


2016

The Need for an International Convention on Data Privacy: Taking a Cue from the CISG

Morgan Corley

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjil>

 Part of the [Commercial Law Commons](#), [Comparative and Foreign Law Commons](#), [Contracts Commons](#), [Courts Commons](#), [European Law Commons](#), [International Law Commons](#), [Internet Law Commons](#), [Legislation Commons](#), [Other Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Morgan Corley, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, 41 Brook. J. Int'l L. (2016).
Available at: <https://brooklynworks.brooklaw.edu/bjil/vol41/iss2/5>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of International Law by an authorized editor of BrooklynWorks.

THE NEED FOR AN INTERNATIONAL CONVENTION ON DATA PRIVACY: TAKING A CUE FROM THE CISG

INTRODUCTION

Since its inception, the Internet was designed to be both borderless and global in nature.¹ The Internet allows for the movement of data around the world with the click of a mouse, making the distinguishing of geographic boundaries within the Internet impossible.² Furthermore, recent technological developments³ have provided companies with low-cost, reliable means to transfer personal data around the world at an exceedingly fast rate.⁴ As a result, the commercial industry has utilized these advances to establish relationships with customers and businesses located in different nations, resulting in increased economic globalization.⁵

Consequently, there is now “a nearly constant flow of personal information across national borders.”⁶ Examples of this type of information include individual’s names, addresses, races, ages, and can span to extremely sensitive information like the fact that someone is currently expecting a child.⁷ With the newfound ease of collecting and transferring personal information, businesses have been able to collect, analyze, and package this

1. Lothar Determann & Karl T. Guttenberg, *On War and Peace in Cyberspace: Security, Privacy, Jurisdiction*, 41 HASTINGS CONST. L.Q. 875, 891 (2014).

2. *Id.* at 892; Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1033 (2013).

3. One specific significant technological advance is the mobile internet. See generally Michael Kende, *Internet Society Global Internet Report 2015: Mobile Evolution and Development of the Internet*, INTERNET SOCIETY, http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf. Other significant technological advances include the use of the Cloud and the employment of multipoint data processing networks. Hirsch, *supra* note 2, at 1032–33.

4. *Id.* at 1032.

5. *Id.* at 1032–33.

6. *Id.* at 1033.

7. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014), <http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>.

sensitive data to sell to advertisers and other entities as a commodity.⁸ Often, individuals are not even aware that their information is being sold in this capacity.⁹ Additionally, the increased flow of personal data has led to a significant growth in the amount of data breaches that occur, which expose consumers' personal information to untrusted hands.¹⁰ The increased transfer of data around the world has therefore raised significant privacy concerns amongst consumers.¹¹

To address these privacy concerns, a number of jurisdictions promulgated regulations aimed to protect the personal information of their citizens.¹² Despite these efforts, the global nature of the Internet renders jurisdictional-specific legislation both weak and ineffective. Specifically, the fast and unpredictable movement of data transfers "makes it difficult to track and enforce compliance" with legislation of this nature.¹³ Additionally, when issues arise regarding data that has passed through a number of jurisdictions, it becomes extremely difficult to determine which laws apply to that data.¹⁴ This is significant because huge disparities exist between the levels of protection afforded by different regions around the world.¹⁵ The lack of

8. Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014), <http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/>.

9. *Id.*

10. Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law*, 32 COMPUTER & INTERNET LAW., May 2015 (noting that approximately 7 percent of American citizens over the age of fifteen were victims of identity theft in 2012).

11. Hirsch, *supra* note 2, at 1037–38.

12. For a survey of data-privacy laws all over the world, see generally BAKERHOSTETLER, 2015 INTERNATIONAL COMPENDIUM OF DATA PRIVACY LAWS (2014), <http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf>.

13. Hirsch, *supra* note 2, at 1029.

14. *See generally id.*

15. For example, there is current debate about what laws have jurisdiction over emails within a Microsoft server in Ireland. *Microsoft 'Must Release' Data Held on Dublin Server*, BBC NEWS (Apr. 29, 2014), <http://www.bbc.com/news/technology-27191500> Ireland, being a member of the EU, is subject to extensive laws protecting personal data, far surpassing the protection U.S. law provides. *Id.* In September 2015, oral arguments were heard at the Court of Appeals for the Second Circuit, where the Department of Justice argued that the U.S. government can "demand emails from anyone in the world from any email provider headquartered in within US borders . . .

uniform standards for data privacy creates uncertainty amongst individuals as to what protections they are guaranteed, which inevitably creates apprehension toward using the services of foreign companies.¹⁶ Furthermore, companies' efforts to comply with the disparate legal requirements of different nations are costly and ultimately lead companies to pass the costs onto consumers through increased prices of goods and services.¹⁷

In the past, an awareness of the problems associated with diverging data-privacy law has led to cooperative endeavors between individual governments. One recent example is the efforts made by the EU and U.S. governments to provide a legal mechanism allowing for the free flow of personal data between the two regions.¹⁸ Due to the fact that the EU has much stricter data-privacy requirements than the United States, U.S. companies face high costs in the implementation of data-privacy practices that are considered legal under the EU regime.¹⁹ In order to mitigate these costs, both governments entered into an agreement in July 2000 that created the U.S.-EU Safe Harbor program (the "Safe Harbor"),²⁰ which allowed U.S. companies to legally transfer personal data from the EU to the United States for fifteen years.²¹ On October 6, 2015, however, the European Court of Justice (ECJ) rendered the Safe Harbor inva-

." Sam Thielman, *Microsoft Case: DOJ Says It Can Demand Every Email From Any US-Based Provider*, (Sept. 9, 2015), <http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant>. The oral argument was concluded by both the counsel for Microsoft and one of the three sitting judges calling for Congress to step in and create legislation in this area. *Id.* A ruling has not yet been issued on this case. *Id.*

16. See Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 E.C.R. 117/15; Hirsch, *supra* note 2, at 1037–38.

17. Hirsch, *supra* note 2, at 1037–38.

18. See James M. Assey, Jr. & Demetrios A. Eleftherious, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing and or Troubled Waters?*, 9 COMM'LAW CONSP'CTUS 145, 147 (2001).

19. *Id.*

20. *Id.*

21. Letter from EU Commission to Robert LaRussa, Undersec'y for Int'l Trade of U.S. Dep't of Commerce (July 28, 2000), https://build.export.gov/main/safeharbor/eu/eg_main_018494; Schrems, 2015 E.C.R. 117/15.

lid, leaving U.S. companies anxiously awaiting the fate of their future ability to do business in the EU.²²

Despite the current obstacles in place, the international flow of personal data remains "fundamental to the Internet economy."²³ Consequently, fragmentation of the Internet would cause serious harm to the global economy, limit the freedom of information, harm communications between nations, and lead to a regress in technology, which in turn could lead to increased tensions between nations.²⁴

In trying to formulate a solution to this global problem, it is useful to look at another area of international law created at a moment when international cooperation was crucial in order to allow the global market and economy to operate fluidly. International sales of goods once faced a similar need for cooperation between nations, which resulted in the creation of a private international law that has been hailed as "by far the most thorough example of diplomatic drafting in multi-jurisdictional private law ever."²⁵ This law is the United Nations Convention on Contracts for the International Sale of Goods ("CISG").²⁶

The CISG was created in 1980 for the purpose of providing a uniform set of laws to facilitate international sales of goods.²⁷ The approach taken in drafting the CISG consisted of creating a simplified body of law that could be easily applied by different legal systems.²⁸ The drafting process involved active participation by interested nations, which established a foundation of trust in its overall operation and well thought-out provisions

22. Tom Jowitt, *EU Safe Harbour 2.0 Data Transfer Deal Set For Next Month*, TECHWEEK EUR. (Jan. 15, 2016), <http://www.techweekeurope.co.uk/e-regulation/eu-to-meet-in-february-for-safe-harbour-2-0-data-transfers-183919>.

23. Hirsch, *supra* note 2, at 1030.

24. Determann & Guttenberg *supra* note 1, at 879.

25. Camilla Baasch Andersen, *General Principles of the CISG—Generally Impenetrable?*, in SHARING INTERNATIONAL COMMERCIAL LAW ACROSS NATIONAL BOUNDARIES 13, 14–15 (Camilla B. Andersen & Ulrich G. Schroeter eds., 2008).

26. United Nations Convention on Contracts for the International Sale of Goods, opened for signature Apr. 11, 1980, S. TREATY DOC. NO. 98-9 (1983), 1489 U.N.T.S. 3 (entered into force Jan. 1, 1988) [hereinafter CISG].

27. *Id.* pmbl.

28. See generally Kazuaki Sono, *The Vienna Sales Convention: History and Perspective*, in INTERNATIONAL SALE OF GOODS: DUBROVNIK LECTURES 1, 1–17 (Petar Sarcevic & Paul Volken eds., 1986).

that have held up over the years.²⁹ Since its creation thirty-five years ago, eighty-four states have adopted the CISG.³⁰

In order to alleviate the problems that currently plague the data industry, an international convention on the collection, transfer, and processing of personal data is needed. To both facilitate and ensure its success, drafters should employ the CISG as an example for modeling this new convention. By doing so, drafters can build upon on the strengths and the weaknesses of the CISG, which has generated years of research and analysis.³¹

Part I of this Note will examine the current frameworks for data-privacy law in the EU and the United States, noting the different approaches each region has taken to regulating data privacy. This Part first provides an evaluation of EU law, which includes an assessment of the European Union Data Protection Directive 95/46/EC (“EU Directive”) and the EU’s newest piece of legislation, the General Data Protection Regulation (“GDPR”). It will then analyze U.S. law, by looking first at the statutory framework in the United States. Subsequently, it will then analyze the Federal Trade Commission’s (FTC) role in data-privacy protection and consider additional efforts in the United States to regulate data privacy. Part II will provide an overview of past efforts toward international cooperation on data privacy. It will first look at the Safe Harbor and outline how it came to be, why it no longer exists, and what the next steps are for EU-U.S. data transfers under the newly agreed upon EU-U.S. Privacy Shield (“Privacy Shield”). It will then go on to look at the Organization for Economic Cooperation and Development (OECD) and examine the contributions it has provided to international data-privacy law, specifically looking to the contribution of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines”). This Part will then examine the Global Privacy Enforcement Network (GPEN), looking at why it was created, what its current efforts involve, and what its creation

29. See generally *id.*

30. Albert H. Kritzer, *CISG: Table of Contracting States*, CISG DATABASE, <http://www.cisg.law.pace.edu/cisg/countries/cntries.html> (last updated Jan. 8, 2016).

31. Pace Law School provides a database dedicated to scholarly material on the CISG. See CISG DATABASE, <http://www.cisg.law.pace.edu> (last updated Jan. 29, 2016).

means for the future of international data-security. Finally, Part III will analyze the CISG and use its framework as a model to propose an international convention on data privacy. This analysis includes a comparison between the current state of data privacy to the state of international trade when the CISG was created. It will also expose the major weaknesses of the CISG and how a new convention on data privacy can ameliorate the weaknesses that promulgated from the implementation of the CISG. Additionally, it will examine the differences between these two areas of law and how the CISG model can be modified to fit the needs of an international data-privacy convention.

I. CURRENT DATA-PRIVACY LAWS

Privacy law is grounded in the protection of personal information.³² More specifically, “[p]rivacy laws regulate various aspects of the collection, use, processing, storage and disclosure” of personal information that relates to identifiable individuals.³³ Two regions that have taken very different approaches to personal data privacy are the EU and the United States. Despite their many differences, these regions’ economies are dependent on one another, as they have the most substantial relationship in both trade and investment in the world.³⁴ Furthermore, despite their different approaches to data privacy, the highest rate of cross-border data exchange occurs between these two regions.³⁵ As a result, both the EU and United States have made a notable effort to cooperate with each other, which continues to evolve over time.

A. The EU

The EU provides the most extensive set of laws governing data privacy in the world.³⁶ The EU’s data-privacy legislation is

32. Brian M. Gaff et al., *Privacy and Data Security*, COMPUTING & LAW, Mar. 2012, at 9, <http://www.edwardswildman.com/files/upload/March%202012.pdf>.

33. *Id.*

34. Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for the U.S. and EU Trade and Investment* 1 (Global Econ. & Dev., Working Paper 79, 2014).

35. *Id.*

36. Publisher’s Editorial Staff, *International Privacy Issues*, 23 No. 3 INT’L HR J. art. 4, 1 (2014) [hereinafter *International Privacy Issues*].

important precedent for purposes of this Note because it recognizes and aims to address the problem of a lack of uniformity in data-privacy law among multiple distinct nations within its own borders. Thus, illustrating the global issues that stem from diverging data-privacy legislation on a micro level and demonstrating a possible solution that if applied more broadly can alleviate these issues on a global level.³⁷ The EU has been proactive about both establishing and improving laws to create a cohesive uniform body of law to protect the personal data of its citizens.³⁸ This will be illustrated by first looking at the original piece of data-privacy legislation that the EU established, the EU Directive, and by reviewing the newly adopted General Data Protection Regulation and its attempts to improve the EU Directive.

1. The EU Directive

The right to privacy has long been recognized as a fundamental right within the EU.³⁹ In order to protect this right, the EU recognized the need to harmonize data-privacy laws and thereby remove barriers to the free flow of data that derived from differing legislation of its member countries.⁴⁰ In order to facilitate this harmonization, the EU Directive imposes mandatory standards for the collection, processing, and transfer of personal data throughout the EU.⁴¹ In October 1995, the EU presented its first piece of legislation on data-privacy protection, the EU Directive.⁴² The EU Directive provides two main objectives: (1) that personal data privacy be treated and protected as a

37. This Note will not provide a comprehensive overview of every law affecting data privacy in each region of the world. There are countless laws in each country that in some way or form relate to data privacy. Rather, this Note focuses on the most significant sources of authority on data-privacy law in order to demonstrate the general policy approaches each region has taken on data privacy.

38. See generally Council Directive 95/46, 1995 O.J. (L 281) 31–39 (EC).

39. The right to privacy is viewed as such under “Article 8 of the European Convention for the Protection of Humans Rights and Fundamental Freedoms and in the general principles of Community law.” *Id.* at pmbl.

40. Omer Tene, *Privacy Law’s Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L. J. 1217, 1222 (2013).

41. See generally Council Directive 95/46, *supra* note 38.

42. *Id.*

fundamental right⁴³ and (2) to prevent the restriction of the free flow of data across the borders of member states.⁴⁴

The EU Directive intended to articulate a set of bare-minimum standards that each Member State must provide for its citizens, while bestowing them with flexibility in how they may implement these standards.⁴⁵ The EU Directive instructed each Member State to enact their own legislation based on its enumerated requirements.⁴⁶ Therefore, the EU Directive allowed each Member State to enact legislation that could provide for even stricter data-privacy protection than that which is provided for by the EU Directive.⁴⁷ In order to promote uniformity, the EU Directive provides definitions of key data-privacy terms in attempts to ensure no contradictions arise in the laws of each Member State.⁴⁸

The EU Directive imposes strict conditions on the collection of personal data.⁴⁹ Data may only be collected for specific, legitimate, and explicit purposes.⁵⁰ Furthermore, personal data that is collected must be “adequate, relevant and not excessive” for such purposes.⁵¹ Additionally, each Member State is responsible for ensuring the collected personal data is current and accurate, as well as maintained in a form that can identify data subjects for a period of time that is no longer than necessary.⁵² When personal data is stored for long periods of time, there must be proper safeguards put in place to protect this data.⁵³ Additionally, when an individual’s personal data is collected, they must be afforded with information regarding the collec-

43. *Id.* art. 1.1.

44. *Id.* art. 1.2.

45. INT’L TELECOMM. UNION, Stephanie Liston, *Introduction to The Cloud: Data Protection and Privacy—Whose Cloud is it Anyway?* 1, 10, (Int’l Telecomm. Union, GSR Working Paper 2012), https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Privacy_Liston_6.pdf.

46. Council Directive 95/46, *supra* note 38, pmbl.

47. *See id.*

48. For example, EU Directive defines “personal data” as any information that relates to an identifiable or identified natural person. *See id.* art. 2.

49. *Id.* art. 6.

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

tion.⁵⁴ At a minimum, this must include the identity of the individual or entity determining the use and means of the data,⁵⁵ the intended purpose of the collection,⁵⁶ and any other information that would “guarantee fair processing” to the data subject.⁵⁷

The EU Directive also imposes strict conditions on the processing of personal data.⁵⁸ Before data can undergo any type of processing, the data subject’s consent must be obtained.⁵⁹ Even with consent, the ability to process personal data is limited to circumstances where the processing is necessary to further a legitimate purpose.⁶⁰ All Member States are required to implement safeguards that will protect personal data from being unlawfully disclosed, altered, destructed, or lost.⁶¹ To provide some flexibility in this provision’s enforcement, the drafters did not mandate that a specific system be followed in establishing safeguards. Instead, the drafters required that all Member States provide security that is “appropriate to the risks represented by the processing” and provide “sufficient guarantees” of protection.⁶²

Under the EU Directive, individuals are given a voice in establishing the safeguards of their personal information. Individuals are guaranteed the right to obtain information pertaining to who is using their personal data and how it is being used.⁶³ The EU Directive further allows individuals to object to the processing of their personal data based on “compelling legitimate grounds,” at any time.⁶⁴ When these objections are

54. *Id.* art. 10.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.* art 7. “Processing” is defined as “any operation or set of operations which is performed upon personal data” *Id.* art 2.

59. *Id.*

60. A list of legitimate purposes are provided by Article 7 including: performing or taking steps to perform a contract to which the data subject is a party; complying with legal obligations; protecting the “vital interests of the data subject”; performing tasks of public interest or official authority, and “for the purposes of legitimate interests . . . except when such interests are overridden by the interests for fundamental rights and freedoms of the data subject” *Id.* art. 7.

61. *Id.* art. 17.

62. *Id.*

63. *Id.* art. 12.

64. *Id.* art. 14.

justified, the processing will be discontinued.⁶⁵ Individuals can also request to have their personal data deleted as soon as its retention is no longer necessary.⁶⁶

In order to uphold the objectives of the EU Directive, each Member State is required to establish at least one data-protection authority ("DPA").⁶⁷ These DPAs "shall act with complete independence in exercising the functions entrusted to them" from any other governmental influence.⁶⁸ The EU Directive also provides a list of specific powers the DPAs must possess in order to ensure they can adequately uphold the laws.⁶⁹ The DPAs are required to "cooperate with one another to the extent necessary for performance of their duties."⁷⁰ This requirement has successfully created a network of regulators that have "become a center of knowledge and core for a community of professionals devoted to data protection."⁷¹

65. *Id.*

66. *Id.* art. 12.

67. Tene, *supra* note 40, at 1223.

68. Council Directive 95/46, *supra* note 38, art. 28; *see also* Steve Peers, *The CJEU Confirms the Independence of Data Protection Authorities Developments*, EU L. ANALYSIS (Apr. 9, 2014), <http://eulawanalysis.blogspot.co.uk/2014/04/the-cjeu-confirms-independence-of-data.html>.

69. The EU Directive requires that the DPAs be afforded with both investigative powers and collective powers, allowing them to access information for performing their duties. Council Directive 95/46, *supra* note 38, art. 28. It further requires the DPAs be afforded with the powers of intervention, which include the power to deliver opinions prior to data processing operations taking place, the ability to order data controllers to block, erase, or destruct data, and the ability to place bans on their processing of data altogether. *Id.* Furthermore, under the EU Directive, each DPA must be afforded with "the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities." *Id.* In addition to these powers, when EU citizens object to the use of their personal data, they will bring such claims before these authorities. *Id.* Once the DPAs issue decisions, they can be appealed through the local courts. *Id.* Additionally, the DPAs are also posed with the duty to issue regular reports to inform the public of recent activities. *Id.* The EU Directive requires Member States provide for DPA members and staff to maintain confidentiality regarding the information accessed through the position both during the operation and after leaving their positions. *Id.*

70. *Id.*

71. Tene, *supra* note 40, at 1223. For a list of all of the DPAs in the EU, *see* List of Data Protection Bodies by Country, EURO. COMM'N,

The EU Directive also established the Article 29 Working Party (“Working Party”) to act independently in advising the Member States on how to apply the directive.⁷² Since the EU Directive’s enactment, the Working Party has become “a very important platform for cooperation.”⁷³ The Working Party has become such a platform by providing expert advice on data protection issues, promoting uniform application of the EU Directive, and advising the European Commission (EC) on how EU laws are affecting the right to personal-data privacy.⁷⁴

In creating the EU Directive, drafters emphasized the importance of the free flow of data throughout the twenty-eight Member States, believing it to be essential to the efficiency of the EU’s internal market.⁷⁵ To facilitate the free flow of data, no Member State may “inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy.”⁷⁶ The rationalization behind this limitation is that there should be no need for such protections when the EU Directive is meant to provide “equivalent protection” throughout all of the Member States.⁷⁷

While most of its provisions focus on how data is handled within the EU, the EU Directive also provides restrictions on the transfer of data to countries outside the EU.⁷⁸ Personal data may only be transferred from within the EU to non-EU countries if such countries can ensure an “adequate level of protection.”⁷⁹ Whether a country’s protection is adequate will be assessed based on “all the circumstances surrounding a data transfer.”⁸⁰ Important factors to consider include the nature of the data, the purpose of the transfer, the duration of pro-

http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm (last updated Feb. 11, 2016).

72. Council Directive 95/46, *supra* note 38, art. 29.

73. *Article 29 Working Party*, EUROPEAN DATA PROTECTION SUPERVISOR, <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Art29> (last visited Dec. 22, 2015).

74. *Id.*

75. Council Directive 95/46, *supra* note 38, pmbl.

76. *Id.*

77. *Id.*

78. *Id.* art. 25.

79. *Id.*

80. *Id.*

cessing, the countries involved, the rules of laws involved, and the security measures the non-EU country complies with.⁸¹

Although this restriction was one of the most controversial aspects of the EU Directive, EU regulators felt it was essential in ensuring the effectiveness of the EU Directive.⁸² Without such a restriction, "the very rights created under the Directive could be systematically violated."⁸³ Had such a restriction not been incorporated, organizations could freely remove data from the borders of the EU to process it in locations that are not subject to the EU Directive, thereby circumventing its requirements and removing the rights and protections it affords.⁸⁴ Nonetheless, U.S.-based multinational and e-commerce organizations objected to this restriction out of fear that in the event that U.S. data-privacy law was found to be inadequate, it would create a barrier inhibiting the flow of data from the EU to U.S. businesses.⁸⁵

Despite the many attributes of the EU Directive, the level of flexibility it permitted in implementing national legislation led to differing and, at times, even conflicting regimes throughout the EU.⁸⁶ In some cases, these disparities are attributable to certain Member States failing to implement the EU Directive properly.⁸⁷ In other cases, the different policy choices each Member State made when creating their own legislation led to the creation of very different and inconsistent laws.⁸⁸ The resulting inconsistencies have created unnecessary costs and diminished the overall effectiveness of the EU Directive.⁸⁹ Despite years of effort, these issues have not been remedied.⁹⁰

81. *Id.*

82. Assey & Eleftherious, *supra* note 18, at 146.

83. *Id.*

84. *Id.*

85. *Id.*

86. Tene, *supra* note 40, at 1224.

87. Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* 24–25, EUR. DATA PROTECTION SUPERVISOR (Sept. 15, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf.

88. *Id.* at 26–27.

89. *Id.*

90. *Id.*

2. The General Data Protection Regulation

As technology evolves, the EU continues to update data-privacy laws to ensure adequate protection for its citizens.⁹¹ In January 2012, the EC adopted the proposal of a new regulation to replace the EU Directive—the GDPR.⁹² The GDPR would function as a “comprehensive reform of the EU’s 1995 data protection rules to strengthen online privacy rights and boost Europe’s digital economy.”⁹³ After extensive negotiations, the

91. One effort involved the passing of the Directive on Privacy and Electronic Communication, which took the principles from the EU Directive and created specific rules for the telecommunications sector. Council Directive 97/66, 1997 O.J. (L 024) 0001 (EC). In 2002, this Directive was replaced by the Directive on Privacy and Electronic Communication (“ePrivacy Directive”). Council Directive 2002/58, 2002 O.J. (L 201) 0037 (EC) at pmb1. The e-Privacy Directive updated the rules promulgated by Directive 97/66 to comport with new developments in technology. *Id.* The e-Privacy Directive directs Member States to produce national legislation that requires communications made over public networks be kept confidential and obliges all providers of telecommunications services to implement adequate security to protect users’ personal data. *Id.* The e-Privacy Directive specifically deals with two new areas of concern that grew out of growing patterns of the Internet: Spam mail and the use of cookies. *See id.* (“So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users.”). Another significant development to the EU’s data-privacy regime is the creation of the “Right to be Forgotten” by the Court of Justice of the European Union in 2014, which affords EU citizens the right to instruct search engines to remove links containing their personal information where it is “inaccurate, inadequate, irrelevant, or excessive for the purposes of the data processing” Eur. Comm’n, *Factsheet on the “Right to be Forgotten: Ruling (C-131/12)*, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited Mar. 8, 2016).

92. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012).

93. *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users’ Control of Their Data and to Cut Costs for Businesses*, EUROPEAN COMM’N (Jan. 25 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

GDPR was adopted on April 14, 2016,⁹⁴ and will go into effect in early 2018.⁹⁵

The GDPR makes some key changes to the current law of the EU.⁹⁶ One significant change is that an entirely different legal instrument—a regulation, rather than a directive—will be used to govern data in the EU.⁹⁷ As is the nature of directives, the EU Directive served merely as a framework and minimum standard for countries to use when drafting their own laws.⁹⁸ Acknowledging the inconsistencies that resulted from Member States' implementation of the EU Directive, the Council of the EU expressed the need to reform EU data-privacy legislation in order to more effectively meet the goals set out by the EU Directive:

The objectives and principles of [the EU Directive] remain sound, but it has not prevented fragmentation in the way data protection is implemented across the [EU], legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the [EU]. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the [EU], distort competition and impede authorities in the discharge of their responsibilities under [EU] law. This difference in levels of protection is due to the existence of differences in the implementation and application of [the EU Directive].⁹⁹

94. Press Release, Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection, EUR. COMM'N, (Apr. 14, 2016) http://europea.eu/rapid.press-release_STATEMENT-16-1403_en/htm.

95. *Id.*

96. See generally Andy Green, *The EU General Data Protection Regulation Is Now Law. Here's What You Need to Know*, INSIDE OUT SECURITY BLOG (Jan. 15, 2016), <http://blog.varonis.com/the-eu-general-data-protection-regulation-is-now-law-heres-what-you-need-to-know/>.

97. *Id.*

98. Dan Svantesson, *The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 68 (2014).

99. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal*

In order to ameliorate the inconsistencies amongst different national laws that resulted from Member States implementing the EU Directive in their own way, the GDPR will automatically bind all EU-Member States to its specific requirements once enacted.¹⁰⁰

Another major change is the fact that the GDPR explicitly encompasses personal data that is handled outside the EU. The GDPR asserts authority over companies who offer their services to EU citizens and play an active role in the EU market.¹⁰¹ Although the EU Directive also had an extraterritorial effect, it had never explicitly identified its jurisdiction as extending beyond the EU.¹⁰² Instead, it banned EU members from conducting business with non-EU members who did not provide an adequate level of protection, which in turn encompassed entities beyond the EU's borders.¹⁰³ This change emphasizes the fact that the EU will not allow its citizens' personal information to be afforded with anything less than the rights the EU provides.

This reform demonstrates the willingness of the EU to continue to improve its laws in order to ensure privacy protection for EU members.¹⁰⁴ Despite the presence of protective legislation, the need for such an improvement also demonstrates the persistence of data-privacy concerns when there is a lack of uniformity in the law.

B. United States

The U.S. approach to data privacy is vastly different from the extensive framework found in the EU. The United States has taken a sectoral approach to data privacy.¹⁰⁵ The U.S. approach delegates the majority of data-privacy protection to self-

Data and on the Free Movement of Such Data (General Data Protection Regulation) – Preparation of a General Approach, 9565/15 (June 11, 2015).

100. *Id.*

101. *Id.*

102. See Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1120–21 (2013).

103. *Id.*

104. See European Commission Memo MEMO/14/186, *Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote* (Mar. 12, 2014).

105. Ryan Moshell, Comment, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 372 (2005).

regulation by individual industries. Legislation only steps in to fix narrowly tailored issues within specific industries.¹⁰⁶ This hands-off approach juxtaposes the EU's approach of enacting broad-sweeping legislation that aims to counter all data-privacy issues in all industries.¹⁰⁷ Some scholars have attributed the United States' lack of legislation in this area to the fact that privacy rights were not written directly into the U.S. Constitution.¹⁰⁸ Whereas, in the EU, privacy is expressly provided as an individual's right within the EU's constitution.¹⁰⁹ In the United States, privacy rights were eventually read in through the courts' interpretation of the Bill of Rights, resulting in piecemeal privacy rights for U.S. citizens.¹¹⁰

1. Statutory Framework of the United States

In the United States, there is no single federal law that governs the protection of all sensitive data.¹¹¹ The U.S. legislature has shown a general reluctance toward enacting broad protections for data privacy.¹¹² Instead, there is a fragmentation of

106. *Id.*

107. *Id.*

108. *Id.*

109. Charter of Fundamental Rights of the European Union, art. 7, Dec. 18, 2000, 2000 O.J. (C 364) 1.

110. Moshell, *supra* note 105, at 372. The Fourth Amendment grants "[t]he right of the people to be secure in their persons, houses, paper, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Courts have shown a general reluctance toward using this protection over data that is provided to a third party. *See United States v. Miller*, 425 U.S. 435, 433 (1976) ("The Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"). These privacy rights have only been enforced against the government and only in cases where an individual had a "reasonable expectation of privacy." Alo, *supra* note 102, at 1101.

111. GINA STEVENS, CONG. RESEARCH SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 1 (2010).

112. For example, in *U.S. v. Miller*, the Supreme Court held that a bank customer was not protected by the Fourth Amendment after his personal information was given to a government agency because he assumed the risk of disclosure. 425 U.S. 435, 442 (1976). The Legislature reacted to the decision by enacting the Right to Financial Privacy Act. 12 U.S.C. §§ 3401–3422 (2015). The Act restricts financial institutions in handing over their customer's information to government agencies. *Id.* § 3402. The law is tailored to-

statutes, which provide limited, sector-specific protections to personal data.¹¹³ As a result, there is more than one definition of “personally identifiable information” found in U.S. law.¹¹⁴ In order to determine which laws govern an entity’s data-security practices, one must look at what sector the entity belongs to and the type of data the entity collects.¹¹⁵

In addition to federal laws, there are state laws that affect data privacy. One significant form of state law is data-breach notification statutes, which can be found in the majority of states.¹¹⁶ Generally, these statutes require companies to notify consumers when their personal data becomes compromised due to a data breach.¹¹⁷ Such “breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensi-

ward a specific issue in a specific industry, thus avoiding the unresolved issue of data privacy that is generally left open by *Miller*. Moshell *supra* note 105, at 373.

113. Alo, *supra* note 102, at 1103. Examples of these sector-specific laws include the Gramm Leach Bliley Financial Modernization Act, Pub. L. No. 106-012, 113 Stat. 1338 (1999) (regulating data processing within the financial industry); Fair Credit Reporting Act, 15 U.S.C. §1681 (1994 & Supp. 1998) (regulating data relating to employment and credit reporting agencies); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat. 1936 (1996) (regulating data collection in the health care industry). Another law that is narrowly applicable to a specific set of individuals is the Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506, which regulates the collection and use of children’s information by websites. COPPA applies to an “operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child.” *Id.*

114. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 879 (2014).

115. STEVENS, *supra* note 111, at 1.

116. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted such laws. *Security Breach Notification Laws*, NAT’L CONFERENCE OF ST. LEGISLATURES (June 11, 2015), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

117. *Id.* Each law at least addresses how it defines “personal information” and “security breach,” who must be notified after a data breach occurs, how individuals must be notified, what information must be included within the notification, timing requirements for notification, and the penalties for failing to satisfy the requirements. Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN’S L. REV. 1569, 1577 (2010).

tive personal information that results in the potential compromise of the confidentiality or integrity of data.”¹¹⁸

Because these notification laws are enacted by each state individually, each statute has different requirements.¹¹⁹ This creates difficulties for businesses that operate across state borders, as they need to know which citizens must be notified under varying circumstances, and must constantly keep up with the amendments to each statute.¹²⁰ Scholars often argue for a federal security breach notification law as a means to fix this problem.¹²¹ However, although a number of bills have been proposed to create a federal data breach law, none have been enacted.¹²²

In the past few years, despite the force of the state notification laws, an alarming amount of data breaches have taken place within the United States.¹²³ An analysis of the costs associated with data breaches throughout the world revealed that American businesses faced the highest average total cost of data breaches compared to companies of any other country, averaging at \$6.53 million in 2015.¹²⁴

2. The FTC

The Federal Trade Commission Act was created on September 26, 1914, establishing the FTC as a U.S. agency with the

118. STEVENS, *supra* note 111, at 1.

119. Tom, *supra* note 117, at 1570 (“Variations are so numerous that it is virtually impossible to convert these state laws into the more manageable format of fifty-state surveys.”).

120. See STEVENS, *supra* note 111, at 2.

121. *Id.* See generally Tom, *supra* note 117, at 1574.

122. Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Breach Notification Act of 2011, S. 1408, 112th Cong. (2011); Data Security Act of 2011, S. 1434, 112th Cong. (2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011); Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Cong. (2011); Secure and Fortify Electronic Data Act, H.R. 2577, 112th Cong. (2011). The most recent attempt to create a federal data breach law was introduced in the Senate on January 13, 2015, where it was read twice and referred to the Committee on Commerce, Science, and Transportation. Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015).

123. Russo, *supra* note 10, at 201.

124. Ponemon Inst., *2015 Cost of Data Breach Study: Global Analysis 7* (May 2015), <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>.

mission of protecting consumers and promoting competition.¹²⁵ Under Section 5 of the Federal Trade Commission Act (“Section 5”), the FTC has the power to protect consumers against “unfair or deceptive acts or practices in or affecting commerce.”¹²⁶

To combat the harm associated with data breaches, the FTC has taken the role of enforcing more secure data-protection practices amongst U.S. businesses.¹²⁷ It was not until 1995, when the FTC’s involvement with consumer privacy issues began.¹²⁸ At that time, the FTC promoted the idea of industries self-regulating data protection.¹²⁹ After realizing this was an ineffective method, however, the FTC reported to Congress that self-regulation was inadequate and began bringing its own enforcement actions to strengthen data-security practices.

The FTC first started using its Section 5 authority through the “deceptive acts” prong of the statute, by taking action against businesses that violated their own policies, deeming such violations to be deceptive practices.¹³⁰ Since 2002, the FTC has used the unfairness prong to bring actions against companies who use unfair practices relating to data security, assessing such practices on a case-by-case basis.¹³¹

As a result of the international nature of the Internet, the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (SAFE WEB Act) was passed to amend the FTC Act to provide the FTC with the au-

125. *Our History*, FED. TRADE COMM’N, <https://www.ftc.gov/about-ftc/our-history> (last visited Feb. 14, 2016).

126. 15 U.S.C.A. § 45(a) (West 2006).

127. Russo, *supra* note 10, at 201.

128. GINA STEVENS, CONG. RESEARCH SERV., R43723, FEDERAL TRADE COMMISSION’S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACT OR PRACTICES (UDAP) AUTHORITY pmbl. (2014).

129. *Id.*

130. STEVENS, *supra* note 111, pmbl.

131. Russo, *supra* note 10, at 201. In order to prove business practices are unfair, the FTC must show that these practices “cause substantial injury to consumers which is not reasonably avoidable by consumers themselves” and that this harm is not “outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C.A. § 45(n) (West 2006). Whether consumers could have avoided the injury depends on whether the consumers’ choice was fully informed and free. *F.T.C. v. Neovi, Inc.*, 604 F. 3d 1150, 1158 (9th Cir. 2010). Businesses can also be found in violation of the Act in cases where they do not directly cause harm to consumers but their practices “facilitate or contribute to” such harm. *Id.* at 1157. Under these circumstances, the FTC must prove that the injury was foreseeable. *Id.* at 1156–58.

thority needed to protect consumers against “cross-border fraud and deception, and particularly to fight spam, spyware, and Internet fraud and deception.”¹³² In addition to providing the FTC with authority to work with foreign governments on these matters,¹³³ the act amends the definition of “unfair or deceptive acts or practices” to include “acts or practices involving foreign commerce that: “(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States.”¹³⁴

In addition to bringing enforcement actions, the FTC has made a continuing effort to educate businesses on acceptable data-protection practices.¹³⁵ In March 2012, the FTC released a report¹³⁶ addressing “privacy challenges associated with the new technological and business landscape.”¹³⁷ The report establishes the best practices for businesses to protect the privacy of American consumers and give them “greater control over the collection and use of their personal data.”¹³⁸ The FTC explored new privacy issues that have arisen due to growths in technology and business developments, looking to public opinion to help shape the report.¹³⁹ The report goes on to propose three pieces of legislation to Congress: a general privacy statute, a data broker statute, and a federal data security and breach notification law.¹⁴⁰

Additionally, the FTC publishes all of its enforcement actions and issues press releases, which allow businesses to view what the FTC considers unacceptable data-security practices.¹⁴¹

132. Pub. L. No. 109-455, codified to the FTC Act, 15 U.S.C. §§ 41 et seq.

133. *See generally id.* at §§ 4–6.

134. *Id.* § 3.

135. *See* FED. TRADE COMM’N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011) [hereinafter 2011 REPORT], https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (iterating the “best practices” for businesses to use when collecting personal data, as well as providing general principles for creating strong data-security plans).

136. FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 1 (2012) [hereinafter 2012 REPORT].

137. Tene, *supra* note 40, at 1234–35.

138. 2012 REPORT, *supra* note 136, at i.

139. Tene, *supra* note 40, at 1234–35.

140. *See generally* 2012 REPORT, *supra* note 136.

141. *Enforcing Privacy Promises*, FED. TRADE COMM’N, <https://www.ftc.gov/news-events/media-resources/protecting-consumer->

Nonetheless, the FTC itself has acknowledged its inability to require businesses to adopt a set of privacy practices.¹⁴² Therefore, this guidance is only useful if companies voluntarily implement security standards in accordance with these recommendations. Recently, however, the significance of these recommendations was emphasized by the Third Circuit.

In August 2015, the Third Circuit issued an opinion in *FTC v. Wyndham Worldwide Corp.*, where the FTC's authority over data-security practices was challenged.¹⁴³ The FTC filed suit against the hotel, alleging that the hotel's conduct constituted an unfair practice, after data hackers stole personal and financial information from Wyndham's customers and consequently accumulated \$10.6 million in fraudulent charges.¹⁴⁴ Additionally, the FTC alleged that Wyndham's privacy policy was deceptive because it overstated the cybersecurity practices the hotel had in place.¹⁴⁵ Wyndham moved to dismiss the case, arguing that the FTC exceeded its statutory authority by asserting unfairness in the context of data security. Although the FTC has been using Section 5 to bring such actions for over a decade, Congress had never explicitly delegated it with the specific authority to regulate data security.¹⁴⁶ Instead, the FTC simply started applying its broad Section 5 authority to govern the area.¹⁴⁷ Until recently, most of the FTC's data-security cases have been settled or abandoned, leaving little judicial guidance regarding the FTC's power to regulate data-security practices.¹⁴⁸ With the issuance of this decision, the Third Circuit affirmed the FTC's ability to "regulate cybersecurity using the unfairness prong" of Section 5,¹⁴⁹ affirmatively setting in motion what seems to be a major shift in the U.S. policy on data security.

Although this case provides a significant step forward in establishing a policy in favor of stronger data-privacy protection,

privacy/enforcing-privacy-promises (last visited Mar. 10, 2016); *Cases and Proceedings*, FED. TRADE COMM'N, <https://www.ftc.gov/enforcement/cases-proceedings> (last visited Mar. 8, 2016).

142. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

143. *Id.*

144. *Id.* at 240.

145. *Id.* at 241.

146. STEVENS, *supra* note 130, at 2, 4.

147. *Id.* at 4.

148. *Id.* at 7.

149. *Wyndham*, 799 F.3d at 248.

it highlights the lack of clarity that still exists in this area of the law. The Court itself “acknowledge[d] there will be borderline cases where it is unclear if a particular company’s conduct falls below the requisite legal threshold.”¹⁵⁰ The Court also went on to suggest that, although not required by law, companies should look to the recommendations the FTC has issued as a means to achieve privacy standards that would not violate the statute.¹⁵¹ However, these recommendations remain solely recommendations and therefore are not useful unless every business voluntarily complies with them in setting up their own data-security practices.¹⁵²

Since the FTC cannot require companies to adopt safe data-security standards, its ability to regulate this area is limited to enforcing policies that companies have already adopted.¹⁵³ Therefore, it can only address major deficiencies in protection once individuals’ personal information has been threatened. Furthermore, the FTC is limited in what individuals it can protect and what entities it can take action against. Its authority only allows for the protection of consumers, and such protection does not extend over various sectors that are governed by other statutes.¹⁵⁴ Additionally, the FTC deals with a broader scope of

150. *Id.* at 256. The Court explained that this standard is sufficient because it alerts parties that they need to apply a cost-benefit analysis, which “considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.” *Id.* at 255–56.

151. *Id.* at 257–59.

152. *See* Alo, *supra* note 102, at 1103. The FTC has taken a variety of steps to try and educate businesses on acceptable data protection practices. In 2011, it issued a report which iterates the “best practices” for businesses to use when collecting personal data, and provides general principles for creating a strong data security plan. 2011 REPORT, *supra* note 135. It has also issued a statement to outline its approach to data security, establishing its standard of assessment as “reasonableness.” *See generally* Fed. Trade Comm’n, *Commission Statement Marking the FTC’s 50th Data Security*, FTC.GOV (Jan. 31, 2014), <http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

153. Alo, *supra* note 102, at 1103.

154. Tene, *supra* note 40, at 1225. Section 5 of the Federal Trade Act, 15 U.S.C. § 45(a)(2) (2015), does not grant the FTC with authority over “financial institutions (which are subject to the jurisdiction of the Federal Reserve Board); common carriers (subject to the Federal Communications Commis-

issues than just data privacy. Therefore, data-privacy concerns are competing for the FTC's attention against other prevalent issues affecting commerce.¹⁵⁵

3. Additional U.S. Data-Privacy Efforts

In addition to the FTC's promotion of a stronger data-privacy policy, other branches of government are stepping forward and calling for national legislation. In February 2012, the Obama administration released a White House Report¹⁵⁶ recommending Congress enact legislation to protect the privacy of consumers.¹⁵⁷ The report also proposes that the United States put effort toward improving cooperation with the international community in the realm of data privacy.¹⁵⁸ Acknowledging the timeliness for such a change, President Obama asserts,

even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.¹⁵⁹

Additionally, the Department of Commerce (DOC) has recently called for stronger privacy legislation. After two years of conducting public workshops and research on how to provide for the protection of consumer privacy in a manner that would promote innovation, the DOC issued its final "White Paper" on February 23, 2012. The White Paper recommends Congress enact a Consumer Privacy Bill of Rights.¹⁶⁰

In addition to these proposals, the U.S. private sector has been noticeably proactive in trying to enhance the industry standards for data-privacy practices.¹⁶¹ Companies such as Fa-

sion); air carriers; insurance companies; and non-profit organizations." Tene *supra* note 40, at 1225 n. 29.

155. *See id.*

156. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 32 n.39 (2012) [hereinafter WHITE HOUSE REPORT], <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

157. *Id.*

158. *Id.*

159. WHITE HOUSE REPORT, *supra* note 156.

160. 2012 REPORT, *supra* note 136, at 3.

161. *Id.* at 7.

cebook and Google have enhanced their practices to protect users' passwords from being stolen.¹⁶² Additionally, tools have been created to afford users with enhanced privacy, such as the HTTPS Everywhere browser add-on, as well as other tools that allow users to encrypt their information.¹⁶³ Furthermore, after the FTC's preliminary report called for the industry to create "a mechanism to allow consumers to control the collection and use of their online browsing data," Do-Not-Track ("DNT") technology¹⁶⁴ has been created and widely adopted throughout the private sector.¹⁶⁵ Data-privacy proponents "argue consumers should be allowed to submit 'Do Not Track' requests to tell a website not to collect information about their online browsing habits."¹⁶⁶ Despite the noticeable improvement in the private sector's perspective on consumer privacy protection, complying with these requests remains completely voluntary.¹⁶⁷

Efforts have been made to pass legislation to require online services to honor users' DNT requests, however, to date, none have been enacted.¹⁶⁸ Attempts have also been made to bring DNT technology under the authority of the Federal Communications Committee (FCC).¹⁶⁹ However, by dismissing a petition requesting the FCC initiate a rulemaking proceeding to force companies to honor these DNT requests, the FCC rejected the opportunity to provide any standard to apply to DNT technology.¹⁷⁰ Therefore, no legal obligation currently exists requiring websites to honor DNT requests, further signifying the need for

162. *Id.*

163. *Id.*

164. DNT is a technology that enables users to opt-out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. *Overview*, DO NOT TRACK, <http://donottrack.us> (last visited Dec. 22, 2015). DNT signals a user's opt-out preference with an HTTP header, a simple technology that is completely compatible with the existing web. *Id.* Generally, they are in the preferences section of your web browser. *Id.* However, not all websites honor these signals. *Id.*

165. *Id.*

166. Dustin Volz, *U.S. Regulators Reject Push For "Do Not Track" Internet Rules*, REUTERS (Nov. 6, 2015), <http://www.reuters.com/article/usa-tech-tracking-idUSL1N1311XW20151106#FDfeJz1gIPLCp972.99>.

167. *Id.*

168. Do-Not-Track Online Act, S. 913 112th Cong. (2011).

169. Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor 'Do Not Track' Requests, 30 F.C.C.R. 12424 (Nov. 6, 2015).

170. *Id.*

a legal instrument to force companies to comply with such practices.

Despite these setbacks, DNT has not been completely ignored by the law. California has been at the forefront of privacy protection for years, stemming back to the 1970s, when “[v]oters amended the state constitution . . . to provide explicit privacy rights far more robust than those guaranteed by the Fourth Amendment.”¹⁷¹ As a result, California has been a trailblazer for enacting data-privacy legislation.¹⁷² On September 27, 2013, California enacted a progressive piece of legislation governing disclosure requirements with regard to DNT signals.¹⁷³ Although the law does not compel companies to adopt the practice of abiding by user’s DNT requests, it forces them to disclose such fact so users are aware their requests are being ignored while using the company’s website.¹⁷⁴

On October 8, 2015—notably two days following the invalidation of the Safe Harbor—the Electronic Communications Privacy Act was enacted in California and has since been hailed as landmark legislation.¹⁷⁵ The statute will prohibit government entities from compelling businesses to provide access to, or turn over, any “electronic communication information or electronic device information, . . . without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions” absent an emergency

171. Kim Zetter, *California Now Has the Nation’s Best Digital Privacy Law*, WIRED (Oct. 8, 2015), <http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/>.

172. California “amended the state constitution in the 1970s to provide explicit privacy rights far more robust than those guaranteed by the Fourth Amendment of the US Constitution.” *Id.* Other comprehensive legislation demonstrates California’s progressive privacy approach. CAL CIV. CODE § 1798.83–84 (West 2015) (requiring businesses to provide customers with information regarding how their personal information is shared for marketing purposes); CAL. BUS. & PROF. CODE §§ 22580–22582 (West 2015) (requiring websites to allow minors to remove online content which they have posted on websites); CAL. BUS. & PROF. CODE § 22575(b)(1)–(3) (West 2015) (providing strict disclosure requirements for companies regarding their collection and use of users’ personal information).

173. Cal. Assembly Bill 370, pmbl. (Sept. 27, 2013) (amending Cal. Bus. & Prof. Code §§ 22575–22579).

174. *Id.*

175. California Electronic Communications Privacy Act, Cal. S. Bill 178, (Oct. 8, 2015); Zetter, *supra* note 171.

situation.¹⁷⁶ This piece of legislation has already gained the support of major industry leaders such as Google, Facebook, Apple, LinkedIn, Dropbox, and Twitter.¹⁷⁷ California's recognition that protection is needed from government surveillance places California's policy more in line with the EU's view on privacy policy than current U.S. federal law.¹⁷⁸ Proponents of this legislation aspire for it to serve as a model for the rest of the states to follow in implementing similar legislation.¹⁷⁹ Privacy proponents hope other states will begin to follow suit and that federal law will eventually catch up with state law.¹⁸⁰

In addition to these improvements, the United States has recently been demonstrating a noticeable increase in its participation in the realm of international data privacy,¹⁸¹ thus signifying a ripening opportunity for international cooperation in this area of law. The FTC expressed that "there is value in greater interoperability among data-privacy regimes as consumer data is increasingly transferred around the world."¹⁸² This recognition provides a window of opportunity for a more cooperative approach to dealing with this problem.

II. PAST EFFORTS TOWARD COOPERATION

Despite the challenges presented, the desire to allow for the free flow of data on an international level has continued to promote global cooperation in the data-privacy realm. This Part will first explore the Safe Harbor Agreement, demonstrating how the EU and United States have made an effort to preserve the free flow of data between these locations, despite their contrasting approaches to data-privacy law. It will then proceed to explore why the Safe Harbor failed, and how these regions are planning to move forward with the newly agreed-

176. California Electronic Communications Privacy Act, Cal. S. Bill 178, pmbl. para. (1) (Oct. 8, 2015).

177. Each of these companies have headquarters in California and therefore are governed by California law. Zetter, *supra* note 171.

178. *See id.*

179. Zetter, *supra* note 171.

180. *Id.*

181. Recently, the United States has engaged in several international cooperative efforts in the realm of data privacy, including the Asia-Pacific Economic Cooperation (APEC), the International Conference of Privacy and Data Protection Commissioners, the OECD, and GPEN. Tene, *supra* note 40, at 1226.

182. 2012 REPORT, *supra* note 136, at 10.

upon Privacy Shield. Subsequently, this Part will explore the OECD's role in data privacy, which has spanned decades. It will look at the organization's contribution of guidelines, and how these guidelines provide an accepted set of principles for data privacy around the world. Finally, this section will look at the development of GPEN, its contributions to data-privacy enforcement around the world, and its significance toward global cooperation in this area of law.

A. The Safe Harbor Agreement

When the EU Directive was passed, barring personal data transfers with non-EU countries who lack adequate data security standards, the ability for U.S. companies to continue doing business within the EU was threatened.¹⁸³ Due to the likelihood that U.S. law would be found to not provide "an adequate level of protection" under the EU Directive's assessment criteria, U.S. organizations became posed with the dilemma of either implementing new and costly data-privacy practices or potentially losing the opportunity to receive important data from entities within the EU.¹⁸⁴ As a result, negotiations commenced between EU and U.S. officials to create a set of principles that would afford U.S. organizations with an alternative means to meet the requirements of the EU Directive.¹⁸⁵

In 2000, the Safe Harbor was created, providing seven principles for U.S. organizations to follow when implementing data-security practices: (1) "Notice," which involves keeping individuals notified about the use of their personal information; (2) "Choice," allowing individuals to choose not to have their personal information disclosed to third parties or used for extraneous purposes; (3) "Onward Transfer," which requires companies to make sure that third parties they transfer personal information to, themselves, have adequate protection standards; (4) "Access" requiring the right for individuals to access their personal information and make corrections; (5) "Security" requiring that there must be reasonable safeguards in place to protect personal data from "loss, misuse and unauthorized access, disclosure, alteration and destruction;" (6) "Data Integrity," which calls for data usage to be relevant and ensures the data

183. *International Privacy Issues*, *supra* note 36, at 5.

184. Assey & Eleftherious, *supra* note 18, at 147.

185. *Id.*

being used is accurate; and (7) "Enforcement," which requires that there are mechanisms in place for reporting complaints, resolving issues, remedying problems, and punishing violations with sufficient sanctions to deter future violations.¹⁸⁶ By submitting to follow these principles, U.S. organizations were purportedly aligning their data-privacy practices with the requirements of the EU Directive.¹⁸⁷

Four months after the Safe Harbor was announced, the EC adopted a decision recognizing that the Safe Harbor provides "an adequate level of protection" for personal data that is transferred from the EU to the United States.¹⁸⁸ Following this announcement, the DOC began accepting applications from U.S. companies to submit to the program.¹⁸⁹ Submitting to the program was completely voluntary.¹⁹⁰ Once a company submitted itself to the Safe Harbor, violations of the standards became actionable under the Federal Trade Commission Act and punishable by sanctions.¹⁹¹ Consequently, the FTC played an important role in upholding this program, placing even more weight on the FTC's role in monitoring data-privacy practices in the United States.

For fifteen years, the EC's decision on the Safe Harbor remained sound law. On October 6, 2015, however, the European Court of Justice (ECJ) issued a decision in *Maximillian Schrems v. Data Protection Commissioner* ("ECJ Decision") declaring this program invalid.¹⁹² The ECJ held that "the Com-

186. U.S. DEP'T OF COMM., U.S.-EU SAFE HARBOR FRAMEWORK: A GUIDE TO SELF-CERTIFICATION (Mar. 2013) http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf [hereinafter U.S.-EU SAFE HARBOR FRAMEWORK].

187. See Assey & Eleftherious, *supra* note 18, at 147.

188. *Id.*

189. *Id.*

190. *International Privacy Issues*, *supra* note 36, at 5. More than three thousand U.S. companies have voluntarily submitted. Determann & Guttenberg, *supra* note 1, at 879.

191. Determann & Guttenberg, *supra* note 1, at 879.

192. The case was brought by an Austrian citizen bringing a claim with an Irish DPA regarding Facebook's transfer of his personal data from Europe to servers within the United States. Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 2015 E.C.R. 117/15. His claim alleged that in light of the Snowden revelations "the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country." *Id.* He brought this complaint to the

mission was required to find that the United States in fact ensures, by reason of its domestic law or international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the" EU Directive.¹⁹³ The ECJ found that the EC failed to make such a finding because it only looked at the Safe Harbor scheme.¹⁹⁴

The ECJ Decision also noted one of the flaws of the Safe Harbor was the fact that it is only applicable to U.S. entities that voluntarily agreed to it, and therefore U.S. government authorities are not subject to the Safe Harbor.¹⁹⁵ It furthered that because of this limitation, the national security, public interest, and law enforcement requirements of the United States will always prevail over and interfere with the requirements of the Safe Harbor, especially in light of the lack of rules or legal protections to prevent such interference.¹⁹⁶ Additionally, the ECJ Decision addressed the Snowden revelations, stating that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."¹⁹⁷

The ECJ Decision further found the Safe Harbor invalid due to the lack administrative or judicial means of redress provided for by the United States.¹⁹⁸ The Court found that because the United States fails to provide a means for individuals "to pursue legal remedies in order to have access to personal data relating to him, or to obtain the ratification or erasure of such data," EU citizens' fundamental right to effective judicial protection is compromised.¹⁹⁹

Additionally, the ECJ declared that even where the EC has issued a decision that found a non-EU country provided adequate protection to personal data, the DPA's powers cannot be

Irish DPA because this is where the Facebook's server is located. *Id.* The Irish DPA rejected the complaint on the grounds that the EC's 2000 decision already found that the United States ensures adequate protection under the Safe Harbor. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.*

199. *Id.*

reduced or eliminated as a result.²⁰⁰ The ECJ asserted that in order for the DPAs to perform the tasks delegated to them by the EU Directive, they must have complete independence to review transfers of data to non-EU countries in order to determine whether these transfers meet the requirements of the EU Directive.²⁰¹

Following the ECJ's decision, the Working Party issued a statement discussing the consequences of the decision, asserting that any transfers taking place in the future under the Safe Harbor will be considered unlawful.²⁰² The Working Party once again highlighted that "surveillance is incompatible with the EU legal framework and that existing transfer tools are not the solution to this issue."²⁰³ The statement called on Member States to work with the United States in finding a solution, which would allow transfers of data from the EU into the United States, without violating the fundamental rights of its citizens.²⁰⁴

B. The Privacy Shield

Although the Safe Harbor was only recently invalidated, the EU's disappointment with the program was recognized years before the ECJ decision was issued.²⁰⁵ Consequently, the EU and United States have been negotiating a new agreement to supplant the Safe Harbor for the past two years.²⁰⁶ On Febru-

200. *Id.*

201. *Id.*

202. *Statement of the Article 29 Working Party* (WP29), EC.EUROPA.EU (Oct. 16, 2015), [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-re-)

[re-lease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf). Following the *Schrems* decision, the Irish High Court now has the task of investigating the transfer of the personal data of Facebook's European users into the United States, and deciding whether the United States affords an adequate level of protection pursuant to the EU Directive. If the Court finds it does not, then such transfers will be suspended. Case C-362/14, Maximilian Schrems v. Data Protection Commissioner, 2015 E.C.R. 117/15.

203. *Statement of the Article 29 Working Party*, *supra* note 202.

204. *Id.*

205. *See Communication from the Commission to the European Parliament and the Council*, COM (2013) 847 Final (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

206. Jowitt, *supra* note 22.

ary 2, 2016, the EC announced that a new agreement had been reached between the U.S. and EU governments called the Privacy Shield.²⁰⁷ On February 29, 2016, draft texts of the new Privacy Shield were released to the public.²⁰⁸ On that same day, the EC also issued a press release²⁰⁹ that highlighted four key elements of the Privacy Shield that are intended to guarantee its compliance with the requirements of the ECJ decision: (1) “strong obligations on companies and robust enforcement”; (2) “clear safeguards and transparency obligations on U.S. government access”; (3) “[e]ffective protection of EU citizens’ rights with several redress possibilities”; and (4) an “[a]nnual joint review mechanism.”²¹⁰

The first element furnishes a lot of similarities to the Safe Harbor. Like the Safe Harbor, the Privacy Shield provides a set of principles for U.S. organizations to follow when implementing data-security standards.²¹¹ The Privacy Shield simi-

207. European Commission Press Release IP/16/216, European Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en.

208. U.S. Department of Commerce, EU-U.S. Privacy Shield Full Text (Feb. 29, 2016) <https://www.commerce.gov/privacyshield> [hereinafter Draft Text].

209. European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm. Within the press release the EC also mentions its negotiation of the EU-U.S. Umbrella Agreement, which provides standards to safeguard data transfers between the EU and United States for law enforcement purposes. *Id.* With the signing of the Judicial Redress Act on February 24, 2015, the EU-U.S. Umbrella Agreement can now be signed and concluded. European Commission Press Release MEMO/15/5612, Questions and Answers on the EU-US data protection “Umbrella agreement” (Sept. 8, 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm; Judicial Redress Act of 2014, H.R. 1428 (Feb. 12, 2016). The passing of the Act was the final step needed by the agreement in order to provide to EU citizens the right under the U.S. Patriot Act of 1974 to sue the United States for the unlawful disclosure of personal information—to EU citizens. European Commission Press Release MEMO/15/5612.

210. European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm.

211. The named principles are nearly identical to those of the Safe Harbor: (1) “Notice”; (2) “Choice”; (3) “Accountability for Onward Transfer”; (4) “Secu-

larly requires organizations to publicly declare their adherence to the principles, as well as publicly provide their privacy policies that they must fully implement.²¹² Furthermore, like under the Safe Harbor, U.S. organizations can voluntarily self-certify to the DOC that they will adhere to these principles, and by doing so, become subject to the FTC's enforcement authority.²¹³ The Privacy Shield, however, will also subject organizations to the investigative and enforcement authority of the U.S. Department of Transportation and other U.S. agencies "that will effectively ensure compliance with the Principles."²¹⁴ Additionally, the Privacy Shield calls for greater transparency than that provided by the Safe Harbor and establishes oversight mechanisms to ensure organizations are continuing to comply with its requirements.²¹⁵ Finally, the Privacy Shield imposes stricter conditions on transfers of data from certified organizations to third parties, as well as a greater potential liability from such transfers than was imposed by the Safe Harbor.²¹⁶

ity"; (5) "Data Integrity and Purpose Limitation"; (6) "Access"; and (7) "Recourse, Enforcement and Liability." Draft Text, *supra* note 208, at 4–7.

212. *Id.*

213. *Id.*

214. *Id.*

215. The draft text states that "[o]rganizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the [DOC] for information relating to the Privacy Shield." *Id.* at 7. Furthermore, those organizations who choose to work with DPAs—which is required for those that handle human resource data—must respond directly to the DPAs regarding EU investigations and must comply with their advice. *Id.* at 7, 20. Those that do not choose to work with the DPAs are still required to respond promptly to such complaints through the DOC. *Id.* at 7. Additionally, if either the FTC or a court order subjects an organization to an investigation for not complying with the Privacy Shield, it must provide all relevant sections of their compliance or assessment reports that were submitted to the FTC to the public (except where confidentiality requirements would be violated). *Id.*

216. The Privacy Shield introduces a number of new requirements that companies must meet in order to transfer data to third parties, including that they supply the DOC with information regarding the agreements that govern these transfers upon the DOC's request. *Id.* Furthermore, potential liability that organizations can face has increased under the Privacy Shield, as an organization will remain liable for any data processing done by third parties acting as agents of the organization that is inconsistent with the Privacy Shield unless it can prove "it is not responsible for the event giving rise to the damage." *Id.* Contrastingly, under the Safe Harbor, organizations avoided such responsibility (assuming the transfers were done in line with the Safe

The second element appears as an obvious response to mitigate the fears caused by the Snowden revelations. The U.S. government has given the EU written assurances proclaiming that “any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalised access to personal data.”²¹⁷ Additionally, the U.S. government committed to establishing an Ombudsperson in the Department of State, who will act independently from any national security services in handling and resolving the complaints of EU citizens regarding U.S. national intelligence.²¹⁸

The third element provides EU citizens with several avenues of redress that were not available under the Safe Harbor. Under the Privacy Shield, EU citizens can bring complaints directly to certified companies, who have to resolve them within forty-five days.²¹⁹ Companies are also required to provide “an independent recourse mechanism by which each individual’s complaints and disputes can be investigated and expeditiously resolved” free of charge.²²⁰ Additionally, these complaints can be submitted to the DPAs, which the FTC has committed to working closely with in order to respond to complaints within ninety days.²²¹ Finally, companies must commit to binding arbitration that will be available to EU citizens to resolve complaints that do not get resolved by the other redress mechanisms.²²²

Harbor principles) unless they knew or should have known about the inappropriate use of personal data by the third parties. U.S.-EU SAFE HARBOR FRAMEWORK, *supra* note 186, at 13.

217. European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm.

218. A Senior Coordinator will serve as the Ombudsperson and will designate additional officials from the DOS to assist in the performance of her duties. Draft Text, *supra* note 208, at Annex A, 2.

219. European Commission Press Release IP/16/433, *supra* note 217.

220. *Fact Sheet Overview of the EU-U.S. Privacy Shield Framework*, DEP’T OF COM. (Feb. 29, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf.

221. *Id.*

222. *Id.*

The final element—the annual joint review mechanism—is intended to monitor the functioning of new agreement.²²³ The review will be conducted by both the EC and DOC, along with U.S. national intelligence experts and European DPAs, to assess the commitments and assurances made by the United States.²²⁴ Additionally, the EC will hold an annual privacy summit with interested non-governmental organizations and stakeholders to discuss the developments of U.S. data-privacy law and its impact on EU citizens.²²⁵

This new agreement marks a step forward in international cooperation on personal-data privacy. Only time will tell how successful the new agreement will be in alleviating many of the problems that plague transfers of personal data between the EU and United States. However, even if successful, this agreement only governs personal data moving between these two locations, and as a result, fails to encompass any personal data moving throughout the rest of the world.²²⁶ To allow for protection of all personal data, a convention encompassing a wide inclusion of different nations is needed and the time is ripe for its creation. With the introduction of the new agreement, the DOC acknowledged that through the cooperation of both governments, “we have the real opportunity to improve the protection of privacy around the world.”²²⁷

C. OECD's Efforts to Improve International Data-Privacy Issues

The OECD is an intergovernmental organization (“IGO”) that operates under the mission of promoting “economic growth, prosperity, and sustainable development.”²²⁸ This mission is effectuated by bringing the governments of its thirty-four members to work together with over seventy non-members, to analyze commonly-held issues and compare their policies to ultimately find solutions that can be implemented in a coordinated fashion around the world.²²⁹ In accordance with this mis-

223. European Commission Press Release IP/16/433, *supra* note 217.

224. The EC will issue a public report on the review to both the European Parliament and the Council. *Id.*

225. *Id.*

226. *See id.*

227. Draft Text, *supra* note 208 (letter from Secretary Pritzker).

228. *About the OECD*, U.S. MISSION TO THE OECD, <http://usoeed.usmission.gov/mission/overview.html> (last visited Apr. 9, 2016).

229. *Id.*

sion, the OECD has taken an influential role in shaping international data-privacy law, bringing forth two major contributions to the harmonization of data-privacy regimes around the world: (1) the OECD Guidelines and (2) the recommendation to create GPEN.

1. Background

The OECD is an IGO established in 1961.²³⁰ Its establishment stemmed from the Organisation for European Economic Cooperation (OEEC), which was created in 1948 to administer funds from the Marshall Plan for the reconstruction of Europe following World War II.²³¹ After participating in the OEEC, governments of member countries came to recognize the interdependence of their economies, thereby inducing a desire for further cooperation amongst their governments.²³² Additionally, the acclaimed success of the OEEC attracted attention from governments outside the EU, creating a desire for other countries to join in future cooperative efforts.²³³ With an eagerness to expand the OEEC's cooperative efforts to a broader range of tasks and objectives, the OEEC was reconstituted as the OECD by the Convention on the Organisation for Economic Co-operation and Development ("OECD Convention").²³⁴

At its inception, the OECD Convention was signed by twenty countries. Today, the OECD has a total of thirty-four member countries, representing some of the wealthiest industrialized

230. The Convention was signed on December 14, 1960. However, the OECD was officially created when the Convention entered into force on September 30, 1961. *History*, ORG. ECON. COOPERATION & DEV., <http://www.oecd.org/about/history/> (last visited Feb. 16, 2016).

231. The Convention on the Organisation for Economic Co-operation and Development acted as a reconstitution of the OEEC in order to allow for the OEEC's "legal personality" to continue on. Article 15 of the Convention on OECD. *About*, ORG. ECON. COOPERATION & DEV., <http://www.oecd.org/about/oecd-convention.htm> (last visited Feb. 16, 2016); *History*, *supra* note 230.

232. *History*, *supra* note 230.

233. Both the United States and Canada, who were neither members of the OEEC, nor the EU, signed the OECD Convention after witnessing the work of the OEEC. *See id.*

234. Convention on the Organisation for Economic Co-operation and Development, Dec. 14, 1960 12 U.S.T. 1729, 888 U.N.T.S. 179 [hereinafter OECD Convention]; *About*, *supra* note 231.

governments in the world.²³⁵ These member countries, together with the five nations that are recognized as active partners of the OECD,²³⁶ presently account for 80 percent of the world's trade and investment.²³⁷ Despite its impressive membership, the OECD has participated in a wide breadth of activities while remaining "a remarkably low-profile institution" in comparison to the more well-known IGOs, like those within the U.N. system.²³⁸ Nonetheless, the OECD performs a variety of roles that have led the organization to operate as "an important and largely unrecognized role as a lawmaking body" in the past, and continues to do so while occupying "a unique space in the international lawmaking field."²³⁹

One of the major roles the OECD performs is that of a "research and networking organization."²⁴⁰ As a research institution, the OECD employs about 2500 staff members, comprised of economists, scientists, lawyers, and other professionals.²⁴¹ These staff members "collect data, monitor trends, forecast economic developments, and develop policy options for consideration by member countries" for essentially all areas of interest of member countries' governments.²⁴² Based on its work, the OECD has been commended for its "ability to gather and synthesize data on members' policy initiatives and results [that] provides a wealth of insight concerning which types of policies work best in particular settings."²⁴³

235. James Salzman, *The Organization for Economic Cooperation and Development's Role in International Law*, 43 GEO. WASH. INT'L L. REV. 255, 256 (2011). The current members consist of Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. *About*, *supra* note 231.

236. The partners are Brazil, India, the People's Republic of China, Indonesia, and South Africa. *History*, *supra* note 230.

237. *Id.*

238. Salzman, *supra* note 235, at 255.

239. *Id.* at 256.

240. *Id.*

241. *Who Does What*, ORG. ECON. COOPERATION & DEV., <http://www.oecd.org/about/whodoeswhat/> (last visited Feb. 16, 2016).

242. These areas include "trade, environment, agriculture, technology, taxation, education, foreign assistance, and employment." Salzman, *supra* note 235, at 257.

243. *Id.*

The OECD's role as a dynamic research institution is largely interrelated to its role as a networking organization.²⁴⁴ The OECD offers unique networking opportunities to governments due to the composition of its members and the level of privacy it offers them.²⁴⁵ While OECD membership is much more restrictive than that of IGOs like the U.N. or the World Trade Organization (WTO), it nonetheless covers just as broad of a range of topics.²⁴⁶ On the other hand, the OECD provides an opportunity for nations from different regions to work together because it has a broader membership than location-centered IGOs like the EU and the North American Free Trade Agreement (NAFTA).²⁴⁷ It also offers for such an opportunity to take place in a private setting where governments can "share experiences, identify issues of common concern, and coordinate domestic and international policies."²⁴⁸ This is especially significant to the field of international lawmaking because "the closed-door meetings of the OECD provide an important alternative forum to what is often viewed as the developing country-dominated and politicized U.N. system."²⁴⁹

Another unique characteristic of the OECD that "offers enormous flexibility and speed compared to other international institutions" is its decentralized structure.²⁵⁰ While decision making and direction planning of the OECD are left to the OECD Council, comprised of one representative of each member country and the EU,²⁵¹ the productive work is handled by specialized directorates.²⁵² These directorates are governed by committees that have representatives of each member country who are members of the relevant government agency to the

244. *See id.*

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.* at 256.

249. *Id.* at 257.

250. *Id.* at 257–58.

251. *Who Does What, supra* note 241; James Salzman, *Labor Rights, Globalization and Institutions: The Role and Influence of the Organization for Economic Cooperation and Development*, 21 MICH. J. INT'L L. 769, 782 (2000).

252. For example, the Trade Directorate "analyzes trade policies, explores the basis for common positions, and fleshes out disagreements in advance of future negotiations under the WTO." *Id.* at 782.

committee's specific policy,²⁵³ and work together to "advance ideas and review progress in specific policy areas."²⁵⁴ These committees are broken down even further into different groups to perform specific tasks.²⁵⁵ In sum, there are about 250 committees and different groups.²⁵⁶ The OECD's "range of inter-governmental committees serve as useful talking shops for countries to share experiences, learning from one another's successes and challenges."²⁵⁷

While the decentralized groups are significant to accruing and disseminating information to shape policies, the OECD Council's role is highly influential in the realm of international lawmaking.²⁵⁸ The OECD Convention grants the OECD Council with the authority to take three types of legal action:²⁵⁹ (1) issue recommendations;²⁶⁰ (2) adopt decisions;²⁶¹ and (3) enter into agreements with both member countries and nonmember countries, as well as international organizations.²⁶²

Recommendations are the least forceful, acting as "nonbinding agreements that generally represent policy advice with a strong base of support."²⁶³ Additionally, recommendations often act as framework to influence member countries' own policy development or serve as a precursor to issuing a decision.²⁶⁴ Generally, decisions are binding on all member countries and taken by their mutual agreement.²⁶⁵ Although, they do not im-

253. For example, "[t]he Environment Directorate's committee is drawn from officials of environment ministries and agencies." Salzman, *supra* note 251 at 782.

254. These specific policy areas include "economics, trade, science, employment, education or financial markets." *Who Does What*, *supra* note 241.

255. *Id.*; Salzman, *supra* note 251, at 782.

256. *Who Does What*, *supra* note 241.

257. Salzman, *supra* note 251, at 782.

258. *Id.* at 257-58.

259. OECD Convention, *supra* note 233, art. 7 ("A Council composed of all Members shall be the body from which all acts of the Organisation derive."); Salzman, *supra* note 236, at 782 ("Decisions and recommendations are voted on by the OECD Council at the ambassadorial level . . .").

260. OECD Convention, *supra* note 233, art. 5(b).

261. *Id.* art. 5(a).

262. *Id.* art. 5(c).

263. See Salzman, *supra* note 270, at 779.

264. *Id.*

265. This is not a universally applied rule because Article 5(a) states that decisions shall be binding on all member countries, "except as otherwise provided." OECD Convention, *supra* note 233, art. 5(a). Article 6(1) states that in

pose the same legal obligations as international treaties, members are required to take the necessary measures to implement them, once adopted.²⁶⁶

Although the OECD's authority to enter into international agreements has been used less frequently than its authority to issue recommendations and decisions, "the OECD's drafting of international agreements has played a significant role in crafting the emerging architecture of global governance."²⁶⁷ Additionally, although a limited number of agreements have been created by the OECD itself, the influence of OECD recommendations and decisions helps shape international policy by leading actors to use these instruments as starting points to build policy from.²⁶⁸

2. The OECD Guidelines

Based on a recommendation issued in 1980, the OECD Guidelines were created.²⁶⁹ Similar to the EU Directive, the OECD Guidelines sought to balance the need for protection of privacy with the free flow of information.²⁷⁰ To achieve this, the OECD Guidelines provide key definitions for implementation, instructions for protecting the flow of data, and set out a scope of restrictions on data transfers.²⁷¹

The OECD Guidelines became highly influential and paved the way for laws in a variety of countries.²⁷² The drafters of the

special cases, decisions will be taken unanimously. *Id.* art. 6(1). An example of a decision taken by the OECD is that which confirmed the importance of the Polluter-Pays Principle, which is "a fundamental principle for allocating costs of pollution prevention and control measures introduced by the public authorities in Member countries." The decision states, where a polluter pollutes, the expenses related to the pollution's impact should be allocated to the polluter. Salzman, *supra* note 235, at 258 (internal quotations omitted).

266. *OECD Legal Instruments*, ORG. ECON. COOPERATION & DEV., <http://www.oecd.org/about/whodoeswhat/> (last visited Mar. 8 2016).

267. An example of a legal instrument the OECD created is the OECD Anti-Bribery Convention. *Id.* at 259.

268. *See generally id.* at 255.

269. Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)58/FINAL (Sept. 23, 1980), <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm> [hereinafter *OECD Guidelines*].

270. Alo, *supra* note 102, at 1176.

271. *Id.*

272. Tene, *supra* note 40, at 1221.

OECD Guidelines recognized the growing privacy concerns that accompanied advances in technology.²⁷³ They also acknowledged the increasing complexities arising out of disparities between the data-privacy laws of different countries.²⁷⁴ The drafters also went on to note that although there are large disparities in the different laws, there seems to be general principles that are widely accepted throughout the international community.²⁷⁵ These principles were the first iteration of what has come to be referred to as the Fair Information Practice Principles ("FIPPS").²⁷⁶ These principles were later adopted by a

273. ORG. ECON. COOPERATION & DEV., THE OECD PRIVACY FRAMEWORK 40 (2013) [hereinafter OECD EXPLANATORY MEMORANDUM], http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Public interest has tended to focus on the risks and implications associated with the computerized processing of personal data and some countries have chosen to enact statutes that deal exclusively with computers and computer-supported activities.").

274. *Id.* at 39 ("These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries.").

275. These principles include:

setting limits to the collection of personal data in accordance with the objective of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions.

Id. at 41.

276. Tene, *supra* note 40, at 1221–22. The first principle of FIPPS is the "Collection Limitation Principle," which holds that there should be restrictions on collecting personal data, limiting collection to lawful and fair means. *OECD Guidelines*, *supra* note 269, pt. 2, § 7. The principle also recommends that consent, or at least knowledge by the data subject, should be given "where appropriate." *Id.* The second principle is the "Data Quality Principle," which recommends that when personal data is being used it should be relevant to the purpose of the use, and the data should be kept up-to-date and accurate. *Id.* pt. 2, § 8. The third principle is the "Purpose Specification Principle," which states that when data is being collected, the purpose of such a collection should be stated. *Id.* pt. 2, § 9. The fourth principle is the "Use Limitation Principle," which contends that data should not be used or disclosed for purposes other than that which was stated. *Id.* pt. 2, § 10. The two exceptions to this are when there is the data subject's consent or when the data is being acquired by a law authority. *Id.* The fifth principle is the

number of different countries in national legislation and are still utilized today.²⁷⁷

One of the strongest aspects of the OECD Guidelines is its use of simple and versatile definitions of key data-privacy terms.²⁷⁸ Its definition of “personal data”²⁷⁹ has been commended as “quite resistant to change” as its technological-neutrality has allowed it to remain adaptable to current innovations.²⁸⁰ The EU Directive’s definition of “personal data” is notably similar, showing the heavy influence the OECD Guidelines still have today.²⁸¹

The OECD Guidelines were created to encourage countries to establish their own data-privacy legislation, utilizing the guidelines as a minimum standard.²⁸² However, they are not binding and, unlike the EU Directive, countries are not mandated to pass legislation based on these recommendations.²⁸³ These minimum standards have no effect if they are not enacted. Another problem with the OECD Guidelines is that they lay the

“Security Safeguards Principle,” which provides that there should be reasonable security protecting personal data from risks such as unauthorized access, use, destruction or some type of loss. *Id.* pt. 2, § 11. The sixth principle is the “Openness Principle,” which holds that the general use, policies, developments, and practices in relation to personal data should be made public. *Id.* pt. 2, § 12. It specifies that the data controllers’ location should be apparent. *Id.* The seventh principle is the “Individual Participation Principle,” which provides that individuals should have some control over the use of their data. *Id.* pt. 2, § 13. They should be able to obtain their data and challenge the use of their data, and if their challenges are successful, they should be able to have their data removed from wherever it resides. *Id.* The final principle is the “Accountability Principle,” which states that “[a] data controller should be accountable for complying with measures which give effect to the principles stated above.” *Id.* pt. 2, § 14.

277. Tene, *supra* note 40, at 1221–26. FIPPS were adopted by the United States in the Privacy Act of 1974, by Canada in the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.), and by the EU in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. 108, as well as in the EU Directive, where it adopted the definition of “personal information.” Tene, *supra* note 40, at 1221–26.

278. Tene, *supra* note 40, at 1221–22.

279. The Act defines it as any information which relates to “an identified or identifiable individual.” *OECD Guidelines*, *supra* note 269, pt. 1, § 2.

280. See Tene, *supra* note 40, at 1221–22.

281. *Id.*

282. *OECD Guidelines*, *supra* note 269, pt. 1, § 6.

283. Tene, *supra* note 40, at 1222.

groundwork for standards that countries should aim to achieve without providing any enforcement mechanisms for achieving such standards.²⁸⁴ Nonetheless, there has been a significant increase in member countries' national privacy legislation, as well as the number of authorities that have enforcement responsibilities related to data privacy since the adoption of the OECD Guidelines.²⁸⁵

In July 2013, the OCED Guidelines were updated to account for the new ways in which data is being used and the new accompanying risks.²⁸⁶ The two themes purported to run through the updated guidelines are risk management and improved interoperability.²⁸⁷ Despite these changes, these guidelines are still not in any way binding.²⁸⁸ As a result, disparities in data-privacy protection continue to exist. Nonetheless, the existence of these guidelines provides the international community with a platform to start building upon in order to create a binding legal instrument.

D. GPEN

In 2007, the OECD adopted a recommendation developed by the OECD Committee for Information, Computer and Communications Policy ("ICC"), which called for more cooperation amongst international authorities in order to better protect personal-data privacy.²⁸⁹ This recommendation was adopted after the OECD recognized that there was a growing rate of cross-border data flow and increased risks to data privacy as a result.²⁹⁰ As has been the

284. *Id.*

285. Whereas, at the time of the OECD Guidelines' adoption, only around one-third of its OECD members had some type of privacy legislation, now nearly all member-countries have legislation that provides for privacy protection, as well as established authorities with enforcement powers. Org. for Econ. Co-operation & Dev., *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* 4 (2007), <http://www.oecd.org/internet/ieconomy/38770483.pdf> [hereinafter *OECD Recommendation*].

286. See generally OECD EXPLANATORY MEMORANDUM, *supra* note 273.

287. The new guidelines provide national privacy strategies, privacy management programs, and data security breach notification standards. Tene, *supra* note 40, at 1231.

288. See generally OECD EXPLANATORY MEMORANDUM, *supra* note 273.

289. *OECD Recommendation*, *supra* note 285.

290. The OECD and other international organizations, including the International Conference of Data Protection and Privacy Commissioners, the EU

case in a number of other areas of law, the OECD recommended that its member countries establish “an informal network of Privacy Enforcement Authorities . . . to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.”²⁹¹

Based on this recommendation, GPEN was established in 2010.²⁹² GPEN is meant to exist as an informal network of data-protection authorities and regulators who can work together in the enforcement of the wide range of data-privacy laws that currently exist.²⁹³ GPEN is specifically meant to target enforcement in the private sector.²⁹⁴ The network is also meant to serve as a mechanism for countries to discuss different issues of data-privacy law and share new information and experiences with one another.²⁹⁵

At its inception, it was not fully understood how GPEN would function.²⁹⁶ In June 2012,²⁹⁷ an action plan was adopted, outlining GPEN’s goals and how it intends to achieve them.²⁹⁸ As time goes on, the number of members continues to rise. GPEN proponents have maintained hope that as members communicate about their different enforcement practices, they will develop similar priorities, ultimately leading to more of a cohe-

Article 29 Working Party, and the Asia Pacific Economic Cooperation, have begun to draw attention to the need for cooperation in data privacy in recent years. *Id.* at 4.

291. *OECD Recommendation*, *supra* note 285.

292. GLOB. PRIVACY ENF’T NETWORK, <https://www.privacyenforcement.net> (last visited Oct. 21 2015).

293. *Action Plan for the Global Privacy Enforcement Network*, GPEN (Jan. 22, 2013) [hereinafter *GPEN Action Plan*], <https://www.privacyenforcement.net/public/activities>.

294. *Id.*

295. *Id.*

296. Amy R. Worley, *On the Heels of FTC, FCC Joins Global Privacy Enforcement Network (GPEN) to Better Watch Data*, NAT’L L. REV. (Oct. 30, 2014) [hereinafter *On the Heels of the FTC*], <http://www.natlawreview.com/article/heels-ftc-fcc-joins-global-privacy-enforcement-network-gpen-to-better-watch-data-abr>.

297. This action plan was amended on January 22, 2013. *GPEN Action Plan*, *supra* note 293.

298. *See generally id.*

sive set of data-privacy laws throughout the world.²⁹⁹ However, this action plan is not legally binding.³⁰⁰ Thus, in practice, it is likely that there will still be varying levels of protections and large inconsistencies between the laws of different nations.

The formation of GPEN and the widening inclusion of different countries into the network shows the global recognition of the need for cooperation in the area of data-privacy law. Members of GPEN have already begun to create certain mechanisms that will facilitate the cooperation amongst participating governments.³⁰¹ One of these mechanisms is the GPEN Alert.³⁰² GPEN members

299. On October 28, 2014, the FCC joined GPEN, adding another U.S. agency to its members alongside the FTC, which was already a member. *On the Heels of FTC*, *supra* note 296. The European Data Protection Supervisor currently represents the EU. For a comprehensive list of all of the member authorities, see GLOB. PRIVACY ENFT NETWORK, <https://www.privacyenforcement.net> (last visited Feb. 16, 2016).

300. The domestic laws will remain the preeminent authority over GPEN:

Cooperation pursuant to this Action Plan remains subject to the domestic laws and international obligations applicable to Participants. Nothing in this Action Plan obliges Participants to provide confidential or sensitive information or cooperate in particular cases. This Action Plan does not create a legally binding mechanism for Participants to exchange information about specific investigations and cases. Such cooperation remains subject to the applicable laws in the jurisdictions involved.

GPEN Action Plan, *supra* note 293.

301. Another recent action taken by GPEN includes the Privacy Sweep (the "Sweep"). *Results of the 2015 Global Privacy Enforcement Network Sweep*, OFFICE OF THE PRIVACY COMM'R OF CAN. (Sept. 2, 2015), https://www.priv.gc.ca/media/nr-c/2015/bg_150902_e.asp. The Sweep consisted of participants visiting "1,494 websites and mobile applications (apps) that were either targeted at or popular among children." *Id.* The purpose of the Sweep was "to determine whether apps and websites are collecting personal information from children, what personal information is being collected, whether protective controls exist to effectively limit the collection and whether the information could be easily deleted." *Id.*

302. At its outset, GPEN Alert will be used

to notify other member authorities of their privacy investigations and enforcement actions, particularly those that have cross-border aspects, for purposes of potential coordination and cooperation. In the future, GPEN Alert functions may be expanded to allow the sharing of additional confidential, non-public enforcement information relating to specific investigations and enforcement matters, and/or to allow the sharing of consumer complaints relating to privacy.

who utilize GPEN Alert will be able to use the mechanism for two purposes: (1) to notify other GPEN members about investigations and law enforcement matters; and (2) to determine whether other GPEN members have previously begun any investigations or law enforcement matters against the same individuals, companies, or practices.³⁰³ So far, the FTC, along with agencies from seven other countries, have signed the Memorandum of Understanding, which is required in order to participate in GPEN Alert.³⁰⁴ Because GPEN Alert was recently created, it is not yet known how effective this mechanism will be in practice.³⁰⁵ It is important to note, however, that GPEN members will not automatically become participants in GPEN Alert. Each member authority that wants to participate must voluntarily submit to a variety of steps in order to gain access to this tool, and even then each member will be able to decide what information they want to input into the system.³⁰⁶ Due to its voluntary nature, this tool will only be as useful as participating members allow it to be.³⁰⁷ Nonetheless,

GPEN, *A Secure Information-Sharing System for the Global Privacy Enforcement Network*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/cooperation_agreements/151026gpen-alert-mou.pdf (last visited Feb 16, 2016).

303. *Id.* at 2. Today, GPEN Alert uses the same technology used in the FTC's Consumer Sentinel Network, which consists of a database that stores consumer complaints submitted to the FTC and provides access to participating U.S. law enforcement agencies. Hunton & Williams, *GPEN Launches New Global Consumer Privacy Protection Initiative*, PRIVACY & INFO. SECURITY L. BLOG (Oct. 30, 2015), <https://www.huntonprivacyblog.com/2015/10/30/gpen-launches-new-global-consumer-privacy-protection-initiative/>.

304. The other agencies that signed on are from Australia, Canada, Ireland, the Netherlands, New Zealand, Norway, and the United Kingdom. *Id.*

305. The FTC issued a press release regarding GPEN Alert on October 26, 2015. *Id.*

306. In order to gain access to GPEN Alert, members have to sign the Memorandum of Understanding, as well as execute both a Data Security and Minimum Safeguard Certification of Access to GPEN Alert Information. *FTC and Seven International Partners Launch New Initiative to Boost Cooperation in Protecting Consumer Privacy*, FED. TRADE COMM'N (Oct. 26, 2015), <https://www.ftc.gov/news-events/press-releases/2015/10/ftc-seven-international-partners-launch-new-initiative-boost>.

307. Despite the FTC's promotion of GPEN Alert, there has been less enthusiasm demonstrated by its other participants. Only one of the seven other participants even published a press release regarding their participation. Keiren McCarthy, *Feds in America Very Excited About New Global Privacy*

this step illustrates the desire amongst participating countries to work together within the realm of data privacy. It also provides the international community with an organization that can be put to good use in the development of a convention on data privacy.

The efforts of the EU and U.S. governments to create a mechanism that allows for the continued transfer of personal data between the regions demonstrates the importance of the free flow of data around the world. The failure of the Safe Harbor, however, demonstrates the issues that continue to hinder governments' ability to protect the personal data of their citizens. By reviewing the contributions of the OECD, it becomes apparent that although there are diverging data-privacy laws, there is a lot of common ground to work with and a shared desire for harmonization of data-privacy policies on a global level. Additionally, the creation of GPEN further demonstrates the desire for different nations to work together in this area of law, further signifying the need for a convention on data privacy.

III. THE CISG AS A MODEL FOR A CONVENTION ON DATA PRIVACY

In 1980, the Vienna Sales Convention was held and the CISG draft text was adopted with very little amendment.³⁰⁸ The CISG is a treaty consisting of a set of laws that govern the international sales contracts between private businesses of participating nations.³⁰⁹ Today, it is recognized as one of the most successful examples of a multijurisdictional private law.³¹⁰ Looking back at its development can provide insight into how comprehensive international private law is developed. Analyzing the strengths and weaknesses of the CISG can facilitate the structuring of a convention on data privacy.

The CISG serves as an excellent example of the diplomatic drafting of a new convention. Using the CISG as a model, a convention on data privacy should be drafted under the auspices of the OECD. The key elements of the CISG that should be implemented for this new convention include the process by which it

Alert System, REGISTER (Oct. 26, 2015), http://www.theregister.co.uk/2015/10/26/ftc_excited_about_gpis/.

308. Sono, *supra* note 28, at 6.

309. *United Nations Convention on Contracts for the International Sale of Goods (Vienna, 1980) (CISG)*, UNCITRAL (last visited Jan. 24, 2014), http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html.

310. Andersen, *supra* note 25, at 14–15.

was developed, its capitalization on key timing, its automatic application to private parties who live in signatory states, its use of simple, clear, and practical language, and its creation of a gap-filling mechanism to deal with issues not explicitly covered by the convention that should nonetheless be governed by it. Additionally, to improve upon the CISG's model and tailor it to the needs of data-privacy, the new convention should provide for supervisory authorities in each signatory state to ensure the convention is being interpreted and applied in a uniform manner.

A. Development

The CISG's success came after decades of efforts directed toward the establishment of a unified body of law that addressed the sale of goods internationally. The road to the CISG started in 1926, when the International Institute for the Unification of Private Law ("UNIDROIT")³¹¹ decided to pursue a uniform body of law for the international sale of goods based on "the principle that a uniform law of international sales should be based on the basic principles of private law which could be arrived at through the comparison of national laws rather [than] commercial practice."³¹² After a number of drafts were presented and reworked, UNIDROIT ultimately produced two separate conventions at the Hague Conference of 1964: the Convention for the Uniform Law of International Sales and the Convention for the Uniform Law on the Formation of Contracts for the International Sale of Goods (together, "the Hague Conventions").³¹³ Despite these efforts, only nine nations ratified the Hague Conventions, prompting the United Nations to embark on a process to gain wider adoption of an international sales law.³¹⁴

311. Sieg Eiselen, *Adoption of the Vienna Convention for the International Sale of Goods (the CISG) in South Africa*, 116 S. AFR. L.J. 323, 333 (1999). UNIDROIT now operates as "an independent intergovernmental Organisation . . . to study needs and methods for modernizing, harmonizing and co-ordinating private and in particular commercial law as between States and groups of States and to formulate uniform law instruments, principles and rules to achieve those objectives." *History and Overview*, UNIDROIT, <http://www.unidroit.org/about-unidroit/overview> (last updated Jan. 13, 2016).

312. Sono, *supra* note 28, at 1.

313. Eiselen, *supra* note 311, at 333.

314. *Id.* at 334.

In 1966, the United Nations Commission on International Trade Law ("UNCITRAL")³¹⁵ was created by the U.N. General Assembly to facilitate the unification of international trade law.³¹⁶ At that time, it became apparent that an international trade law was needed in order to "provide a uniform law to apply to private transactions of companies with businesses in different nations."³¹⁷ As businesses from different countries began to conduct cross-border transactions on an increasingly common basis, problems began to arise with conflicting contract interpretation by different nations' legal systems.³¹⁸ This created both uncertainty and difficulty for parties from different countries in entering sales contracts.³¹⁹

In order to better understand how to promote wider adoption of a convention amongst different nations, UNCITRAL conducted analyses of the Hague Conventions.³²⁰ Through its research, UNCITRAL discovered that the most prominent areas of concern with these conventions were their overall complexity and the lack of global representation during their creation.³²¹ As a result, UNCITRAL created a working group to determine ways to revise the Hague Conventions to more appropriately fit both the needs and desires of more countries.³²² At each stage of the drafting process, the text was sent to governments and other interested international organizations for their feedback, which was subsequently used to help improve the text.³²³

Just like UNCITRAL, GPEN was created to research an area of law that, due to its lack of uniformity, causes a great deal of confusion and difficulty for parties of different nations to do business with one another. UNCITRAL can be compared to GPEN in a variety of ways. Both organizations were created to

315. UNCITRAL is "[t]he core legal body of the United Nations system in the field of international trade law." *About UNCITRAL*, UNCITRAL, http://www.uncitral.org/uncitral/en/about_us.html (last visited Feb. 16, 2016).

316. Sono, *supra* note 28, at 1.

317. Maureen T. Murphy, *United Nations Convention on Contracts for the International Sale of Goods: Creating Uniformity in International Sales Law*, 12 FORDHAM INT'L L.J. 727, 728 (1988).

318. See Eiselen, *supra* note 311, at 324–27.

319. *Id.*

320. Sono, *supra* note 28, at 1–2.

321. *Id.* at 2–5.

322. This group is titled the "Working Group on the International Sale of Goods." *Id.* at 3.

323. *Id.* at 3–5.

assist in alleviating problems arising out of the lack of uniform law in their respective industries.³²⁴ Additionally, both were created in order to research and analyze the current state of law and determine how to improve it. Finally, the ultimate goal in creating both UNCITRAL and GPEN was to foster the discovery of the best framework for governing their respective industries in order to help unify the law of different nations governing said industries.³²⁵

In order for a convention on data privacy to be successful, there should be a similar drafting process to the CISG, utilizing GPEN to facilitate the process. Just as UNCITRAL researched the problems impeding the development of a unified law in international sales, GPEN is planning to research the current issues hindering the enforcement of different national laws regarding personal data protection, and preventing cross-border cooperation in order to strengthen personal privacy protection on a global level.³²⁶ GPEN should take this research a step further and look into what is needed to adopt a unified law on data privacy. Just as UNCITRAL reviewed and analyzed failed attempts at harmonizing sales law, GPEN should examine the failed attempts to harmonize data-privacy law amongst different nations, including the Safe Harbor and the EU Directive.

GPEN's current goals are focused on cooperation and education.³²⁷ However, this is the perfect platform to begin drafting legislation. There are already forty-four different jurisdictions represented within GPEN.³²⁸ Following in UNCITRAL's footsteps, after sufficient research has been conducted, GPEN should create a working group to start drafting laws. Just as the drafts leading to the CISG were passed to different coun-

324. *Id.* at 1–5; *GPEN Action Plan*, *supra* note 293.

325. Sono, *supra* note 28, at 1–5; *GPEN Action Plan*, *supra* note 293.

326. *GPEN Action Plan*, *supra* note 293.

327. *Id.*

328. Currently, this includes Albania, Argentina, Australia, Belgium, Bulgaria, Canada, China, Colombia, Czech Republic, the EU, Estonia, France, Germany, Georgia, Ghana, Gibraltar, Guernsey, Hungary, Ireland, Isle of Man, Israel, Italy, Korea, Kosovo, Lithuania, Luxembourg, Macedonia, Malta, Mauritius, Mexico, Moldova, Monaco, Morocco, Netherlands, New Zealand, Norway, Poland, Singapore, Slovenia, Spain, Switzerland, Ukraine, the United Kingdom, and the United States. *About the Network*, GLOB. PRIVACY ENFT NETWORK, https://www.privacyenforcement.net/about_the_network (last visited Feb. 15, 2016).

tries for revision and recommendations,³²⁹ the drafts created by this working group should be passed around to the members of GPEN. Through this process, countries can decide on transparent and clearly-defined procedures for turning personal information over to domestic governments, thereby eliminating fears of secret government surveillance. This process will allow countries to ensure their desires are reflected and will ultimately help gain wider adoption.

One major difference between the development of a convention on data privacy and the development of the CISG is that this convention should be enacted under the auspices of the OECD instead of the U.N. With the statistics of data transfers continuing to rise at a rapid pace, a convention on data privacy is needed as quickly as possible. Unlike the U.N., which has a much broader global representation, the OECD has a more restrictive membership, inclusive of countries with similar economic interests and levels of development, and therefore offers more opportunity for similar policy approaches to creating a data-privacy law. Furthermore, the privacy offered by the closed-door meetings of the OECD provides an opportunity for participating governments to talk about the sensitive problems associated with national security openly, without fearing that information will be released to unwanted parties, which will help facilitate a solution between the involved nations.

B. Timing

In addition to the efforts put into drafting the CISG, timing was a key factor that led to its success. Whereas prior attempts at drafting an international sales law had failed due to ill-timing,³³⁰ the CISG was formulated when international trade was becoming so pervasive that countries were receptive to a law that would protect those engaging in international sales, while still promoting the growth of the international market.³³¹ Similarly today, the global community is reaching the point

329. Sono, *supra* note 28, at 3–5.

330. *Id.* at 5. ("Although the legislative process was open to all States, the newly emerging developing countries were not yet necessarily at the forefront of the international scene. Socialist countries were almost about to join or even to initiate the global unification effort of the law of trade, perhaps partly based on the then new trend for the strengthening of the East-West economic relations, but the timing was still a few years short.")

331. *See id.*

that it needs an international law on data privacy that will protect those whose data is being used, while promoting the free flow of data of the world.

Significantly, it has been noted that during the Hague Conference of 1964³³² the fact that the United States “was not well-prepared” to participate in the unification process was a contributing factor to this attempt’s lack of success.³³³ When the CISG was finally adopted, the United States had finally developed to a point that it could participate.³³⁴ Similarly, today the global community is reaching the point that it needs an international law on data privacy that will protect those whose data is being used, while promoting the free flow of that data.³³⁵ As seen with the failure of the Safe Harbor, until nations sign onto a piece of binding legislation, domestic law will remain the prevailing force governing personal data and inconsistent levels of protection will continue to exist.

As was the case with the CISG, the United States’ current position on data privacy is finally maturing to a point that would allow for participation in an international convention. The United States’ policy on regulating personal data has made a noticeable migration towards providing stricter protections, and thus offers a ripening opportunity for a convention on data privacy to be proposed at this time when the country is receptive to such legislation. The FTC, whose approach to data privacy had in the past reflected the general U.S. policy in favor of self-regulation, is now at the forefront of pushing for broad legislation and heightened data protection.³³⁶ Thus, indicating a dramatic shift from prior U.S. policy regarding data-privacy legislation. Additionally, the push toward international cooperation by the Obama administration demonstrates an openness to participating in a data-privacy convention.³³⁷ Furthermore, U.S. companies that engage in international data transfers

332. *Id.*

333. *Id.* (“The United States decided to join in the unification movement in 1964 for the first time, but was not well-prepared for the Hague Conference although it participated.”)

334. *See id.*

335. This goal is represented in the EU Directive. Council Directive 95/46, *supra* note 38, pmbl. This goal is also represented in the OECD’s privacy framework. OECD EXPLANATORY MEMORANDUM, *supra* note 273, at 3.

336. *See generally* 2012 REPORT, *supra* note 136.

337. Tene, *supra* note 40, at 1235.

have recently exhibited a willingness to abide by stricter standards, which demonstrates that parties who would be governed by this convention are on board for its adoption. Furthermore, the United States' willingness to agree to stricter restrictions on governmental access to personal data covered by the Privacy Shield demonstrates the ability for nations to cooperate and modify their domestic policies to allow for the free flow of data. Finally, the United States is currently represented by both the FTC and FCC in GPEN,³³⁸ demonstrating both the willingness and an ability to participate in unification efforts.

C. Automatic Application with an Opt-Out Option

The CISG is automatically applied to agreements between parties who reside, or have their place of business, in countries that are members of the CISG.³³⁹ If these parties do not want the CISG to apply to their transactions, they can utilize the opt-out mechanism the CISG provides.³⁴⁰ With this option, the CISG operates as a default rule.³⁴¹ If the participating parties want to avoid the application of the CISG, there are certain requirements that must be fulfilled.³⁴² These requirements ensure that the parties are fully aware of the rights provided by the CISG before consenting to its exclusion, which protects each party from being taken advantage of.³⁴³

The convention on data privacy should have a similar opt-out option. The freedom to contract out of the convention will allow for a level of flexibility that will entice more countries to join. However, because these agreements will often be between large companies and individuals using their services, it is important to have stringent requirements for opting out. By providing an opt-out option, companies can avoid the requirements of this convention when doing business with other sophisticated parties. How-

338. *On the Heels of the FTC*, *supra* note 296.

339. Morten M. Fogt, *Private International Sales Law Issues in Opt-Out and Opt-In Instruments of Harmonization: The CISG and the Proposal For a Common European Sales Law*, 19 COLUM. J. EUR. L. 83, 89–90 (2013).

340. CISG, *supra* note 26, art. 6.

341. Fogt, *supra* note 339, at 89–90.

342. The parties must be aware of the CISG and their automatic application. The parties must wish to opt-out of the CISG, and this decision has to be reached by both parties. The decision to avoid the CISG cannot be unilateral. *Id.* at 90–91.

343. *See generally id.*

ever, it will still ensure that individuals' privacy rights are protected and will make sure they are completely aware of how their personal information is being used by these companies. These requirements should reflect those of the CISG: both parties should understand the convention exists and is automatically applied; after having full knowledge of the convention they must actively opt-out of its use; and there must be consent on both sides of the agreement before the opt-out is valid.³⁴⁴ By having such a requirement, companies will be unable to hide their data-collection practices in a remotely-placed website privacy policy that assumes user's consent solely by using the website. Instead, companies will be required to explicitly tell users what information they plan to collect from them, how they plan to collect it, and who they plan to share it with, and will be required to ensure that users fully understand these rights before they can consent to the collection and processing of their personal information. Furthermore, this opt-out provision could be accompanied by a similar requirement to that of the EU Directive that limits the circumstances by which personal data can be processed to those that further a legitimate purpose, thereby further safeguarding individuals' privacy.

D. Simple, Clear, and Practical

One of the largest obstacles in regulating data privacy is drafting a law that can apply to future unforeseen innovations in technology. Three characteristics of the CISG that have been fundamental to its success are its "simplicity, practicality, and clarity."³⁴⁵

During the drafting process, drafters of the CISG recognized that the use of short-hand expressions in the text could result in varying interpretations.³⁴⁶ As a result, the drafters avoided the use of short-hand expressions as much as possible.³⁴⁷ When the use of such expressions was unavoidable, drafters made sure to provide a clear definition of what they were referring to.³⁴⁸

344. Fogt, *supra* note 339, at 90–91.

345. Sono, *supra* note 28, at 6.

346. *Id.* at 6–7.

347. *Id.*

348. For example, the word "delivery" was unavoidable, but drafters made sure to provide a clear definition that could not be misconstrued by interpreters. *Id.*

Similar to the way CISG drafters avoided short-hand expressions, drafters of this convention should avoid using language that is too specific to current technologies. It would be useful for drafters to look to the technology-neutral language found within the OECD Guidelines, which has remained relevant with the passage of time.³⁴⁹ For example, the definition of “personal data” established in the OECD Guidelines is any information, which relates to “an identified or identifiable individual.”³⁵⁰ This definition avoids referencing anything other than how the data relates to an individual. Its simplicity allows it to apply to different forms of data, whether it be data stored in “the Cloud”³⁵¹ or data stored on a hard-drive.³⁵² Simple, clear, and practical language will allow the convention to remain practical, while technology continues to develop.

E. Gap-Filling Mechanism

Another way to address the rapid growth of technology is by creating a gap-filling mechanism to cover issues that are not originally written into the convention, but nonetheless should be governed by it. The CISG has its own gap-filling mechanism, which is meant to assist courts and tribunals with filling in areas left out of the CISG in a way that continues to promote uniformity.³⁵³ This mechanism is to be used when a matter arises that is “governed by” the CISG, but has not been expressly dealt with by any of its provisions.³⁵⁴ When confronted with a matter of this nature, the CISG requires that the matter be “settled in conformity with the general principles on which it is based.”³⁵⁵ If no general prin-

349. See Tene, *supra* note 40, at 1221–22.

350. *OECD Guidelines*, *supra* note 269, pt.1 § 1(b).

351. “The Cloud” is a “collection of computing resources such as applications, storage space and processing power to be delivered via the Internet.” Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 363–64. (2010).

352. A hard drive stores data within a computer on a disk. Tim Fisher, *What is a Hard Disk Drive?*, ABOUT TECH, http://pcsupport.about.com/od/componentprofiles/p/p_hdd.htm (last visited Feb. 16, 2016).

353. CISG, *supra* note 26, art. 7(2).

354. *Id.*

355. *Id.*

cipals can be applied to govern the matter then as a last resort, the appropriate domestic sales law will be applied.³⁵⁶

The issue with the use of general principles to fill gaps within the CISG is that the text of the CISG never actually defines any general principles.³⁵⁷ Without a clear set of principles to turn to, courts and tribunals often skip over the step of trying to fill in a gap with the general principles and instead refer to domestic law.³⁵⁸ This problem eliminates the predictability and reliability that the CISG is meant to provide to foreign merchants.³⁵⁹ Furthermore, avoiding use of the general principles is unfair to foreign parties who are unfamiliar with domestic laws and should not be subject to them under circumstances where the CISG applies.³⁶⁰

Conveniently, a lack of clear, defined principles will not be an issue in the realm of data privacy. Since their first iteration in the OECD Guidelines, FIPPS have been internationally recognized as the general principles of data privacy.³⁶¹ These principles are already reflected in different pieces of national data-privacy legislation throughout the world and continue to be promoted by proposals for new legislation.³⁶² These principles

356. Andersen, *supra* note 25, at 15.

357. *Id.* Because no list could be exhaustive of all of the potential principles, the drafters feared that if any were codified, the remaining principles would never be utilized. *Id.* at 25. Refraining from listing the principles also served to provide courts with a level of flexibility to adequately address concepts such as fair practice, public policy, and fundamental justice. *Id.* at 26. As a result, “the ‘general principles’ alluded to are not tangible, but can best be described as non-codified expressions of the underlying ideas which permeate the CISG.” *Id.* at 24. Often they are described as embodying the “spirit of the convention.” *Id.* at 25.

358. Philip Hackney, *Is the United Nations Convention on the International Sale of Goods Achieving Uniformity?*, 61 LA. L. REV. 473, 474–75 (2001).

359. Franco Ferrari, *Homeward Trend and Lex Forism Despite Uniform Sales Law*, 13 VINDOBONA J. INT’L COM. L. & ARB. 15, 20 (2009), <http://www.cisg.law.pace.edu/cisg/biblio/ferrari17.html>.

360. Mauricio Gomm Santos & Quinn Smith, *Reviewing the History and Application of Article 7*, CISG BRASIL (2011), http://www.cisg-brazil.net/doc/Reviewing_the_History_and_Application_of_Article_7_%28Final%29.pdf.

361. Tene, *supra* note 40, at 1221.

362. See, e.g., WHITE HOUSE REPORT, *supra* note 156. Additionally, the FTC noted in its 2012 Report, “[n]umerous comments, including those from large industry stakeholders, consumer and privacy advocates, and individual con-

should be provided within the convention and utilized to govern matters that fall within the jurisdiction of the convention, but are not expressly settled within it. By utilizing the same mechanism that the CISG provides, along with an accompanying set of explicit, widely accepted principles, this convention will be able to circumvent the issues that have been associated with the interpretation of the CISG's gap-filling provision.³⁶³

F. Supervisory Authority

Another way to improve upon the CISG's model is by providing for supervisory authorities that can assist in upholding the convention, and facilitate its application and interpretation. Despite the large number of signatories to the convention, "there is no court with general jurisdiction on the CISG throughout the world, and the decisions and writings from one country are little more than persuasive authority in another location."³⁶⁴ The CISG encourages courts and tribunals to look to one another for guidance, calling for uniformity and regard to the CISG's international character when interpreting its provisions.³⁶⁵ Therefore, objectives of the CISG should take precedence over the objectives of one's own domestic laws during interpretation.³⁶⁶ However, often

sumers supported some form of baseline privacy legislation that incorporates the FIPPs." 2012 REPORT, *supra* note 136, at 11.

363. An illustrative example of this problem is the Argentine case *Alejandro Mayer v. Onda Hofferle GmbH & Co.*, Apr. 24, 2000 (Cámara Nacional de Apelaciones en lo Comercial), *translated at* <http://cisgw3.law.pace.edu/cases/000424a1.html>. The gap in this case was "whether the quality of goods met the standards of the contract." *Id.* Despite the court's finding that the CISG governed the case, when a gap was found within one of the CISG's provisions, instead of trying to fill it in with a general principle, the court went straight to the Argentine Commercial Code. *Id.* Commentators have criticized this decision, arguing that "[w]hile the CISG does not contain the precise procedure for quality testing of goods, it certainly addresses the issue of the quality of the goods and provides a framework for dissolving the dispute." Santos & Smith, *supra* note 360, at 11–12. In its assessment, the court never performed the broader analysis under Article 7(2) that is called for by the CISG. *See id.* Instead it went back and forth between the CISG and the Argentine Commercial Code, picking and choosing when to apply each law on its own accord. *See id.*

364. *Id.* at 9.

365. CISG, *supra* note 26, art. 7(1).

366. *See* Martin Gebauer, *Uniform Law, General Principles and Autonomous Interpretation*, UNL L. REV. 683, 685–87 (2003).

there is “the tendency by interpreters to turn to their familiar and nonuniform, norms of domestic law in the interpretation of international standards.”³⁶⁷

To ensure this issue does not arise with the interpretation and application of a convention on data privacy, the convention should delegate appropriate supervisory authorities. One of the recognized strengths of the EU Directive was its requirement that each Member State set up a regulatory authority that is independent from any national influence for individuals to bring claims.³⁶⁸ As discussed earlier, one of the ECJ’s reasons for invalidating the Safe Harbor was the concern that the United States does not currently provide individuals with a means for seeking judicial redress of data-privacy issues.³⁶⁹ Although the Privacy Shield provides for new avenues of redress, it still does not provide for an authority that is solely dedicated to the protection and enforcement of data-security practices. Therefore it continues to place agencies in a position where data-privacy concerns are competing for their attention amongst a plethora of other issues. By requiring signatories to set up independent data protection authorities, this concern will be eliminated for any country who becomes a member to the convention. Furthermore, requiring these authorities to be independent from national influence will ensure that data-privacy issues get the full attention they require, thus avoiding the issues seen with the FTC.³⁷⁰ Just as is provided for by the EU Directive, claims may be appealed from these authorities up to the courts of each country.³⁷¹ GPEN should play a role in this process as well, either operating as a commission itself or creating one to act as a higher authority that can investigate cases and watch over enforcement of the law, as well as provide advice to these authorities in a similar manner to the way the Working Party has provided advice regarding the EU Directive. This commission should punish violations of

367. Ferrari, *supra* note 359, at 24–25.

368. Council Directive 95/46, *supra* note 38, art. 28.

369. *Schrems*, 2015 E.C.R. 117/15.

370. Data-privacy issues must compete with other areas of the law that the FTC enforces, which inevitably leads to a lack of necessary attention to the data-privacy issues. See Tene, *supra* note 40, at 1225.

371. Council Directive 95/46, *supra* note 38, art. 28.

the convention with sanctions, similar to what the Safe Harbor Program had called for.³⁷²

CONCLUSION

The current issues the international community faces due to the varying data-privacy laws can only be alleviated by creating a uniform binding instrument. Past efforts toward creating recommendations and providing countries with the flexibility to draft their own laws have continued to result in inconsistencies and widely disproportionate laws that have failed to facilitate cooperation. Just as the EU recognized the need for a binding instrument within its own borders, the members of the international community looking to participate in the free flow of data need to recognize that a convention on data privacy would substantially mitigate the problems associated with a lack of uniform law.

Drafters of a new data-privacy convention should utilize the CISG to their advantage, as it provides practical benefits that can be transferred over into the realm of data privacy. By modeling a data-privacy convention on the CISG, drafters can utilize a successful framework by adopting its strengths and building upon its weaknesses, which have generated years' worth of research and scholarship regarding how to improve upon these areas. The convention on data privacy should utilize the development process by which the CISG was created, using GPEN as a similar devise as UNCITRAL, but utilizing the OECD instead of the U.N. as a forum. The current state of data privacy calls for a need for a uniform data-privacy law to facilitate companies' ability to transfer data and therefore do business in foreign nations, just as the CISG was needed in order to facilitate companies to enter into contracts with foreign parties and therefore do business in foreign nations. The element of timing needs to be taken advantage of and the drafting process must start immediately. Just like the CISG, this convention must be automatic, thus allowing for consumer protection. The terms should be simple, clear, and practical just like those of the CISG in order to stay current with technology's progression, and a gap-filling mechanism should be used to ensure the

372. The Safe Harbor called for sanctions to "be sufficiently rigorous to ensure compliance by the organization." U.S.-EU SAFE HARBOR FRAMEWORK, *supra* note 186 at 6.

currentness continues. Luckily, the presence of commonly accepted data-privacy principles will help this convention avoid the weaknesses the CISC faces with its gap-filling mechanism. Finally, supervisory authorities should be created just as they were in the EU in order to uphold this convention and facilitate its interpretation and application.

By creating this convention, the international community can create a mechanism whereby the free flow of data around the world can be facilitated. By doing so, technological innovation will be promoted, the freedom of information can be preserved, and transfers of data can be used to enhance the global economy, yielding increased prosperity instead of increased tensions amongst different nations around the world.

*Morgan A. Corley**

* B.A., University of Maryland, College Park (2013); J.D., Brooklyn Law School (Expected 2016). I would first like to thank the editors of the Brooklyn Journal of International Law for the admirable effort and support they have shown me during the publication of this Note. I would also like to thank my friends for the love and encouragement they have provided throughout this process. Additionally, I would like to thank my sister, Kymberly Corley, for constantly challenging me to think outside of the box and inspiring me to be creative throughout this undertaking. Finally, I would like to thank my parents, Robin and David Corley, for their love and guidance they continue to give me, and for the enormous sacrifices they have made so that I could fulfill my dreams. All errors or omissions are my own.