to have played an important role in the creation of the GDPR.[131] The GDPR balanced pro-economic benefits by achieving a "one-stop-shop" concept to dramatically reduce transaction costs for companies—especially those operating in more than one EU nation—and secured pro-individual rights through greater transparency and accountability from companies processing personal data.

B. HOW DOES THIS AFFECT DATA TRANSFER MECHANISMS?

As alluded to in the previous section, there are more than a few new and unique challenges that companies will face in trying to transfer data across the Atlantic. The GDPR, however, does quite a bit to clarify the transfer mechanisms available to companies, while also introducing a few new ones. I will focus on BCRs, Model Clauses, and Codes of Conduct and Certification Mechanisms.

127. *Accountability and Governance*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance (last visited Nov. 16, 2017).

128. Sebastian, *supra* note 82, at 231.

129. *Accountability and Governance*, *supra* note 127.

130. European Commission Memorandum 15/6385, *supra* note 49. To understand the potentially massive scope of these penalties, the fines that could be levied against Amazon and Google, based on their 2016 reported revenues, would be approximately $5.4 and $3.6 billion, respectively. Richard Stiennon, *Unintended Consequences of the European Union's GDPR*, FORBES (Nov. 27, 2017, 6:26 P.M.), https://www.forbes.com/sites/richardstiennon/2017/11/27/unintended-consequences-of-the-european-unions-gdpr/#46aae406243c,

131. *Id*.

1. BCRs

The GDPR provides a very important upgrade to the BCRs that were developed based on the Directive. In an attempt to increase consistency of the enforcement of the data protection laws, indirectly reducing transaction costs and thus appeasing businesses, the GDPR formally recognizes the use of BCRs and lays out a mechanism for utilizing and monitoring BCRs in Article 47.[132] Prior to this change, companies would need separate approvals from each country in which they handled personal data, and only two-thirds of EU member nations recognized BCRs as appropriate protective measures.[133] These upgrades will certainly help to make BCRs much more efficient for companies with entities in various countries.[134] However, as will be discussed in Part IV, BCRs are still far from a perfect option for the vast majority of companies.

2. Model Clauses

As stated in Article 46, Model Clauses will remain an appropriate safeguard for transferring data so long as the clauses are approved as described in Article 93(2).[135] As with BCRs, the provisions of the GDPR substantially reduce the administrative burden of Model Clauses. There are a few relevant changes that facilitate this increase in efficiency. First, the EU commission will create a new set of Model Clauses pursuant to the GDPR, which will not require the prior authorization of the nation from which the data is being processed.[136] While the Model Clauses have long been intended to need little-to-no approval from individual nations under the Directive, nation-specific issues still existed regarding appropriate filings, monitoring, and additional objections.[137] Another relevant change involves ad hoc contractual clauses. These can include independently drafted clauses or some variations to the terms of the Model Clauses. The GDPR makes it so that these clauses will need to be approved only by an appropriate supervisory

132. General Data Protection Regulation, *supra* note 8, art. 47, at 62–64.

133. Gilbert, *supra* note 56, at 5 (stating that fewer than one hundred companies have sought to use BCRs, despite this option having been available for a decade).

134. *See* PRACTICAL LAW INTELLECTUAL PROP. & TECH, *supra* note 66.

135. General Data Protection Regulation, *supra* note 8, arts. 46, 93, at 62, 86.

136. Gilbert, *supra* note 56, at 4–5.

137. *See* Directive 95/46/EC, *supra* note 8, arts. 21, 26, at 44, 46 (outlining the roles of member states in ensuring adequate protection for data transfers and the objections and limits that they may put in place). *See* also *ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14* (Oct. 14, 2015), https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf (arguing that Model Clauses are an inappropriate transfer mechanism for transfers to the United States, due to direct conflicts between U.S. law and the provisions in the Model Clauses.).

authority in order to apply to all EU nations.[138] In contrast, the Directive's clauses required approval by each and every nation's data protection authority before they could be considered adequate.[139] Here, the important differences are that these clauses are intended to increase efficiency—accomplished by the overarching "one-stop-shop" notion—and to provide flexibility for companies to create adequate provisions that better fit their businesses.

3. Codes of Conduct and Certification

Two of the unique transfer mechanisms detailed in the GDPR are the Codes of Conduct and Certification. Article 40 of the GDPR explains that a notable goal of EU privacy officials is to encourage the creation of Codes of Conduct.[140] The Codes of Conduct in large part work like a non-member state seeking to acquire an adequacy decision under the Directive or a single entity seeking approval of BCRs, except that the codes apply to associations or representative bodies.[141] This option is targeted at small- and medium-size companies within certain sectors of the economy that frequently do business with one another.[142] The codes—if certified by an appropriate supervisory authority and combined with binding and enforceable commitments of the controller/processer to use adequate safeguards—qualify as an appropriate transfer mechanism for data leaving the EU.[143] The codes, however, must be reviewed by multiple levels of the EU data privacy hierarchy in order to be deemed to have "general validity within the Union," which places an administrative hurdle on the use of this option.[144]

Certification, as described in Article 42, is a transfer mechanism that remains in its infancy, but it is very similar to the Codes of Conduct.[145] Certification mirrors the Codes of Conduct in the sense that it is intended to benefit small- and medium-size companies, it has a similar registration and approval process, and it legitimizes data transfers when combined with appropriate commitments of the controller/processer.[146] It also bears similarity in that it is has the effect of a non-member state's receiving an

138. General Data Protection Regulation, *supra* note 8, arts. 92–93, at 85–86.
139. Cunningham, *supra* note 10, at 438–40.
140. General Data Protection Regulation, *supra* note 8, art. 40, at 56.
141. *See* Directive 95/46/EC, *supra* note 8, arts. 25–26, 30, at 45–46, 48–49 (providing language regarding adequacy decisions).
142. General Data Protection Regulation, *supra* note 8, art. 40, at 56.
143. Gilbert, *supra* note 56, at 5.
144. General Data Protection Regulation, *supra* note 8, art. 40, at 57.
145. *See generally id*. art. 42, at 58–59.
146. *Compare id*. *with id.* art. 40, at 56.

adequacy decision, but the key difference between the two is that Certification can be obtained by a single company.

IV. THE FATAL FLAWS OF THE PRIVACY SHIELD, MODEL CLAUSES, AND BCRS

A. PRIVACY SHIELD

It is worth stating at the outset that the Privacy Shield agreement is between the United States and the EU. This is an important starting point, because this transfer mechanism is unique: companies relying on it are relying not just on their own compliance with EU data regulations, but also on the assumption that actions of the U.S. government (such as the illegal surveillance actions that led to *Schrems I* and the Safe Harbor invalidation) will not jeopardize privacy relations with Europe. This is a risky position for a corporation to place itself in, as the relationship between the EU and the United States is sewn with distrust and remains incredibly fragile due to the Snowden revelations. Additionally, the necessity for a better understanding of the shortcomings of the Privacy Shield is underscored by the fact that over 2,400 companies have signed up for it as of late 2017.[147] This Note will now address some of the risks associated with choosing this method.

First, the Privacy Shield is an unsatisfactory solution for companies aware of the GDPR's imminence. The Privacy Shield was created in line with the no-longer-applicable provisions of the Directive, instead of with the stronger privacy protections contained in the GDPR. Because of this, it will likely fail to meet the heightened requirements of the GDPR, and it will thus have to undergo serious revision.[148] As seen with the struggle to agree on the Privacy Shield in a quick and efficient manner following the invalidation of the Safe Harbor,[149] revisions to the Privacy Shield or the drafting of a new agreement altogether may create substantial delays and unwanted uncertainty.

Second, as laid out in Part II of this Note, the United States and EU have

147. *Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S. Privacy Shield*, at 4, SWD (2017) 344 final (Oct. 18, 2017) [hereinafter *Report on the First Annual Review*]; Grant Gross, *Tech Companies Like Privacy Shield but Worry About Legal Challenges*, PCWORLD (Dec. 21, 2016, 3:00 AM), http://www.pcworld.com/article/3152559/security/tech-companies-like-privacy-shield-but-worry-about-legal-challenges.html.

148. Doron S. Goldstein et al., *Understanding the EU-US "Privacy Shield" Data Transfer Framework*, 20 No. 5 J. INTERNET L. 1, 1, 21 (2016).

149. *Privacy Shield Timeline*, PRIVACYTRUST, https://www.privacytrust.com/privacyshield/privacy-shield-timeline.html (last visited Nov. 16, 2017).

vastly different views on privacy rights. Granted, they each have a strong incentive to bridge the gap, given the undeniable economic benefits for doing so. But this may be especially hard to do in light of President Trump's strong stance regarding the utilization of surveillance to combat terrorism. Before taking office, Trump had already encouraged a boycott of Apple products due to its refusal to create a "back door" entry into the cell phone of one of the San Bernardino shooters,[150] and said that he believed that the NSA "should be given as much leeway as possible. However . . . . [t]here must be a balance between those Constitutional protections and the role of the government in protecting its citizens."[151]

Once in the White House, Trump further strained EU-U.S. privacy relations by issuing an executive order excluding non-U.S. citizens from the protections of the Privacy Act of 1974.[152] In reply, Jan Philipp Albrecht, the rapporteur for the EU's data protection regulation, tweeted that the EU should immediately suspend the Privacy Shield and sanction the United States.[153] The European Commission issued a statement noting that the Privacy Shield "does not rely on the protections under the U.S. Privacy Act."[154] Nonetheless, this has added to the tension between the EU and United States and further brought the validity of the Privacy Shield into question. While it is unclear how President Trump and Congress will handle impending issues related to privacy protections, like the expiration of Section 702 of the U.S. Foreign Intelligence Surveillance Act,[155] companies should be aware of the potential for the White House and Congress—each with an eye toward increasing government surveillance—to drastically increase U.S.-EU tensions and put the Privacy Shield at risk.

Third, there are fundamental aspects of the Privacy Shield that are inconsistent with the GDPR and are subject to the same criticisms that led to the Safe Harbor's invalidation. First, the EU hails U.S. "assurances" that it

150. Reuters, *Trump Election Ignites Fears over U.S. Encryption, Surveillance Policy*, FORTUNE, (Nov. 9, 2016), http://fortune.com/2016/11/09/trump-encryption-surveillance-policy.

151. Yoni Heisler, *A Comprehensive Look at All of Donald Trump's Positions on Technology Issues*, BOY GENIUS REP. (Oct. 19, 2016, 10:53 A.M.), http://bgr.com/2016/10/19/donald-trump-politics-technology-opinions.

152. *See* Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017).

153. Jan Philipp Albrecht (@JanAlbrecht), TWITTER (Jan. 26, 2017, 1:45 AM), https://twitter.com/JanAlbrecht/status/824553962678390784.

154. Natasha Lomas, *Trump Order Strips Privacy Rights from Non-U.S. Citizens, Could Nix EU-US Data Flows*, TECHCRUNCH (Jan. 26, 2017), https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows.

155. *See Report on the First Annual Review*, *supra* note 147, at 4. For additional discussion, see Kaye, *supra* note 99.

will limit mass surveillance.[156] Not only did these assurances come from the potentially more privacy-friendly Obama administration, but they also seem weaker than is acceptable under the GDPR standards. For instance, the NSA maintains the ability to utilize "bulk" collection tactics, so long as they are consistent with various opaque limitations subject to a good deal of interpretation.[157] Second, the Privacy Shield's lauded redress mechanisms, which utilize an independent ombudsperson,[158] are vastly overstated, as well as undermined by a clear conflict of interest: the ombudsperson is appointed by, and reports to, the U.S. Secretary of State.[159] Certainly, the Privacy Shield attempts to lay out provisions to ensure the independence of the ombudsperson, but these provisions are speculative at best. Most importantly, it is difficult to imagine their being considered protections "essentially equivalent" to those afforded by EU member nations.

Fourth, the Privacy Shield is already facing legal challenges, largely in line with the above points,[160] and the initial version received harsh criticism from the Article 29 Working Party regarding the precise issues that led to the Safe Harbor invalidation.[161] Are these legal challenges likely to succeed? It is unclear. Was the Privacy Shield revised to try and appease the Article 29 Working Party? Yes.[162] Regardless, it is concerning that the Privacy Shield is facing such hurdles so early on, especially considering the panicked state in which the Safe Harbor invalidation left so many companies, as well as the already tenuous relationship between the U.S. and EU.[163]

In summation, the Privacy Shield agreement is a potentially dangerous option for U.S. companies. While it certainly has some benefits in terms of relative ease of implementation and flexibility,[164] it is shrouded in uncertainty and question marks. The question marks remain the same as

156. European Commission Press Release IP/16/2461, *supra* note 43.

157. *See* Commission Implementing Decision 2016/1250, 2016 O.J (L 207) 1, 13–20 (EU).

158. *See id.* at 28–29 (explaining that the ombudsperson is supposed to be independent from the U.S. intelligence agencies and is in charge of following up on complaints and enquiries from individuals regarding potential privacy violations).

159. *See id.* at 27–29, 71.

160. *See* Loyens & Loeff, *Digital Rights Ireland Challenges EU-US "Privacy Shield*," LEXOLOGY (Nov. 4, 2016), http://www.lexology.com/library/detail.aspx?g=5055de04-e2d7-4b0b-9bbe-789a4a97b318; Reuters, *French Privacy Groups Challenge the EU's Personal Data Pact with U.S.*, FORTUNE (Nov. 2, 2016), http://fortune.com/2016/11/02/privacy-shield-pact-challenge.

161. *See* Opinion 01/2016, *supra* note 15, at 9–14.

162. *See generally* Voss, *supra* note 85 (discussing how the Privacy Shield came about and what it is meant to do).

163. *See* Steven C. Bennett, *EU Privacy Shield: Practical Implications for U.S. Litigation*, 2 PRAC. LAW., Apr. 2016, at 60, 62–64.

164. Goldstein et al., *supra* note 148, at 20 (discussing the Privacy Shield requirements and implications for participating organizations).

those that led to the invalidation of the Safe Harbor, and with a surveillance-friendly administration in the White House, the relationship between the EU and U.S. will likely remain uneasy going forward. A potential invalidation would leave thousands of companies scrambling for an alternative method of compliance while risking steep fines. Therefore, the decision to certify under the Privacy Shield is the decision to place faith in a hastily prepared band-aid fix for the bursting dam that followed the invalidation of the Safe Harbor. It requires not only trust in one's own ability to comply with the more complex EU regulations but also trust that U.S.-EU privacy relations will not slip from the shaky ground on which they already reside. That is a scary decision to make, and one that I would not advise.

B. MODEL CLAUSES

While the forecast for the Privacy Shield is decidedly gloomy, the outlook for Model Clauses seems at least somewhat brighter. However, there are a few definitive practical flaws that make Model Clauses an insufficient option for long-term GDPR compliance. I will briefly discuss some of the basic practical issues with using Model Clauses, including their rigidity and the cumbersome aspect of having to include them in every data-transfer-related contract, before focusing on the more concerning, potentially fatal flaws regarding the legal validity of this compliance mechanism.

First, the GDPR has not expressly accepted the current Model Clauses. Instead, as described in Part III above, the GDPR outlines a process through which the EU Commission will create a new set of Model Clauses.[165] Utilizing one of the three current sets of Model Clauses is therefore a temporary solution at best. One additional general criticism of Model Clauses is that companies must be sure to include them in every single contract they have in order to validly transfer data. Thus, if the current Model Clauses are not valid under the GDPR, companies will be forced to amend every single contract relating to data transfers. While it is certainly possible that the current Model Clauses may be determined to provide adequate safeguards, it seems unlikely that the GDPR would make no mention of them if this were more assuredly the case, particularly since BCRs were explicitly included and described.

Second, and to go even further with the point above, the current Model Clauses' validity is hotly contested. One of the strongest examples of pushback came in a position paper from the Independent Center for Privacy

165. *See* Cunningham, *supra* note 10, at 426–28; Gilbert, *supra* note 56, at 4–5.

Protection in Schleswig-Holstein ("ULD").[166] In this paper, the ULD took a powerful stance, stating that "a data transfer on the basis of Standard Contractual Clauses to the US is no longer permitted."[167] Soon after, a conference of Germany's data protection commissioners largely agreed.[168] Model Clauses also face legal challenges via Maximilian Schrems's class-action lawsuit against Facebook.[169] The case is progressing slowly due to procedural issues, but it highlights the volatility surrounding the Model Clauses.[170] However, the views of those objecting to the validity of the Model Clauses are not unanimously held. For instance, the Article 29 Working Party and the EU Commission have continued to back the Model Clauses in spite of *Schrems I*.[171] Even so, it is difficult to ignore the uncertainty surrounding these clauses—and the potential expense their invalidation or amendment would incur.

Third, the current challenges described above have legitimacy. As the ULD stated, American companies using Model Clauses are subject to American surveillance laws—the same ones that led to the invalidation of the Safe Harbor and which make it impossible to provide the necessary protections for citizens.[172] The notion is simple: having Model Clauses in a contract will do nothing to stop the United States from conducting the types of surveillance that led to the invalidation of the Safe Harbor. Because of this, U.S. companies will not be able to comply with the section of the clauses stating that U.S. companies are not subject to laws that make it impossible to follow the instructions of the data exporter.[173] This contention has not yet led to the invalidation of the Model Clauses, but it remains a cloud hanging over their legitimacy.

In summation, Model Clauses are a risky option for companies for multiple reasons. First, using the current Model Clauses will lead to companies having to amend every one of their contracts when the GDPR begins to be enforced. This will be both costly and time-consuming. Also, the Model Clauses already face scrutiny from certain nations' data protection

166. *See ULD Position Paper*, *supra* note 137.

167. *Id*., at 4.

168. *See DSK Position Paper* (Oct. 21, 2015), https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/DSK_position_paper_Safe-Harbor_2015-10-21.pdf.

169. Matt Burgess, *Facebook Privacy Case Is Making Its Way to the European Court of Justice*, WIRED (Sept. 13, 2016), http://www.wired.co.uk/article/facebook-privacy-eu-case-cjeu.

170. *Id*.

171. Darren Isaacs, *Practical Strategies for Maintaining HR Data Flows from Europe to the US and Beyond—After the* Schrems *Case, 'Safe Harbor 2.0' and the Incoming Data Protection Regulation*, 1 EMP. & INDUS. REL. L. 33, 33, 35 (2016).

172. *ULD Position Paper*, *supra* note 137, at 4. *See also* Gross, *supra* note 147.

173. *See* Commission Decision 2001/497/EC, app. 2, 2001 O.J. (L 181) 19, 22, 30 (EC).

authorities and could very well be invalidated even before the GDPR comes into play. Again, this would leave companies scrambling to find a new, legally valid mechanism. All this being said, of course, once the EU Commission approves GDPR-compliant Model Clauses, it may well be smart to utilize them, and they should be analyzed at that time. The issue is that these clauses do not yet exist, and the current Model Clauses are riddled with issues.

C. BCRs

BCRs are a long-standing mechanism available by which U.S. companies comply with EU privacy laws. Despite having a history of valid and adequate protection, however, BCRs today are practically useless for most companies. The fatal flaws of BCRs generally stem from the practical impediments to their use as well as their now-questionable legal validity.

First, BCRs only apply to a very specific type of data transfer, making them unavailable to many companies. They apply when data is transferred amongst entities that are part of the same corporate group.[174] Because of this, BCRs are useless for companies that transfer data externally. This excludes a wide variety of industries, including those which transfer human resources data to third parties and which transfer third-party market research data. Thus, many companies cannot use BCRs based upon a basic limiting factor.

Second, practical impediments to BCR approval eliminate this option for the vast majority of remaining companies. Companies must receive approvals from each separate data protection authority, which can take between eighteen and twenty-four months.[175] To further illustrate the difficulty and limited usefulness of BCRs, in more than ten years of their validity as a transfer mechanism, only around one hundred companies have actually obtained approval.[176] The enormous costs of compiling the BCRs make them viable only for massive multinational corporations like General Electric or Shell.[177] Entities with both the resources to pursue the BCR process and strictly (or mainly) intra-company data transfer requirements comprise a decidedly limited category, and many within it will still choose to pursue less burdensome and more practical mechanisms.

Third, BCRs currently face the same legal challenges as Model Clauses.

174. *Overview on Binding Corporate Rules*, *supra* note 57. *See also* Cunningham, *supra* note 10, at 439–40.

175. *See* Cunningham, *supra* note 10, at 440; Gilbert, *supra* note 56, at 5.

176. *See* Gilbert, *supra* note 56, at 5.

177. Sebastian, *supra* note 82, at 242.

To summarize, some data protection authorities have stopped considering BCRs as an acceptable transfer mechanism.[178] Currently, BCRs are only recognized by about two-thirds of member nations.[179] Ultimately, companies must recognize that the validity of BCRs, like Model Clauses, is necessarily clouded following *Schrems I*, and that countries have already begun to show distaste for them.

However, BCRs were significantly strengthened via the GDPR, and their future legal validity seems to stand on much firmer ground than the Model Clauses. The GDPR will also allow BCRs to apply to transfers outside the corporate group.[180] These transfers must be accompanied by commitments and agreements of the external parties to provide adequate protections,[181] a requirement that essentially replicates the Model Clauses. Companies will now have to take the time and effort to include contractual protections in every contract they make, thus removing one of the benefits of BCRs—not having the burden of exacting privacy commitments in every contract. Additionally, if a company is going to pursue this option, it is important to guarantee that its BCRs are GDPR-compliant. Companies *currently* using BCRs may see them invalidated or in need of revision in the future.

Nonetheless, BCRs remain an untenable option for most companies. While the GDPR appears to streamline the process of BCR adoption through the "one-stop-shop" concept that is inherent in the regulation,[182] it is still a complex process demanding substantial resources. Further, there is no evidence that approvals will indeed be streamlined using the GDPR. At this point, any increase in efficiency promised by the GDPR's passage is speculative at best.

Ultimately, BCRs may be better suited to overcome legal concerns than the other mechanisms and may serve as a relatively stable transfer mechanism under the GDPR. However, BCRs still face the limitations mentioned in the first two points above: they are only viable for large, multinational corporations that are primarily transferring data amongst their own corporate groups. Because of this, BCRs are a solution in only very limited circumstances.

178. *DSK Position Paper*, *supra* note 168, ¶ 2.
179. Gilbert, *supra* note 56, at 5.
180. *See* General Data Protection Regulation, *supra* note 8, art. 47, at 63.
181. *See id*.
182. European Commission Statement 16/1403, *supra* note 48.

V. SO, WHAT OPTIONS DO COMPANIES HAVE?

All hope is not lost. Data is still going to flow across the Atlantic. Many of the above mechanisms will continue to be used, and companies will, at least for the time being, be able to get away without updating and adjusting their privacy policies to conform with the upcoming implementation of the GDPR. For instance, a survey from July 2017 found that 89% of U.S. organizations impacted by the GDPR are unprepared for the upcoming changes.[183] Companies that choose not to address this matter risk facing massive expenses if and when their privacy policies become inadequate.

There are a few potential options that companies can begin to adopt in order to best prepare themselves for privacy regulations going forward. However, there simply is no right answer, no magic solution to insulate companies from all risk. The suggestions below have their flaws, but in my estimation, they provide additional security for companies facing an uncertain privacy landscape. Finally, though it almost goes without saying, companies must strongly consider layering their privacy measures. Having multiple levels of transfer mechanisms enables companies to continue operations if one mechanism faces legal troubles, and they can save companies from the substantial costs of having to rapidly institute new compliance measures. It would be foolish for cautious firms not to diversify their privacy measures, just as it would be foolish for cautious investors not to diversify their investments.

That said, I will discuss how obtaining consent and utilizing the GDPR Codes of Conduct and Certification are useful privacy protections to layer on top of other transfer mechanisms.

A. CONSENT

As discussed above, a major goal of the GDPR is to increase transparency and give individuals more of a role in how their data is handled.[184] Because of this, consent is discussed at great length in the GDPR.[185] The notion of consent necessarily depends on providing information to the individual whose data will be transferred. Thus, obtaining consent is a valuable tool for acting in accordance with the spirit of the GDPR and thus (potentially) appeasing privacy officials. Consent, however,

183. Alex Hickey, *6 Months to GDPR: What's Next*, CIO DIVE (Nov. 28, 2017), https://www.ciodive.com/news/6-months-to-gdpr-whats-next/511761.

184. *See* European Commission Statement 16/1403, *supra* note 48.

185. *See* General Data Protection Regulation, *supra* note 8, *passim*.

is not a perfect solution. Consent must be free and specific.[186] This standard can be difficult to achieve in some situations and may not be in a company's best interest in other situations. For instance, consent to the transfer of human resource data is problematic in an employer-employee relationship in which there is a clear bargaining advantage for the side receiving the data.[187] For example, if a job offer is conditioned on consent to data transfers, the consent that is received is unlikely to be considered "free." Also, the GDPR mandates that individuals need to consent to the specific use of their data.[188] Some companies may be using data in ways that may be dissatisfying to its users or customers, which could cause bad publicity. Consent is also limited by the age of the individual whose data is being processed. The GDPR states that the processing of data of individuals younger than sixteen will require parental permission, and it gives member nations the choice to lower this age to thirteen.[189] Because of this, companies—like Facebook—with younger users face real difficulties in obtaining adequate consent.

Nonetheless, this is a very good starting point for many firms. Companies are already required to process data in a manner consistent with a clear purpose.[190] This purpose should be articulable to the individuals whose data is being processed, and so consent should be at least theoretically possible. Finally, the cost and additional burden associated with obtaining consent may be minimal for companies, depending on their specific situations, and proper attempts to obtain that consent will likely be viewed positively by the data protection authorities, who have clearly placed an emphasis on this transfer mechanism.

B. PREPARE FOR THE GDPR

During this notably volatile time for data privacy compliance, a company should utilize multiple transfer mechanisms, and beyond this, organizations would be wise to begin preparing to meet the stricter regulations of the GDPR. Updating transfer mechanisms in line with the GDPR is a time-consuming and expensive venture,[191] but it is the single best way to minimize risk during this volatile time. To do this, companies will

186. *See id.*, arts. 4, 6–8, at 34, 36–38.

187. *See* Isaacs, *supra* note 171, at 35.

188. General Data Protection Regulation, *supra* note 8, art. 6, at 37.

189. Gilbert, *supra* note 56, at 4.

190. General Data Protection Regulation, *supra* note 8, at 6–7.

191. *See Pulse Survey: GDPR Budgets Top $10 Million for 40% of Surveyed Companies*, PWC, https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html (last visited Nov. 29, 2017) (finding that 40% of companies that have completed their GDPR preparations have spent more than $10 million).

want to work with data protection authorities and/or hire a data protection officer to revise their current Model Clauses or BCRs in line with what the GDPR expects. Further, companies should consider pursuing Codes of Conduct and Certification. These options allow for a certain level of flexibility and insulation from regulatory charges in the country.[192] Additionally, the EU Commission specifically emphasized using these mechanisms.[193] Using the mechanism may thus show an intention to act in line with the goals of the Commission and engender some goodwill. It is not to say that these *must* be pursued, but at minimum, they should be considered and evaluated. Moreover, despite the criticisms of Model Clauses and BCRs, they can be viable options when drafted in compliance with the GDPR. What is most important here is that companies take the time to work with data protection officers or agencies to ensure that the mechanisms they plan to utilize are GDPR compliant.

In conclusion, depending on the company's data processing activities, Model Clauses, BCRs, Informed Consent, and/or Codes of Conduct/Certification may be utilized as viable transfer mechanisms if managed and developed in line with the stricter language of the GDPR. On the other hand, companies relying solely on the Privacy Shield, despite its questionable validity and the fragile state of EU-U.S. affairs, expose themselves to substantial risk, which could prove costly to the greater of €20,000,000 or 4% of annual revenue. That being said, determining the best way to insulate any given company from the risks associated with volatile data privacy laws is incredibly difficult. The best thing a company can do to combat this difficulty is to understand what exactly the GDPR will demand and to prepare accordingly. In the meantime, companies can weather the storm, using their understanding of the GDPR to revise current policies to align with the stricter realities of the future. Ultimately, developing an understanding of the variety of options that can be used, employing different transfer mechanisms based on particular data transfer needs and data types, and being proactive will save a company substantial costs and significantly reduce its risk exposure.

192. *See* General Data Protection Regulation, *supra* note 8, art. 40, at 56–58. *See also* Gilbert, *supra* note 56, at 3–5.

193. *See* Gilbert, *supra* note 56, at 3–5.