Catholic University Journal of Law and Technology

Volume 27 | Issue 1 Article 5

2018

The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?

Matthew Humerick

THE TORTOISE AND THE HARE OF INTERNATIONAL DATA PRIVACY LAW: CAN THE UNITED STATES CATCH UP TO RISING GLOBAL STANDARDS?

Matthew Humerick[*]

> *"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies."*[1]

[*] J.D. 2018, *magna cum laude*, Michigan State University College of Law; B.S.B.A. 2015, Western New England University. The author is a licensed attorney in Massachusetts and hopes to obtain work in the data privacy or business law fields.

[1] Steven Levy, *Bill Gates and President Bill Clinton on the NSA, Safe Sex, and American Exceptionalism*, WIRED (Nov. 12, 2013, 6:30 AM), https://www.wired.com/2013/11/bill-gates-bill-clinton-wired/ (quoting Bill Gate's response to the discovery of widespread data collection by the NSA and how surveillance and security must strike a balance).

The evolution of information technology catalyzes economic globalization as larger quantities of data are easily stored, processed, and circulated across the globe in a matter of seconds.[2] Online shopping, also known as e-commerce, has contributed significantly to the issue of data privacy because records are instantly updated with a large breadth of customer information.[3] While the simple disclosure of a name, address, phone number, and credit card number may not seem like much information, this basic data enables algorithms to compile more complete personal data profiles.[4] For example, a website with registered accounts is able to track consumer search and purchase histories.[5] Predictive algorithms process information to predict buyer behavior, such as what products a consumer is likely to purchase as well as the most effective type, and placement, of advertisements.[6] These activities have become the norm, as consumers are either numb or oblivious to the information they consent to disclosing to companies.[7] After all, the only way a consumer can utilize online

---

2 Gao Shangquan, *Economic Globalization: Trends, Risks and Risk Prevention*, U.N. Doc. ST/ESA/2000/CDP/1, at 1 (2000), http://www.un.org/en/development/desa/policy/cdp/cdp_background_papers/bp2000_1.pdf (discussing the rapid growth of technology and its ability to cut costs and expedite communications as well as providing statistics to show how even sixteen years ago, technology was beginning to shape the global economic landscape); *see also* Nicolas Pologeorgis, *How Globalization Affects Developed Countries*, INVESTOPEDIA (Mar. 6, 2017, 2:59 PM), http://www.investopedia.com/articles/economics/10/globalization-developed-countries.asp (explaining how globalization has continued to increase as newer, more efficient technologies promote international trade).

3 *The Importance of Gathering and Using Demographic Data for Fulfillment*, FLOSHIP, http://www.floship.com/importance-gathering-using-demographic-data-fulfillment (last visited Nov. 13, 2018) (detailing how online shopping and the growth of e-commerce has rapidly expanded the amount and types of data companies can instantaneously collect and analyze to predict consumer spending, to target advertising, and to improve customer relations, among other many benefits) [hereinafter *Demographic Data*]; *see also* Adam C. Uzialko, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (Aug. 3, 2018, 7:25 AM), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (discussing means of data collection and potential business uses for consumer data).

4 *Demographic Data*, *supra* note 3 (stating that simple purchase data is the surface level of information that companies can collect as technology and analytics continue to improve).

5 *See* Nicole Fallon, *Boosting Customer Loyalty with Big Data*, FOX BUS. (Apr. 28, 2014), http://www.foxbusiness.com/features/2014/04/28/boosting-customer-loyalty-with-big-data.html (reporting the benefits of customer loyalty programs, the emphasis of companies on targeting repeat buyers, and the ability to track and predict purchase tendencies).

6 Charles Duhigg, *How Companies Learn Your Secret*, N.Y. TIMES MAG. (Feb. 12, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0.

7 Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-

services is to agree to a company's privacy policies, accept the internet cookies, and to supply their personal information.[8] However, until a data breach occurs, consumers continue to carelessly accept these agreements to information privacy.[9]

Companies store large quantities of personal data that can easily be traced back to individuals.[10] Corporate data mining and collecting is a global practice, so governments must ensure the protection of consumer data beyond industry and individual company levels.[11] With the continual growth of e-commerce, the spread of consumer information transcends national borders.[12] After all, consumer data concerns citizens from around the world, so each government must do its part in ensuring its protection.[13]

In 2000, the European Union and the United States, as two of the largest economic markets in the world, entered into the U.S.–E.U. Safe Harbor Agreement.[14] Under this Agreement, the European Union and the United States reconciled existing gaps between the European Union's data protection

---

and-trust (discussing how companies use general consumer consent to gather as much consumer data as possible, even if not useful at the present time, and how customers do not know standard data collection practices or the breadth of the data they are giving up).

8 *Id.*

9 *New FireEye Research Reveals the Impact of High-Profile Security Breaches on U.S. Consumers' Trust of Brands*, FIREEYE (May 12, 2016), http://investors.fireeye.com/releasedetail.cfm?ReleaseID=970718 (releasing studies on consumer reactions and attitudes toward large data breaches); *see also* Zach Walker, *The Impact of Data Breaches and Customer Loyalty*, RIPPLESHOT BLOG (Dec. 17, 2015), http://info.rippleshot.com/blog/data-breaches-and-customer-loyalty (discussing prevalence and dangers of data breaches).

10 Morey et al., *supra* note 7.

11 Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 356 (2015) (introducing the concept of data protection and the ways in which consumers value its collection, use, and protection against companies across the world; companies that have evolved in storing, processing, and selling data to third-parties, or giving it to the government for security purposes); Courtney M. Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER (Dec. 23, 2015), http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ (explaining how the E.U.'s GDPR increases protections for its citizens).

12 John C. Eustice, *Flying into the cloud without falling: understanding the intersection between data privacy laws and cloud computing solutions*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing (last visited Sept. 22, 2018).

13 Brookman, *supra* note 11, at 357 (describing the responses of nations around the world to personal data as it becomes easier to access); Bowman, *supra* note 11.

14 *Commission Staff Working Document on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related FAQs Issued by the U.S. Department of Commerce*, Commission Decision 2000/520/EC, 2000 O.J. (L 215) 8 [hereinafter *Safe Harbor]*.

requirements[15] and the United States' privacy laws to allow for the legal transfer of personal information collected in Europe of European citizens.[16] On October 6, 2015, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement in the landmark case of *Maximillian Schrems v. Data Protection Commissioner*.[17] The Court of Justice emphasized in its holding the significant data privacy and data protection policy gaps, and the differences that exist between the European Union and the United States.[18] In the European Union, citizens possess fundamental rights to both privacy[19] and the protection of personal data.[20] The E.U. has embraced this concept through its adoption and continual evolution of legislation that guarantees individual's privacy and data protection from misuse by the government and companies alike.[21] In contrast, there is no explicit individual right to consumer data privacy in the United States nor an overarching regulatory scheme.[22]

In 2014, under the Safe Harbor Agreement, the European Union and the United States participated in transatlantic trade valued over $1.09 trillion and approximately $4 trillion in parallel trade of stocks and investments.[23] The investment of United States based companies into the European economy, and

---

15 *Id*. at 10.

16 *Id*. at 7; MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1 (2016) (giving an overview of U.S. and European data privacy laws and a history of their interaction).

17 Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN (invalidating the Safe Harbor Agreement between the European Union and the United States in a case arising out of an Irish Facebook user's suit claiming an unlawful transfer of his personal information to Facebook servers located in the United States due to inadequate data protection against the United States' National Security Agency's surveillance practices).

18 *Id.*

19 Charter of Fundamental Rights of the European Union art. 7, Oct. 26, 2012 O.J. (C 326) 393, 397.

20 *Id*. at art. 8.

21 Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1973 (2013) (discussing how the European Union's proactive approach to privacy and its continual efforts for improvement has caused countries outside the E.U. to develop similar stringent approaches to privacy protection).

22 Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 668 (1999) ("Individual privacy in the United States is protected through a combination of constitutional guarantees, federal and state statutes, regulations, and voluntary industry codes of conduct that apply to the public and private sectors in different ways.").

23 *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: Joint Hearing Before the Subcomm. on Commerce, Mfg., and Trade and the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce*, 114th Cong. 21 (2015) (statement of Dr. Joshua P. Meltzer, Senior Fellow, Global Economy and Development program at the Brookings Institute).

vice versa, drove this economic boom where "[s]ixty-one percent of U.S. imports from the EU and 33 percent of EU imports from the U.S. consist of intra firm trade."[24] Roughly 4,500 U.S. companies operated under the Safe Harbor Agreement to allow for the transatlantic data transfers.[25] Due to such heavy reliance on the Safe Harbor, its invalidation has put the international economy in jeopardy and companies are left wondering whether they are adequately protected from liability in conducting transatlantic data transfers.[26] Without the Safe Harbor Agreement's protections, United States based companies must consider alternative mechanisms to ensure compliance with the European Union's stringent standards or otherwise face harsh liability.[27]

The European Union and the United States recently entered into the E.U.–U.S. Privacy Shield to restore privacy protection in transatlantic data flows.[28] While quickly enacted with stronger data protections, stark contrasts remain between data protection regulations in the European Union and the United States.[29] The European Union is the global standard for international privacy law, and is continuously developing, while the United States continues to

---

24 *Id.* at 23 (stating these statistics dwarf those of other United States trade partners where "intra firm trade as a share of U.S. imports from the Pacific Rim (37.2 percent), and South/Central America (37 percent)" account for a much smaller percentage of international trade).

25 Weiss & Archick, *supra* note 16.

26 *European Court of Justice Invalidates U.S.-EU Safe Harbor Agreement*, BARNES & THORNBURG LLP (Oct. 9, 2015), http://www.btlaw.com/data-security-and-privacy-and-ediscovery-data—document-management-law-alert—-european-court-of-justice-invalidates-us-eu-safe-harbor-agreement-10-09-2015.

27 Brian McCormac, *Invalidation of Safe Harbor, EU to US Data Security Measures Tested, Failed*, BROWN WINICK (Mar. 4, 2016), http://www.brownwinick.com/news-blogs/legal-news/invalidation-of-safe-harbor-eu-to-us-data-security-measures-tested-failed.aspx (recommending companies take proactive steps to protect their liability while continuing to conduct transatlantic data transfers following the Safe Harbor Agreement's invalidation. Steps include: reviewing data transfer processes using strict privacy principles, implementing the E.U. Model Contract Clauses or Binding Corporate Rules (BCRs) as alternative adequacy measures, and ensuring that company privacy policies are accurate and complied with); *see also European Court of Justice*, *supra* note 26 (providing recommendations on how companies can protect themselves from liability in the aftermath of the Safe Harbor Agreement's invalidation); Francoise Gilbert, *EU General Data Protection Regulation: What Impact For Business Established Outside the European Union*, 19 NO. 11 J. INTERNET J. 3, 3-6 (2016) ("Today, less than 100 companies have sought and obtained approval of their BCRs, even though using BCRs as a method to legalize cross-border transfers has been available for approximately 10 years").

28 *See* European Commission Press Release IP/16/216, EU 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.

29 *See* Paul M. Schwartz & Karl Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 117, 120 (2017) (outlining policy differences between U.S. and E.U. despite the effort behind the implementation of the Privacy Shield).

embrace an antiquated, ineffective approach.[30] Additionally, with the United States' view towards international cooperation shifting, negotiations will likely become more tense and result in significant delays.[31] For companies, this means that international data transfers and trade will continue to take place without the security of agreements that bridge the gap between internal data privacy laws.[32] Congress must acknowledge that it is unsustainable to continue to simply contract around higher global standards through trade agreements destined for failure.[33] Congress should ease the Federal Trade Commission's (FTC) burden to promulgate rules within the data privacy context.[34] However, even if Congress does not ease the burden, the FTC must promulgate a rule that establishes a standard for general data protection and requires industry agencies to monitor data protection compliance throughout the States.[35]

---

30 *See generally* Dan Jerker B. 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 (2014) (discussing the reach that European and U.S. privacy law has on the rest of the world, how the emergence of rapid technological innovation shapes global data privacy, and how international data privacy law is likely to progress).

31 *See* Toluse Olorunnipa et al., *Trump Revamps U.S. Trade Focus by Pulling Out of Pacific Deals*, BLOOMBERG (Jan. 23, 2017, 7:25 PM), https://www.bloomberg.com/politics/articles/2017-01-23/trump-said-to-sign-executive-order-on-trans-pacific-pact-monday (showing the Trump presidency has taken an inward, protectionist approach. Within a week of taking office, President Trump has taken executive action to withdraw the United States from the Trans-Pacific Partnership (TPP) and vowed to reevaluate the North American Free Trade Agreement (NAFTA)).

32 *See* Mark Scott, *U.S. and Europe Fail to Meet Deadline for Data Transfer Deal*, N.Y. TIMES (Feb. 1, 2016), at B1 (discussing how in the absence of an agreement between the European Union and the United States, companies are relying upon untested contractual measures to reduce liability in data transfers. Concerns over foreign legal remedies and the use of transferred data have highlighted key areas of concern and discrepancy between the foreign policies).

33 *See also* Eric Shimp, *Data Privacy in the Transatlantic Trade Agreement? US-EU Ponder the Way Forward*, ALSTON & BIRD: PRIVACY & DATA SEC. BLOG, http://www.alstonprivacy.com/data-privacy-in-the-transatlantic-trade-agreement-us-eu-ponder-the-way-forward (last visited Sept. 23, 2018) (discussing how data protection and privacy concerns have already arisen in T-TIP negotiations); *see generally* Ioanna Tourkochoriti, *The Snowden Revelations, The Transatlantic Trade and Investment Partnership and the Divide Between U.S.-E.U. in Data Privacy Protection*, 36 U. ARK. LITTLE ROCK L. REV. 161 (2014) (discussing how an international lack of trust in the United States' legal emphasis on privacy is threatening the negotiations for increased trade partnerships because separate agreements are necessary to protect the European Union's fundamental right to privacy).

34 Jugpreet Mann, *Small Steps for Congress, Huge Steps for Online Privacy*, 37 HASTINGS COMM. & ENT. L.J. 365, 388 (2015).

35 *See* Alex Y. Seita, *Globalization and the Convergence of Values*, 30 CORNELL INT'L L.J. 429, 472-76 (1997) (discussing how the increasing globalization of trade and the importance of data collection serve as impetuses for the United States to adopt federal privacy standards to ease international data transfer relations); *see also* Amanda C. Border,

Part I of this Note provides an overview of the sectoral privacy law landscape currently in the United States. Part II discusses privacy law in the European Union and how its development of the General Data Protection Regulation (GDPR) is creating a quasi-global standard for data protection. Part III forecasts the long-term impact that the GDPR and rising global data privacy standards will have on U.S. data privacy laws and international data transfers. Additionally, Part III argues that the FTC must promulgate a rule to create a uniform set of data standards across the states and form data compliance agencies to oversee domestic and international affairs.

I. THE ROLE OF PRIVACY AND DATA PROTECTION IN THE U.S.

Although the right to privacy is not explicitly enumerated in the Constitution, judicial and legislative interpretations have acknowledged that individuals have certain privacy rights.[36] While this right has not been extended by the Court to protect private personal information (PII),[37] several states have enumerated a right of consumer data and personal privacy within their constitutions.[38] This attitude toward personal privacy rights has formed the basis for its protection in the United States.[39] Rather than a preventative, singular rule of law, data protection in the United States is governed by a reactive patchwork regulatory system.[40] Although federal statutes govern the protection of consumer data in

---

Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States, 35 SUFFOLK TRANSNAT'L L. REV. 363, 384 (proposing that "the United States should shift away from its "piecemeal approach" to data privacy.").

36 Roe v. Wade, 410 U.S. 113, 152 (1973) (demonstrating how the Supreme Court has relied on interpretations of the Bill of Rights to conclude that "a right of personal privacy, or a guarantee of certain areas or zones of privacy [do] exist under the Constitution"); *see also* Katz v. United States, 389 U.S. 347, 360 (1967) (developing a "reasonable expectation of privacy" test to gauge whether a person has a right to privacy, based on having (1) an actual expectation of privacy that (2) society deems reasonable and is prepared to recognize); *see also* Privacy Act of 1974, 5 U.S.C. § 552(a) (1974) (noting that a "right to privacy is a personal and fundamental right protected by the Constitution of the United States").

37 Tan, *supra* note 22, at 669.

38 *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); CAL. CONST. art. I, § 1 ("All people are by their nature free and independent and have inalienable rights. Among these are enjoying and defending liberty . . . and privacy.").

39 *See generally* Tan, *supra* note 22, at 662-63 (noting that nearly every country recognizes a right to privacy; however, differences amongst comprehensive laws are apparent based on the level of emphasis that individual countries place on this right).

40 Ieuan Jolly, *Data protection in the United States: overview*, PRACTICAL L. (July 1, 2017), http://us.practicallaw.com/6-502-0467 (emphasizing that rather than enacting a single federal law, the United States utilizes "a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another."); *see also* Tan, *supra* note 22, at 671 ("Presently, there is no comprehensive law in the United States guaranteeing privacy rights in personal information. There are, however, various privacy

particular sectors, such as private health information,[41] financial information,[42] and electronic communications,[43] many industries fall outside the scope of these regulations.[44] Instead, a system of company self-regulation governs consumer data protection in the United States.[45] Privacy law in the U.S. is primarily enforced by the FTC[46] and state privacy laws.[47]

A. The FTC and its Role on Data Protection in the United States

The FTC was not originally formed to function as a privacy protection agency; however, that is now one of its primary duties.[48] The FTC's mission

---

and security statutes that address specific privacy needs.").

41 Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1302(a) (2012) (explaining that the power to regulate the governing of privacy and medical regulations is given to the Department of Health and Human Services under the Act).

42 *See* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802 (2012) (requiring privacy notice and opt-out rights for consumers when financial institutions attempt to share personal data with other companies).

43 Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 (2002) (protecting personal information on the Internet from unauthorized government surveillance).

44 Stephen Cobb, *Data privacy and data protection: U.S. law and legislation*, ESET 6 (2016) (stating large sectors, such as airline reservation data, sales and marketing prospect databases, and library borrowing records fall outside the scope of federal privacy protection laws); *see also* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2233 (2015) "The FTC has filled gaps when a number of large industries have not been regulated by federal data protection statutes.".

45 Tan, *supra* note 22, at 674 (detailing how the United States' regulatory system for online privacy protection consists of self-regulation where companies establish their own policies).

46 Jolly, *supra* note 40, at 1, 17 ("The FTC is the primary U.S. enforcer of national privacy laws" and "has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data.").

47 *See id.* at 3 ("There are many laws at the state level that regulate the collection and use of personal data."); Cal. CIV. CODE § 1798.150(a)(1) (2018) (discussing the newly enacted California Consumer Privacy Act of 2018 which demonstrates how privacy law is enforced on the state level by stating that "any consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" may institute certain civil actions).

48 Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41-58 (2006)) (stating that the FTC was primarily formed to "prevent persons, partnerships, or Corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce"); Clayton Antitrust Act of 1914, Pub. L. No. 63-212, 38 Stat. 730 (codified as amended at 15 U.S.C. §§ 12-27 (2006) and 29 U.S.C. §§ 52-53 (2006)) (showing that one of the primary purposes of the FTC was to prevent the acquisition of "the whole or any part of the assets of one or more persons engaged in commerce or in any

does not specifically address the protection of consumer data privacy; however, its power to pursue companies for unfair and deceptive practices now includes data practices.[49] Modern interpretations of the Federal Trade Commission Act (FTC Act) prohibit unfair or deceptive practices with regard to online and offline privacy, data security policies of the company, and the company's failure to safeguard consumers' personal information.[50] While the FTC's "unfair and deceptive" authority under § 5 of the FTC Act broadens the FTC's jurisdiction and scope of authority,[51] certain industries remain exempt.[52] Only the FTC can enforce the FTC Act, and therefore, private causes of action are not possible.[53] Instead, the government and U.S. consumers must rely upon FTC orders to obtain injunctive remedies, and fine companies accordingly.[54] While advocates

---

activity affecting commerce," when the intention of the person seeking to acquire such assets was to lessen competition or to create a monopoly); Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 814-15 (2011) (explaining that the "FTC was originally created in 1914 in order to protect competition among businesses" and the establishment of the FTC occurred concurrently with the Clayton Act, which focused on antitrust law, to ensure that businesses operated on a level playing field).

49 *See About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Oct. 20, 2016) (stating that the FTC's mission is to prevent business practices that are "anticompetitive, deceptive, and unfair" to consumers, to enhance "informed consumer choice and public understanding of the competitive process", and to accomplish this "without unduly burdening legitimate business activity"); *Division of Privacy and Identity Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited Sept. 23, 2018) (discussing that in response to growing concerns regarding data privacy, the FTC created a subdivision focused solely on data privacy issues).

50 *See* Serwin, *supra* note 48, at 814 (explaining that through amendments to section 5 of the FTCA in 1938, "the FTCA was extended to cover consumers, primarily through the addition of authority to address unfair and deceptive acts or practices," which has been interpreted to include safeguarding personal information); Jolly, *supra* note 40, at 1 ("The Federal Trade Commission Act (15 U.S.C. §§41-58) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies."); Hartzog & Solove, *supra* note 44, at 2235 (explaining how under the FTC Act, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" and when companies fail to live up to promises made in their privacy policies, the FTC considers this a deceptive trade practice that can be prohibited under the Act).

51 *See* Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1) (2012) (stating that under the relevant section of the act "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful" and the FTC has the power to regulate said methods and practices).

52 *See* 15 U.S.C. § 45(a)(2) (explaining that examples of industries outside the scope of the FTC's § 5 authority include financial institutions, airlines, non-profits, and telecommunications carriers, among others).

53 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFO. PRIVACY L. 848-49 (Erwin Chemerinsky et al. eds., 5th ed. 2015).

54 *See Injunction*, BLACK'S LAW DICTIONARY (10th ed. 2009) (defining an injunction as "a court order commanding or preventing an action"); *see* 15 U.S.C. § 45 (l) (stating that

for the federal regulation of data privacy and security, separate from the FTC, have introduced numerous bills to Congress, such as the Personal Data Privacy and Security Act of 2014;[55] the Data Security Act of 2014;[56] and the Data Security Act of 2015,[57] Congress continues to balk at passing federal data privacy legislation.[58] Since the invalidation of the Safe Harbor Agreement, the United States' only recourse to buffering its data privacy law regime has been through the enactment of the Judicial Redress Act of 2015,[59] which primarily concerns government use of personal data.[60]

"any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States. Each separate violation of such an order shall be a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense. In such actions, the United States district courts are empowered to grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission"); *see* 15 U.S.C. § 53 (explaining that "whenever the Commission has reason to believe . . . that any person, partnership, or corporation is violating, or is about to violate, any provision of law enforced by the Federal Trade [Commission] . . . may bring suit in a district court of the United States to enjoin any such act or practice," with some limitations); *see* SOLOVE & SCHWARTZ, *supra* note 53 (describing how the FTC cannot subject first-time offending companies to fines under § 5. Instead, the FTC can only issue fines when a company violates an existing consent decree previously entered stemming from an earlier § 5 violation).

55 Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2d Sess. 2014) (describing the purpose of the bill was to "prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.").

56 Data Security Act of 2014, S. 1927, 113th Cong. (2d Sess. 2014) (stating the purpose of this bill was to "protect information relating to consumers, to require notice of security breaches, and for other purposes.").

57 Data Security Act of 2015, S. 961, 114th Cong. (1st Sess. 2015) (revising Data Security Act of 2014 but with the same stated purpose).

58 *See* J. Caleb Boggs III. & Lauren Donoghue, *Congress taking action to protect data security*, LEXOLOGY (Jan. 21, 2014), http://www.lexology.com/library/detail.aspx?g=c5f0404e-d581-4911-aa50-eeea8921b60d; Conor Dougherty, *Push for Internet Privacy Rules Moves to Statehouses*, N.Y. TIMES (Mar. 26, 2017), https://www.nytimes.com/2017/03/26/technology/internet-privacy-state-legislation-illinois.html.

59 Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2016) (authorizing the Attorney General to designate foreign countries or specific organizations whose citizens may then bring civil suits under the Privacy Act of 1974 against certain U.S. government agencies for unlawful disclosures of records transferred from a foreign country pursuant to criminal prosecution).

60 Eric Geller, *Everything You Need to Know About the Big New Data-Privacy Big in Congress*, DAILY DOT (Feb. 24, 2016, 2:28 PM), http://www.dailydot.com/layer8/what-is-the-judicial-redress-act-europe-data-privacy-bill; H. Jacqueline Brehmer, Data Localization:

The FTC has developed accountability standards that delineate best practices for companies using consumer data within their specific industry.[61] However, companies do not have to accept these practices due to their voluntary nature.[62] While the FTC can prescribe interpretive rules and general standards,[63] it has minimal practical authority to make binding rules.[64] From a practical standpoint, the FTC's rulemaking authority is a highly burdensome procedural process known as Magnuson-Moss[65] authority.[66] Due to this burdensome process, the FTC has not used its rulemaking power in over thirty-two years, leaving companies and industries with general policy statements and interpretive rules.[67] Companies that accept these standards are accountable to the FTC and are liable for acts or practices deemed unfair or deceptive under the FTC Act.[68] Non-

---

The Unintended Consequences of Privacy Litigation, 67 AM. U. L. REV. 927, 941-42 (2018) (stating the Judicial Redress Act expands civil redress of surveillance by federal agencies to foreign nationals).

61 THE PRIVACY, DATA PROTECTION AND CYBERSECURITY L. REV. 148 (Alan Charles Raul ed. 2014) (explaining these standards have led to best practices like the opt-out for cookies and the "about advertising" icon); *see* Privacy & Data Security Update (2016), FTC, Oct. 22, 2018, https://www.ftc.gov/reports/privacy-data-security-update-2016#rules (detailing the FTC's various discussions and reports on how businesses should operate to protect consumer data under the "Consumer Education and Business Guidance" section).

62 THE PRIVACY, *supra* note 61.

63 Federal Trade Commission Act of 1914, 15 U.S.C. § 57a(a)(1)(B) (2006) (granting the FTC power to prescribe interpretive rules and general statements of policy, but not those regarding "the regulation of the development and utilization of the standards and certification activities pursuant to this section").

64 15 U.S.C. § 57a(a)(2) (stating that the "Commission shall have no authority under this subchapter, other than its authority under this section, to prescribe any rule with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title)").

65 Magnuson-Moss Warranty Act – Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (affirming the FTC's legislative authority to make rules, subject to first conducting an industry wide investigation, preparing draft staff reports, proposing a rule, and engaging in a series of public hearings, including cross-examination).

66 Beth DeSimone & Amy Mudge, *Is Congress Putting the FTC on Steroids?*, SELLER BEWARE BLOG (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html; s*ee also* Magdalena Gathani, *Internet of Things Report: The FTC Overstepped its Agency Rulemaking Authority*, 9 BUS. PUBL. ADMIN. STUD. 27, 27-8 (2016), https://www.bpastudies.org/bpastudies/article/viewFile/203/380 (describing the FTC's current rulemaking authority, and how some view the issuing of best practices and recommendations as overstepping the FTC's authority).

67 Jon Leibowitz, Chairman, Fed. Trade Comm'n, Remarks at the Association of National Advertisers: Advertising Law and Public Policy Conference (Mar. 18, 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/association-national-advertisers-advertising-law-and-public-policy-conference-prepared-delivery/100318nationaladvertisers.pdf ("The requirements to promulgate a rule under [the Magnuson-Moss Act] are so onerous that the agency has not proposed a new [Magnuson-Moss Act] rule in 32 years.").

68 THE PRIVACY, *supra* note 61; *Cases and Proceedings*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings (last visited Sept. 23, 2018) (showing

compliant acts or practices include inadequate protection of consumer personal data, failure to post or comply with company privacy policies, and lack of notice for privacy policy revisions.[69] The FTC uses two models to promote consumer privacy: (1) a notice-and-choice model, characterized by the fair information practice principles[70] (2) and a harm-based approach.[71]

In 2000, the FTC first used the notice-and-choice model in an effort to have Congress require businesses to comply with the Fair Information Practice Principles.[72] The FTC proposed that Congress enact several substantive principles to promote consumer privacy in organizational processes, including "data security, reasonable collection limits, sound retention and disposal practices, and data accuracy."[73] Though unsuccessful in convincing Congress to enact legislation to cover this area, the FTC has used its authority under Section 45 of the FTC Act to promote consumer data protection.[74]

Section 45 of the FTC Act prohibits unfair and deceptive practices.[75] Deceptive practices are found when there is a "material" misleading representation, practice, or omission, when viewed from the perspective of a

---

all actions filed by the FTC against corporations under its Section five authority, including those specifically for privacy violation; *see, e.g.*, Atl. Ref. Co. v. Fed. Trade Comm'n, 381 U.S. 357, 367 (1965) (finding that 'unfair practices' is a flexible and evolving concept, best left to FTC interpretation so that it may bring future suits to hold companies accountable for their actions).

69 Jolly, *supra* note 40.

70 Privacy Policy Guidance Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. Dep't of Homeland Sec., on The Fair Information Practice Principles: Framework for Privacy Policy (on file with author) (describing the Fair Information Practice Principles (FIPPs) that govern the use of personally identifiable information (PII) are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The memorandum elaborates on the meaning of each principle).

71 Serwin, *supra* note 48, at 817-22 (discussing the evolution of the FTC's role in policing the right to privacy. The right to protection of privacy and information security was not a reasoning for the enactment of the Federal Trade Commission Act. § 5 of the FTC Act embraced privacy issues as another way for the FTC to combat unfair and deceptive practices).

72 FTC Staff Report on Internet of things: Privacy & Security in a connecting world, FED. TRADE COMM'N, at v (Jan. 2015).

73 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at i, vii (2012).

74 15 U.S.C. § 45 (2006) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."); FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017, at 1-8 (2017) (citing lawsuits and enforcement actions brought by the FTC in 2017 to protect consumer data privacy both domestically and abroad).

75 15 U.S.C. § 45(a)(1).

reasonably acting consumer.[76] When examining the consumer's likely detriment upon reliance of a deceptive act or practice, there is often a presumption of injury and actual harm.[77] Under this model, deception serves as the basis for the FTC's authority to regulate consumer privacy protection in all industries not specifically targeted by federal law.[78] Under Section 45, the FTC is able to bring actions against companies for using deceptive practices. There are two ways in which the FTC can bring suit: (1) either on its own or (2) upon referrals, from either E.U. data protection authorities or third-party private dispute resolution providers.[79] Critics have claimed that this notice and choice enforcement model is impractical because it results in implementations of lengthy, incomprehensible privacy statements which do not benefit consumers, and are not responsive to a rapidly changing technological environment.[80]

The FTC has adopted the harm-based approach as the primary enforcement model.[81] This model shifts from a focus on deception to a focus on unfairness, where an emphasis is placed on the likelihood of substantial injury rather than on business practices.[82] Application of the harm-based enforcement model has resulted in the development of four privacy tort causes of action: (1) intrusion upon seclusion; (2) appropriation of name or likeness; (3) public disclosure of private facts; and (4) dissemination of false information.[83] This privacy tort cause of action model has been criticized for its inability to address all potential privacy harms and to adapt to the evolving technological environment.[84] The following subsections detail the FTC's roles in data privacy and protection as

---

76 Letter from James C. Miller III, Chairman of the Fed. Trade Comm'n, responding to an inquiry on FTC enforcement policy for deceptive acts and practices from Congressman John D. Dingell, Chairman of the House Comm. on Energy Commerce (Oct. 14, 1983) (on file with author), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

77 *Id*.

78 15 U.S.C. § 45.

79 *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: Joint Hearing Before the Subcomm. on Commerce, Mfg., and Trade and the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce*, 114th Cong. 21 (2015) (statement of Dr. Joshua P. Meltzer, Senior Fellow, Global Economy and Development program at the Brookings Institute).

80 Serwin, *supra* note 48, at 816; *see also* FED. TRADE COMM'N, *supra* note 73, at 2.

81 Serwin, *supra* note 48, at 842-43.

82 Fed. Trade Comm'n v. Accusearch, Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (quoting 15 U.S.C. § 45(n) (2006) in explaining that "[t]o be 'unfair,' a practice must be one that '[1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition.").

83 THE PRIVACY, *supra* note 61, at 288.

84 Serwin, *supra* note 48, at 816-20.

(1) a self-regulating body and (2) a foreign ambassador for data privacy.[85]

1. The FTC as a Self-Regulating Body

In a legal landscape riddled with gaps, the FTC rules have been compared to a privacy common law.[86] Though the law does not require companies to enact specific practices or privacy policies, the FTC can use its authority under Section 45 to bring actions against companies for unfair and deceptive practices.[87] The FTC can only bring suits against companies for Section 45 violations, which reduces the number of claims filed.[88] Additionally, the majority of FTC cases against companies end in settlements or consent decrees to cease deceptive and unfair practices.[89] While both parties benefit, it does not establish a privacy law foundation, based on case law nor establish precedent for future actions.[90] Instead, the FTC develops its power by relying on past settlements and practices to enforce its authority and to ensure that companies cease unfair and deceptive practices.[91] Companies have responded by developing their own state-of-the-art privacy practices beyond the scope of the FTC's requirements and more closely

---

85 *See infra* Sub-subsections I(A)(1), (2).

86 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586-88 (2014) (analyzing the FTC as a common law because it acts as the primary regulatory system for privacy within the United States); *see also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3rd Cir. 2015) (explaining that FTC may deem a practice unfair without needing to support finding with privacy common law when the practice causes substantial injury to customers).

87 Solove & Hartzog, *supra* note 86, at 600-04 (describing that as more regulatory schemes develop within various industries, the FTC receives additional authority to ensure that companies continue to operate under these principles in addition to the baseline protections already set by the FTC).

88 SOLOVE & SCHWARTZ, *supra* note 53.

89 Solove & Hartzog, *supra* note 86, at 604-64 (describing perhaps the biggest reason why companies seek to avoid court and to abide by the FTC is because Congressional action may occur if the FTC proves to be inadequate.); *see also* Shulamit Shvartsman, *To Settle or Not to Settle? That Is the Question*, LAWYERS.COM, http://research.lawyers.com/to-settle-or-not-to-settle-that-is-the-question.html (last visited Sept. 16, 2018) (explaining companies do not like to go to court because of high costs, bad publicity, wasted time, and the possibility for an admission of guilt).

90 Solove & Hartzog, *supra* note 86, at 588-89; Christina Ma, *Into the Amazon: Clarity and Transparency in FTC Section 5 Merger Doctrine*, 87 ST. JOHN'S L. REV. 953, 954 (2013).

91 *See* Solove & Hartzog, *supra* note 86, at 588-89 (illustrating that critics argue that the FTC has acted beyond its intended scope, resulting in a disposal of due process and legal constraints); *see also Now in Its 100th year, the FTC Has Become the Federal Technology Commission*, TECHFREEDOM (Sept. 26, 2013), http://techfreedom.org/now-in-its-100th-year-the-ftc-has-become-the/ (showing that coupled with a lack of rulemaking authority, the FTC's lack of binding precedent creates a regulatory regime based on discretionary exercises of power unbound by legal principles).

aligned to stricter global standards.[92] Companies anticipate future FTC actions and regulations, resulting in increased consumer-oriented protections, as opposed to compliance-oriented procedures.[93] In the United States, industries have embraced this self-regulating system because it does not mandate the stringent privacy standards found in data laws of the European Union and across the globe.[94]

2. FTC as an Ambassador

While the FTC is the main privacy power in the United States, Section 45 of the FTC Act restrains the FTC from expanding its jurisdiction to direct actions against international organizations, absent extreme circumstances.[95] According to the FTC Act, unfair or deceptive practices involving foreign commerce must rise to the level that they "cause or are likely to cause reasonably foreseeable injury within the United States,"[96] or must "involve material conduct occurring within the United States."[97] If international jurisdiction is found, the FTC can use any available remedy for unfair or deceptive acts, including restitution to relieve victims both domestic and abroad.[98]

The FTC also serves as an ambassador to discuss data privacy law with foreign nations.[99] In this capacity, the FTC is able to resolve disagreements between foreign leaders over privacy standard issues and sign memoranda of understanding to memorialize those agreements.[100] These memoranda of

---

92 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 269-70 (2011) (stating how companies have become increasingly proactive in ensuring international privacy compliance by adopting European standards, which provide for the highest level of consumer data protection); *see, e.g.*, *Amazon Privacy Notice*, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Aug. 29, 2017) (outlining Amazon's robust privacy policy, including the corporation's participation in "EU-US and Swiss-US Privacy Shield frameworks").

93 *See* Bamberger & Mulligan, *supra* note 92, at 273.

94 *See* Solove & Hartzog, *supra* note 86, at 593-94.

95 *See* Serwin, *supra* note 48, at 821 (explaining that the FTC can expand its jurisdiction into the international context only when needed to "prevent unfair methods of competition involving commerce with foreign nations unless the competition has a direct, substantial effect on U.S. commerce." The FTC can investigate and report to Congress on business conducts and foreign trade conditions that affect United States' commerce, but the FTC cannot take significant action against these foreign entities unless there are direct, substantial effects on commerce); *see also* Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41, 45(a), 46 (establishing the FTC, outlining the prohibition on various unfair business practices and granting the Commission regulatory authority).

96 15 U.S.C. § 45(a)(4)(A)(i).

97 15 U.S.C. § 45(a)(4)(A)(ii).

98 15 U.S.C. § 45(a)(4)(B).

99 THE PRIVACY, *supra* note 61, at 280.

100 *Id*. at 280-81.

understanding are made between the FTC, as a representative of the United States, and a foreign nation's governing privacy body, to recognize and reconcile privacy law differences.[101] Because the United States' view on privacy is in sharp contrast to that of its largest trade partner, the European Union, these memoranda are essential in dealing with European Union Member States.[102] For example, unlike the European Union, the United States does not place significant governmental restrictions in the international transfer of data.[103] In response, the FTC assumes the role of ensuring that companies under its jurisdiction comply with more stringent global standards.[104]

Safe Harbor violations in particular have been a top priority for international policy actions.[105] The FTC will continue to serve this role under the Privacy Shield.[106] Though the FTC has evolved into a broad privacy protection regulatory agency, it alone is insufficient to ensure the vitality of data transfers between the United States and the European Union.[107]

---

101 *Id*. at 281 (describing that these memoranda are "designed to promote increased cooperation and communication in both agencies' efforts to protect consumer privacy." The FTC has signed multiple memoranda of understanding including one with Ireland's Office of the Data Protection Commission in June 2013, and with the UK Information Commissioner's Office in March 2014. Without such memoranda, certain nations are unwilling to participate in data transfers because they are hesitant of any nation's privacy protections that are not "adequate" in the eyes of the European Union).

102 Memorandum of Understanding Between the United States Federal Trade Commission and the Information Commissioner's Office of the United Kingdom on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.K.-U.S., Mar. 6, 2014, Fed. Trade Comm'n, https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf (agreeing to enforce across borders, due to the "increase in the flow of personal information across borders [and] the increasing complexity and pervasiveness of information technologies.").

103 THE PRIVACY, *supra* note 61, at 280.

104 *Id*. at 280-81 (explaining that the FTC has an Office of International Affairs, which "works with competition and consumer protection agencies around the world to promote cooperation and convergence toward best practices."); *see also* Randolph W. Tritell, *Office of International Affairs*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs (last visited Sept. 23, 2018).

105 *See, e.g.*, *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed to Comply with International Safe Harbor Framework*, FED. TRADE COMM'N (Aug. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed.

106 *See Privacy Shield*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (last visited Sept. 1, 2018) (stating, "[the] FTC has committed to make enforcement of the [Privacy Shield] Framework a high priority").

107 *See generally* Brookman, *supra* note 11*; see also* Julian Hattem, *Rep. Issa takes aim at FTC 'inquisitions,'* THE HILL (July 24, 2014, 1:00 PM), http://origin-nyi.thehill.com/policy/technology/213242-issa-takes-aim-at-ftc-inquisitions (accusing the FTC of overstepping its boundaries in pursuing companies for privacy violations because, absent notice about the precise way a company should secure data, there is no way for

B. State Privacy Laws

Federal privacy laws address certain industries; however, the majority of consumer privacy protection laws are individualized at the state level, with California setting the standard.[108] Many states have begun to incorporate privacy as a core right by amending their state constitutions to enumerate individual rights to privacy.[109] States have also responded to the increased demands for privacy by enacting data breach laws that require notification to consumers in the event of data security breaches involving personal information.[110] Minnesota and Nevada have even gone so far as to protect consumer personal information by barring internet service providers from knowingly disclosing PII to third parties.[111] Even without privacy statutes, state attorneys general retain similar powers from the FTC to prohibit unfair or deceptive trade practices.[112] Increasingly, states have begun to embed a fundamental right to privacy within their legislation, including how such rights should be protected.[113] However,

businesses to tell if they are abiding by their stated security procedures).

108 CAL CIV. CODE § 1798.82 (2008); Jolly, *supra* note 40 (explaining that California was the first state to enact a data breach notification law, which generally requires that "any person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorized person.").

109 *E.g.*, Ariz. CONST. art. II, § 8 (1911) ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); *see also* 9 R.I. GEN. LAWS § 9-1-28.1 (2018) ("It is the policy of this state that every person in this state shall have a right to privacy…"); *see also Privacy Protections in State Constitutions*, NCSL (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (including a list of the ten states that have incorporated the right to privacy into their state constitutions and these provisions).

110 Jolly, *supra* note 40 ("As of April 2016, 47 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands all have enacted laws requiring notification of security breaches involving personal information."); Stephen Embry, *State data breach notification laws just got crazier*, AM. BAR ASS'N (May 2016), http://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html (discussing how many state data breach notification laws are confusing, contradictory, and difficult to comply with for companies operating under multiple state data breach notification laws).

111 MINN. STAT. ANN. § 325M.02 (2003) ("Except as provided in sections 325M.03 and 325M.04, an Internet service provider may not knowingly disclose personally identifiable information concerning a consumer of the Internet service provider."); NEV. REV. STAT. ANN. § 205.498 (1999) (providing when an Internet service provider shall keep consumer personal information confidential).

112 Cary Silverman & Jonathan L. Wilson, *State Attorney General Enforcement of Unfair or Deceptive Acts and Practices Laws: Emerging Concerns and Solutions*, 65 KAN. L. REV. 209, 212 (2016); THE PRIVACY, *supra* note 61, at 285.

113 Petrina McDaniel & Keshia Lipscomb, *Data Breach Laws on the Books in Every State; Federal Data Breach Law Hangs in the Balance*, SQUIRE PATTON BOGGS (Apr. 30, 2018), https://www.securityprivacybytes.com/2018/04/data-breach-laws-on-the-books-in-every-state-federal-data-breach-law-hangs-in-the-balance (discussing how all 50 states have

state privacy laws are narrow in scale and do not adequately establish standards for data protection, collection, monitoring, or use.[114] Though states have begun to emphasize and enforce data privacy, this process is too slow and sporadic to create a legal scheme in the United States that can adequately comply with rising international standards.[115]

C. Why the United States' System is Unsustainable and Ineffective

Critics of the United States' privacy law regime believe that the reactive, patchwork system is unsustainable in a world where technology and privacy concerns are continuously developing.[116] Through the FTC, the United States has pursued privacy protection as an unfair or deceptive practice rather than as a separate area of concern.[117] Under this method, companies are able to avoid privacy concerns by not following the voluntary best practices.[118] New businesses are able to circumvent federal regulatory and FTC provisions under the United States privacy model.[119] This situation becomes a cost-benefit analysis for companies where they must determine whether the potential loss on

---

laws and some worry a federal law may interfere with the States if not structured effectively).

114 Cory Bennett, *Lawmakers see momentum for data breach legislation*, THE HILL (Jan. 27, 2015, 12:34 PM.), http://thehill.com/policy/cybersecurity/230867-data-breach-bill-is-achievable-goal (indicating that while states have begun to dabble in creating data privacy and protection rights, the inherent nature of data to freely flow throughout the world calls for a greater encompassing approach to its governance).

115 Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

116 Daniel J. Solove & Paul M. Schwartz, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 897-900 (2014); O'Connor, *supra* note 115.

117 Brookman, *supra* note 11, at 358-59; *see also* Hattem, *supra* note 107 (discussing how critics argue that the "unfair and deceptive practices" authority is overly broad and should not address privacy matters because there is no substantive standard practice to follow that provides guidance on whether or not companies are properly securing data).

118 Brookman, *supra* note 11, at 359 (illustrating that "it would be challenging to argue that failure to provide access and correction rights constitutes a deceptive practice (as no deception occurs) or that failure to offer users control of their data is unfair (as no substantial harm is likely to occur), and consumers could avoid any potential harm by merely not using the service." Under this scheme, you can only be accountable if you decide that it is worth providing for consumer data protections rather than simply disregarding the subject).

119 Schwartz, *supra* note 21, at 1978 (stating the United States' system for regulating information privacy allows companies the freedom to innovate new data processing, storage, and mining techniques. Though this can have positive effects on technological development, it can also allow businesses to niche themselves into regulatory gaps to "test new innovative practices or find new ways to violate privacy.").

consumer trust outweighs the potential costs from implementing, complying with, and reconciling for violations of self-mandated privacy promises.[120] On an international basis, the FTC's limited jurisdiction weakens its international presence and authority.[121] While the FTC has sufficed so far, the evolving technological and global landscape outpaces the FTC's ability to remain effective as the United States' primary privacy law enforcer.[122]

Critics of the state privacy law system in the U.S. argue that this reactive approach causes inconsistencies, thus resulting in information remaining unprotected.[123] For companies this creates a potential for liability; if companies operate on a national or international scale, staying in compliance with individual jurisdiction requires monumental efforts.[124] Without these barriers to international transfers, companies would be able to rapidly expand into international markets, which could stimulate economic spending and job growth.[125] Instead, the potential risks and associated costs adversely impact the growth of trade amongst nations because companies, in their cost-benefit analyses, cannot conclude that the most efficient allocation of wealth is worth the price of trade.[126]

On the other hand, proponents of the United States' approach to privacy counter that this individualized structure promotes cooperation in the pursuit of companies that fail to sufficiently protect individuals' rights to privacy.[127] Even

---

120 Morey et al., *supra* note 7 (illustrating that consumer trust, particularly through transparency of business practices has become increasingly important to consumers' buying behaviors. Especially now that technological innovations have catalyzed data transfer and collection, business must invest more heavily in compliance and data security or risk losing the trust of their consumers).

121 Schwartz, *supra* note 21, at1977-78 (observing that the United States lacks a commission to oversee international data transfers, which allows for limitless exportation of individual data by companies to third countries. The FTC attempts to fill this role by monitoring international data sharing, however, can only do so under its unfair and deceptive practices authority and not as a limiting agency).

122 *Id*. at 1978-79; *see also* Marc Rotenberg, *In support of a data protection board in the United States*, 8 GOV'T INFO. Q. 79-94 (1991) (positing a proposal to create a federal privacy agency in the United States to better allow the United States to respond to the rapidly changing, global data privacy landscape).

123 Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law.

124 COBB, *supra* note 44, at 8-9 (discussing an example of how a lack of consistency in law has affected the legality of Stingrays, a data technology used by United States law enforcement agencies. Further contemplates whether the government can use this technology to conduct pre-emptive surveillance on suspected terrorists).

125 R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 42-44 (1960) (advancing the theory that, absent transaction costs, those operating within the economy will always pursue the course of action most effective in allocating wealth).

126 *Id*.

127 THE PRIVACY, *supra* note 61, at 285 (describing the benefits of having state privacy

if increased cooperation exists, critics contend that state laws will remain ineffective because they often conflict with one another or, at times, are subject to federal law preemption.[128] Furthermore, state laws are subject to constitutional challenges, which have invalidated state privacy laws.[129] Despite speculation regarding the ineffectiveness of the approach adopted by the United States, it has not taken any progressive steps toward an omnibus approach to privacy, as most countries have done.[130]

In the United States, courts have been reluctant to grant relief for petitioners by claiming a breach of privacy.[131] Often, courts dismiss data breach claims due to a lack of standing based on insufficient evidence of direct or actual harm.[132] As Stephen Cobb, an advocate for universal privacy rights argues, "commercial data controllers culpable in breach can argue that there is no harm to the subject whose records have been exposed, unless they suffer a financial loss directly

---

laws as opposed to overarching federal laws – it requires "increased cooperation and coordination in enforcement" between the FTC and state Attorneys General, which strengthens FTC actions against unfair and deceptive practices).

128 Jolly, *supra* note 40 (contending that federal government and state governments often conflict with one another regarding privacy law, where one sets higher standards than the other, making it difficult for companies to know which laws to comply with. For example, while federal law regarding the regulation of commercial e-mails preempts many state laws on the same topic, state laws are the standard to follow with privacy concerning medical or health records).

129 Schwartz, *supra* note 21, at 1976-77 (expressing that data processors have successfully challenged state information privacy laws because the sharing of information is a constitutionally protected right of the freedom of expression); Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2659-60 (2011) (invalidating a Vermont law that stopped "detailers" from selling, disclosing, and using pharmaceutical records for identification of doctors to target market specific pharmaceuticals).

130 SOLOVE & SCHWARTZ, *supra* note 53 (explaining omnibus approaches can create expansive catch-all provisions that provide general privacy guidelines to address any regulatory areas or issues not previously accounted for. Though countries adopting an omnibus approach still use sectoral privacy provisions, their presence is to supplement a standard minimum based on the requirements of a certain industry); *see also* Brookman, *supra* note 11, at 367-68 (portraying Congress' primary efforts towards promoting federal privacy legislation as focusing on data breach notification, however, forty-seven states already address this concern); *see also Data protection across the world*, MEDIUM (Jan. 30, 2018), https://medium.com/@privacyint/data-protection-across-the-world-fe66ca1e138f (discussing the approaches toward data privacy that Argentina, China, and India have taken).

131 COBB, *supra* note 44, at 7-8; In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F.Supp.3d 14, 20-21 (D.D.C. 2014) (stating increased risk of injury is not enough to confer standing and grant relief).

132 Khan v. Children's Nat'l Health Sys., 188 F.Supp.3d 524, 534 (D. Md. 2016) (explaining how the plaintiff did not "allege an injury in fact as required to establish Article III standing" given the complaint did not allege an actual misuse of personal data, and thus the district court dismissed the claim due to a lack of subject matter jurisdiction).

attributable to the breach."[133] For example, standing is hard to establish in data breach cases without evidence of pecuniary loss, but it is even harder to prevail when standing is granted based on alleged future harm.[134] Standing in data breach claims rests upon three theories: "(a) existing financial injuries[;] (b) actual misuse of information that may fall short of specific financial injuries[;] and (c) the alleged near-term risk of the misuse of information."[135] The first two theories, actual financial harm and actual misuse of information, are sufficient to establish standing.[136] However, the majority of data breach cases rely upon speculative future harm, absent evidence of pecuniary losses.[137] To assess standing for speculative harm, U.S. courts have looked at the underlying circumstances of the breach and the length of time passed since the breach occurred without incident.[138] While United States' courts are reluctant to grant standing based upon allegations of possible risk of future harms, foreign courts are beginning to recognize the severity of potential harm inherent in data breaches.[139]

In the United States, companies can get privacy and data breach claims dismissed based on assertions of a lack of standing due to no injury.[140] However, at an international level, courts are transitioning toward allowing standing in tort privacy claims without showing of pecuniary harm.[141] For example, between

---

133 COBB, *supra* note 44, at 7-8 (noting that other countries, such as Canada, have begun to apply the tort cause of action "intrusion upon seclusion" to data breach cases).

134 *See, e.g.* Friends of the Earth, Inc. v. Laidlaw Envtl. Servs, 528 U.S. 167, 180-81 (2000) (stating that plaintiffs must establish standing through a showing that "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."); COBB, *supra* note 44, at 7-8 (stating absent an actual pecuniary loss, courts have been hesitant to agree that an "injury in fact" has occurred and that it is imminent to occur based on the dissemination of data).

135 Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, BLOOMBERG BNA (Sept. 25, 2015), https://www.cov.com/-/media/files/corporate/publications/2015/09/standing_in_data_breach_cases.pdf.

136 *Id.*

137 *Id.* (stating, "the most commonly alleged injury . . . is an increased risk of future identity theft.").

138 *Id.* (stating that the courts evaluate factors such as the likelihood of actual harm and the length of time between the data breach and litigation); In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F.Supp.3d at 20-21 (stating, "an attenuated chain of possibilities does not confer standing").

139 *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1156-60 (2013) (holding that plaintiffs did not establish standing because there was no threatened imminent injury or concretely traceable injury resulting from the implementation of Section 702 of the Foreign Intelligence Surveillance Act of 1978).

140 Fram et al., *supra* note 135 (stating that courts usually agree with companies moving to dismiss because an increased risk from a breach is insufficient for standing).

141 Lisa R. Lifshitz, *A New Tort Is Born! Ontario Recognizes its First Privacy Tort*, BUS.

2011 and 2012, allegations arose that Google circumvented consumer Safari privacy settings to allow for the installation of data tracking cookies.[142] Then, Google sold the data collected from the cookies to third-party companies to use in direct marketing campaigns towards individual consumers.[143] While Google obtained settlements in the United States,[144] on June 12, 2013, the United Kingdom's Master of the Rolls permitted three claimants, domiciled in England, to serve Google at its principal place of business in Mountain View, California.[145] On January 16, 2014, the High Court of Justice in Strand, London ruled that the claims for tortious misuse of private information and breach of the Data Protection Act of 1998 were triable issues and that jurisdiction was proper.[146] Coupled with a willingness to apply long arm statutes to allow international citizens to serve United States based companies, more of these

---

L. TODAY (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/blt/2012/03/keeping-current-new-tort-born-201203.authcheckdam.pdf (discussing how Ontario recently recognized that privacy torts for data breaches exist); Halley v. McCann, 2016 CanLII 58945 (Can. Ont. Super. Ct.) (awarding damages for a breach of privacy claim and acknowledging that invasion of privacy torts in Ontario do not require proof of pecuniary loss or any sort of economic harm); Jones v. Tsige, (2012) 108 O.R. (3d) 241 (Can. Ont. C.A.).

142 Doug Drinkwater, *Google-Vidal Hall "opens the floodgates" to data breach compensation*, SC MAG. UK (May 15, 2015), http://www.scmagazineuk.com/google-vidal-hall-opens-the-floodgates-to-data-breach-compensation/article/414910.

143 *Id.*; *see generally* Duhigg, *supra* note 6 (explaining how companies conduct target marketing and the types of consumer information used to develop predictive targeting of advertisement).

144 Omer Tene, *The European Privacy Judicial Decision of a Decade: Google v. Vidal-Hall*, INT'L ASS'N OF PRIVACY PROF'LS (Apr. 2, 2015), https://iapp.org/news/a/the-european-privacy-judicial-decision-of-a-decade-google-v-vidal-hall (stating "Google settled with the Federal Trade Commission and state attorney general in the U.S. for more than $22 million and $17 million respectively."); THE PRIVACY, *supra* note 61 (explaining when the Google Safari cookie scandal occurred, Google settled with 37 states for $17 million); A.G. Schneiderman Announces $17 Million Multistate Settlement with Google Over Tracking of Consumers, N.Y. ST. ATT'Y GEN. (Nov. 18, 2013) (on file with author), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-17-million-multistate-settlement-google-over-tracking (explaining that Google entered into a $17 million multistate settlement agreement "concerning its unauthorized placement of cookies on computers using Apple Safari Web browsers during 2011 and 2012").

145 Vidal-Hall v. Google [2015] EWCA (Civ) 311, [6], (Eng.); Greg Palmer, *UK – Google v Vidal-Hall: A green light for compensation claims?*, LINKLATERS (June 15, 2015), https://www.linklaters.com/en/insights/publications/tmt-news/tmt-news—-june-2015/uk—-google-v-vidal-hall-a-green-light-for-compensation-claims (concluding that claimants received permission to serve Google, Inc. under the United Kingdom's long arm statute on the grounds that Google had committed the tort of misuse of private information, with the damages occurring within the United Kingdom and for breach of provisions in the Data Protection Act 1988); *see also Principal Place of Business*, BLACK'S LAW DICTIONARY, (10th ed. 2009).

146 Vidal-Hall v. Google [2014] EWHC (QB) 13; Drinkwater, *supra* note 142.

types of actions will arise as international standards continue to develop.[147]

United States data privacy law is a sectoral scheme that reacts to egregious changes in public policy and on a case-by-case basis.[148] The FTC is the United States' primary regulatory body for data protection and privacy; however, the FTC was not founded with the intention of occupying this field of law.[149] Because the FTC's authority relies upon its unfair-and-deceptive-practices power under Section 45 of the FTC Act, the FTC's power only extends to the poor practices of individual companies.[150] While there have been proposals to Congress that would create a federal data privacy statute or data protection board, none have yet to pass through both the Senate and the House.[151] Overall, the United States' approach to data privacy law is in stark contrast with the European Union, therefore Congress must reconcile these differences to avoid greater future consequences.[152]

II. DATA PROTECTION IN THE EUROPEAN UNION

Unlike in the United States, the European Union embraces a fundamental right of privacy for citizens, both online and offline.[153] While the United States views data protection as the broad concept of general privacy, the European Union narrows its view to specifically protect citizen rights from "the collection and processing of personal data."[154] Unlike the American system for privacy protection, the European Union proactively seeks to strengthen privacy protection—both internally and externally, when dealing with non-European

---

147 Lifshitz, *supra* note 141, at 2 (discussing how Ontario recently recognized that privacy torts for data breaches exist among companies that do business in Canada).

148 Cameron F. Kerry, *Filling the Gaps in US Data Privacy Laws*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws.

149 Serwin, *supra* note 48, at 811.

150 THE PRIVACY, *supra* note 61, at 275.

151 Boggs & Donoghue, *supra* note 58; *see, e.g.*, Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2d Sess. 2014); Data Security Act of 2014, S. 1927, 113th Cong. (2d Sess. 2014); Data Security Act of 2015, S. 961, 114th Cong. (1st Sess. 2015).

152 *See infra* Part III.

153 Charter of Fundamental Rights of the European Union art. 7, Oct. 26, 2012 O.J. (C 326) 393, 397 (explaining Article 7 concerns the right to respect for private and family life where "[e]veryone has the right to respect for his or her private and family life, home and communications.". Article 8 concerns the protection of personal data where "[e]veryone has the right to the protection of personal data concerning him or her.").

154 Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L. J. 461, 470 (2000) (stating the United States uses the term "privacy" to address a wide range of issues, ranging from the right to an abortion, the lack of security cameras within a dressing room, to voter confidentiality. This disparity between views is why Americans are less concerned with data protection security: they think of privacy as an overarching, general concept rather than as a singular issue).

Union countries.[155] European Union consumers are also given greater power in limiting what data they expose to the world with a "right to be forgotten."[156] The European Union's proactive approach towards personal privacy protection has made it the global leader in privacy law and data security.[157]

A. The Data Protection Directive

On October 24, 1995, the European Parliament adopted the Data Protection Directive (DPD) 95/46/EC, the European Union's primary source for data protection law, "to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States."[158] The DPD also extends beyond Member State borders by providing data protection adequacy requirements to companies located in third world countries.[159] Under the DPD, Member States have the ability to impose

---

155 Schwartz & Peifer, *supra* note 29, at 118 (exploring the differences in data protection between the European Union and the United States where the former takes a broad, proactive approach and the latter is reactive to specific crises).

156 David Streitfeld, *European Court Lets Users Erase Records on Web*, N.Y. TIMES (May 13, 2014), http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html?_r=0 (explaining the decision of the European Union to allow consumers to have the right to make search engines erase certain links to webpages upends traditional notions of free flows of information); *see also* Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKLEY J. INT'L L. 161, 169-72 (2012) (finding in the United States, First Amendment issues arise grounded on the belief of a contradiction to the fundamental protections for freedom of speech and press).

157 Schwartz, *supra* note 21, at 1974-79 (explaining how the E.U. has embraced an "Omnibus" approach to privacy laws that sets a minimum standard for privacy protection amongst its Member States with incentives for states to both incorporate, and strengthen, its concepts. This omnibus method has shaped future privacy laws for nations a part of, and external to, the European Union).

158 S.T.S., Nov. 24, 2011 (Spain), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0468&from=EN (defining personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."); O.E.C.D., *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (as amended on July 10, 1980), https://legalinstruments.oecd.org/en/instruments/114 (describing how the Directive enforces a minimum standard on privacy protection laws within the European Union, based upon the 1980 Organization for Economic Cooperation and Development's Recommendations Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines), which set forth recommended, non-binding privacy principles for countries to abide by).

159 Schwartz, *supra* note 21, at 1972-73.

stricter privacy protection standards than what the DPD requires.[160] The DPD requires that the processing of personal data occur only when:

> [T]he data subject has unambiguously given his/her consent; processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject, or it is in the public interest.[161]

By providing minimum standards for data processing across its Member States, the European Union ensures that it protects its citizens' fundamental right to privacy.[162] This protection is enforceable both within the European Union and against third-party countries participating in international data transfers.[163]

Prior to the adoption of the DPD, the structure of the European Union's system for privacy protection resembled that of the United States.[164] In contrast, while the United States remained content with this approach to data privacy, the European Union sought to set a standard minimum level of protection amongst all of its Member States.[165] Even though the majority of the countries previously had broad data protection laws, the European Union used the DPD to ensure that

---

160 1995 O.J. (L 281) 31 art. 5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=En (explaining that individual member states must adhere to the minimum levels of privacy protection standards set forth in the DPD, however, states have the authority to "determine more precisely the conditions under which the processing of personal data is lawful.").

161 *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: Joint Hearing Before the Subcomm. on Commerce, Mfg., and Trade and the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce,* 114th Cong. 21 (2015) *(*statement of Dr. Joshua P. Meltzer, Senior Fellow, Global Economy and Development program at the Brookings Institute*)*; 1995 O.J. (L 281) 31 art. 6, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=En (stating that data processors must prove the quality of any personal data processed, where it must be: "(a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. . .; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date . . .; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed").

162 *See* Fromholz, *supra* note 154, at 468-69.

163 *See id.* at 468 n.40.

164 *See id.* at 468.

165 *See id.* (explaining the European Commission headed this effort by directing member countries to make data protection a fundamental right, to create independent supervisory bodies, to establish redress for enforcement, and to ensure that international data transfers complied with these high standards); Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 at art. 25 & 26 (setting out adequacy standards, and exemptions, under Articles 25 and 26, respectively).

its Member States protected its citizens' fundamental rights to privacy.[166] By setting the minimum standard, while leaving certain powers to the Member States, the European Union has allowed for easier data flow throughout Europe and with non-member countries.[167] Even if third party countries do not meet the European Union's stringent adequacy standards, like the United States, exceptions are made as long as one of a list of certain conditions is met.[168] However, the European Union's data protection laws are rapidly evolving in ways that affect both Member States and non-Member States alike.[169] While the DPD has been successful in protecting its citizen data privacy, it has only been a directive.[170] The European Union passed, on the approval of all of its members, a uniform regulatory regime to ensure that one system of data protection law governs the entire European Union.[171] This legislation comes in the form of the

---

166 *See* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 433 (1995) (illustrating that most countries in Europe had statutes broadly protecting data within the public and private sectors); Council Directive 95/46 art. 13, 1995 O.J. (L 281) 42 (EC) (stating the establishment of a standard minimum for protection still allows individual countries to enact legislation defining their means for monitoring and enforcing data protection).

167 *See* Jennifer M. Myers, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United* States, 29 CASE W. RES. J. INT'L L. 109, 118-19 (1997) (enacting the Directive has increased and expedited data transfers amongst member states because each must adhere to, at least, minimum standards. Even if the data transfers from one Member State to another, then to a non-Member State, the Directive protects the original country's data privacy interest because the second Member State must adhere to the Directive's minimum adequacy standards).

168 *See* Council Directive 95/46 art. 25-26, 1995 O.J. (L 281) 45-46 (EC) (illustrating exceptions to adequacy include unambiguous consent; necessity for the performance or execution of a contract with the data subject; performance of a contract with a third-party in the data subject's interest; necessity for the public interest or in furtherance of a legal claim; protection of vital interests of the data subject; and, lawful transfers made from a public register).

169 *See* Warwick Ashford, *EU Data Protection Rules Affect Everyone, Say Legal Experts*, COMPUTERWEEKLY (Jan. 11, 2016, 5:00 PM), http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts; *see* Shan Wang, *Europe's General Data Protection Regulation is Coming May 25. How Have News Publishers Prepared?*, NEIMAN LAB (May 3, 2018), http://www.niemanlab.org/2018/05/europes-general-data-protection-regulation-is-coming-may-25-how-have-news-publishers-prepared/.

170 SOLOVE & SCHWARTZ, *supra* note 53, at 902 (describing that the directive grants rights rather than obligating specific actions to facilitate a minimum end result rather than a comprehensive set of steps towards such goal. As a directive, the DPD faced limitations of only having the authority to set minimum data protection standards for Member States rather than as a uniform standard of regulation); *see* Bowman, *supra* note 11 (stating that while this allowed for easier trade across the European Union, member states implemented privacy laws at varying degrees of stringency, making trade sometimes difficult).

171 *See* Bowman, *supra* note 11; Council Directive 95/46, 1995 O.J. (L 281) 32 (EC).

General Rules of Data Protection (GDPR), which replaced the DPD on May 25, 2018.[172] Through the GDPR, E.U. privacy law and global privacy law standards will dramatically increase at a rate that the United States' current regulatory scheme cannot keep pace with.[173]

B. Evolving Global Data Privacy through the General Data Protection Regulation

On May 25, 2018, the GDPR replaced the DPD as the European Union's data protection framework.[174] The GDPR came in response to the changing technological environment where electronic data transfers have become more prevalent and further reaching.[175] The GDPR aims to strengthen the effects of the DPD by creating a uniform and enforceable data protection scheme.[176] Though certain similarities between the GDPR and DPD exist, the GDPR contains a broader territorial scope, the enumeration of stronger rights of control for data subjects, and higher penalties for company violations.[177] Additionally, while the scope of the DPD only allowed Member States to govern controllers and processors within their borders, the GDPR applies to three broad situations: (1) when an organization physically operates anywhere within the European Union; (2) when the data processed concerns an individual within the European Union; and (3) where the national law of an individual Member State is applied to benefit public international law.[178] With greater concerns for privacy protection in a continuously evolving technological environment, the European

---

172 *See* Ashford, *supra* note 169 (explaining that the GDPR will have significant impacts on companies operating within, and out of, the European Union if operations involve the personal data of E.U. citizens. Stewart Room, cyber security and data protection partner at Pricewaterhouse Cooper stated his belief that the GDPR "will impact every entity that holds or uses European personal data both inside and outside of Europe.").

173 Hartzog & Solove, *supra* note 44, at 2294-300 (discussing how the FTC has only scratched the surface of its power to regulate U.S. data privacy and how it is presently unable to keep pace with the rising global standards; however, authors take a different approach in rectifying this current situation); *cf.* De Hert & Papakonstantinou, *supra* note 173, at 315-23 (advocating for an international data privacy organization to reconcile differences amongst countries in their data privacy and protection policies).

174 *See The EU General Data Protection Regulation*, *supra* note 174, at 2.

175 *See* Bowman, *supra* note 11 (explaining that since the DPD's passage twenty years ago, technological innovations and the way that society has interacted through technology has changed tremendously. Social media, phone apps, and increased spread and function of the Internet have all contributed to greater degrees of data transfer).

176 *See id.*

177 *See id.*

178 *See* Gonzago Gallego et al., FUTURE-PROOFING PRIVACY: A GUIDE TO PREPARING FOR THE EU DATA PROTECTION REGULATION, (2016); Robert Madge, *GDPR's Global Scope: The Long Story*, MEDIUM (May 12, 2018), https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f.

Union is setting the global standard for individual privacy protection.[179]

The GDPR defines its territorial scope in Article Three to include all relevant controllers or processors of E.U. citizens' personal data, regardless of whether they physically operate within the European Union.[180] Chapter V, Articles 44 through 49,[181] of the GDPR, govern the cross-border transfers of E.U. citizens' data, and are primarily predicated on a certification of the adequacy standard.[182] Under Article 45 of the GDPR, adequacy decisions reaffirmed the ability to conduct data transfers when a third party can ensure that its country's data security standards are sufficient to comply with those in the European Union.[183] Adequacy determinations of a country allows for the simplest process for data transfers because it requires no additional safeguards to be implemented by a business and no additional authorization requirements.[184] However, the adequacy decision remains subject to periodic review by the European Commission.[185] In certain circumstances, Article 46 of the GDPR allows for cross border data transfers, absent an adequacy decision, with the presence of

---

179 *See* Gallego et al., *supra* note 178 (explaining how Article 3 of the GDPR creates a global standard for privacy protection law because it encompasses "any company that markets good or services to EU residents . . . regardless of whether the company is located or uses equipment in the EU or not"); O'Connor, *supra* note 115.

180 Council Regulation 2016/679, 2016 O.J. (L 119) 5 (EU) (illustrating that any processing of consumer data related to the offering of goods or services to data subjects, regardless of payment occurs, and to the monitoring of data subject behavior within the European Union).

181 *Id.* at art. 45-49 (emphasizing that Article 45 specifies terms for transfers predicated on adequacy decisions. Article 46 states the conditions necessary for cross-border transfers, absent an adequacy decision. Article 47 details conditions for transfers using binding corporate rules as an adequacy mechanism. Article 48 addresses situations where foreign governments and judiciaries order cross-border transfers unpermitted under the GDPR. Article 49 lists the conditions for derogations, exceptions, to the GDPR's prohibition on cross-border data transfers, absent an adequacy decision or the use of approved safeguards).

182 *See* Dr. Detlev Gabel & Time Hickman, *Chapter 13: Cross-Border Data Transfers-Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Sep. 13, 2017), https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection; Anna Myers, *Top 10 Operational Impacts of the GDPR: Part 4 – Cross-Border Data Transfers*, IAPP (Jan. 19, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/.

183 Council Regulation 2016/679, art. 45, 2016 O.J. (L 119) 61 (EU).

184 Ariel Teshuva, *Why Has the EU Made So Few Adequacy Determinations?*, LAWFARE (Jan. 2, 2017, 2:25 PM), https://www.lawfareblog.com/why-has-eu-made-so-few-adequacy-determinations.

185 *See* Myers, *supra* note 182 (discussing that the European Commission determines adequacy based on the consideration of numerous factors, including but not limited to, "the specific processing activities, access to justice, international human rights norms, the general and sectoral law of the country, legislation concerning public security, defense and national security, public order, and criminal law.").

appropriate safeguards.[186] Article 49 of the GDPR lists appropriate situations for safeguards and derogations.[187]

Data subjects receive greater rights to data privacy under the GDPR.[188] Under the DPD, use of safeguards and derogations required unambiguous consent by data subjects through either a statement of affirmation or clear affirmative action.[189] The GDPR raises the standard for applying these derogations to require explicit consent, either orally or in writing.[190] The explicit consent requirement must involve the signing of a separate request for consent by the data subject, which grants their permission to have their personal information stored and transmitted.[191] This standard puts more power in the hands of consumers to dictate what personal information is transmitted across borders.[192] The GDPR also grants data subjects several additional rights, including but not limited to: the right to restriction processing;[193] the right to portability;[194] and the right to erasure, also known as the right to be forgotten.[195]

Unlike in the United States, the GDPR takes a strong stance to ensure that companies, both internal and external to the European Union, comply with its

---

186 Council Regulation 2016/679, art. 46, 2016 (EU).

187 *Id.* at art. 49 (listing appropriate situations allowing for the use of safeguards in the absence of an adequacy decision including explicit consent upon knowledge of the risks, necessity for contract performance either between the data subject and the controller or in the data subject's interest, strong public interest, and defense of legal claims).

188 *See* Myers, *supra* note 182.

189 Council Directive 95/46, art. 13, 1995 O.J. (L 281) 31 (EC).

190 *See* Myers, *supra* note 182.

191 *See id.* (acknowledging the GDPR does not explicitly state whether consent is necessary only initially or throughout the data management and transfer process. It is recommended that companies provide adequate information in their consent requests regarding potential data transfers, in addition to actively renewing consumer consent.); *see also* Andrew Clearwater & Brian Philbrook, *Practical tips for consent under the GDPR*, IAPP (Jan. 23, 2018), https://iapp.org/news/a/practical-tips-for-consent-under-the-gdpr/.

192 *See The EU General Data Protection Regulation*, *supra* note 174 (describing the subject of explicit consent is controversial because it states that consumers must have rights to withdraw consent as they see fit. In the context of e-commerce and contract performance, explicit consent is likely to raise issues because consent is a non-negotiable condition on obtaining a service with arguable freedom of choice).

193 Council Regulation 2016/679, art. 18 & 21, 2016 (EU) (stating data subjects can restrict controller data processing of their personal data when the subjects contest the data's accuracy, the process of the data is unlawful, the personal data is no longer necessary for processing purposes, or if the data subject objects to the process of the data pursuant to Article 21(1)).

194 *Id.* at art. 20 (explaining that data subjects, when the processing of data is machine automated and based on either consent or contract, have the right to order a controller to deliver the personal data concerning him or her in a "structured, commonly used and machine-readable format.").

195 *Id.* at art. 17(1)-(2) (demonstrating that data subjects have the right to require a controller to erase personal data controlling him or her, without undue delay, when one of several broad circumstances apply).

high standards for citizen data protection.[196] Data subjects covered by the GDPR receive remedial rights, and mainly, the right to compensation for controller, or processor violations that result in either material, or non-material, damages.[197] For example, infringement of GDPR provisions, with regard to cross-border data transfers, subjects the violating entity to "administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."[198] While on its face 4% seems minimally intrusive, for multibillion dollar companies, this can add up to hundreds of millions of dollars in violations and noncompliance.[199] These remedial rights make the GDPR's reach act as a quasi-global law, because even the slight risk of violation for a medium or large sized company outweighs the possible financial repercussions if an administrative fine is found to be applicable.[200] Now with the GDPR's implementation and the remaining compliance uncertainty, companies must change their practices now or face enormous penalties later.[201]

The GDPR's implementation has further increased the data privacy gap that existed between the United States and the European Union.[202] While the DPD built the European Union's foundation of privacy law, the GDPR attempts to create a uniform standard amongst its Member States that transcends the E.U.'s borders.[203] The potential implications and ramifications that noncompliance with GDPR standards may have on international dealings has raised red flags

---

196 *See* Bowman, *supra* note 11; Svantesson, *supra* note 30.

197 *GDPR Training*, HIPPA J., https://www.hipaajournal.com/gdpr-training/ (last visited Sept. 12, 2018).

198 *See* Council Regulation 2016/679, art. 83(5), 2016 (EU) (explaining the GDPR includes additional circumstances for administrative fines for violations of its provisions).

199 *See* Bowman, *supra* note 11; Bernard Marr, *GDPR: The Biggest Data Breaches and The Shocking Fines (That Would Have Been)*, FORBES (Jun. 11, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#719f62826c10.

200 *See* Council Regulation 2016/679, art. 83(2), 2016 (EU) (describing that a variety of factors determine whether an infringement warrants an administrative fine and its severity. Examples of determinative factors include the nature, gravity, and duration of the infringement; the intentional or negligent character of the infringement; actions taken to mitigate the damage; and the degree of controller or processor responsibility, to name a few).

201 *See* Ashford, *supra* note 169 (illustrating that the GDPR's scope goes beyond effecting data processors but also those who provide services to them. All companies will need to assess whether the GDPR affects them, either directly or indirectly, and, if so, how to proactively prepare to comply).

202 *See* Bowman, *supra* note 11.

203 *See* Ashford, *supra* note 169; *see generally* Gilbert, *supra* note 27 (discussing how the GDPR will affect companies worldwide involved in international commerce because its protection transcends E.U. Member State borders by following the data trail of E.U. citizens).

among companies and government officials in the United States.[204] Though it may be costly upfront, the impetus for change will only increase costs and liability if action is not soon taken by the United States.[205] To reconcile its privacy laws with more stringent global standards, the United States can no longer rely on the negotiation of trade agreements, like the Privacy Shield, to come to an arguable middle ground.[206] The United States must take significant preemptive steps toward raising its own standards.[207]

C. The GDPR's Impact on U.S. Based Companies

Already, the impact of the GDPR has been felt by businesses operating outside of the United States.[208] On the first day of its implementation, Facebook, Inc. and Google, Inc., both U.S. based companies, were sued for alleged coercion of consumer consent to sharing their personal data.[209] According to the complaints, the companies did not allow users free choice to consent to the use of their personal data because they were forced into accepting each respective

---

204 *But see* Paul Merrion, *Survey Reveals Widespread Ignorance of Europe's New Privacy Regulation*, 2016 WL 5955365 (Oct. 14, 2016) (presenting survey findings regarding the lack of preparation and knowledge about the GDPR and its potential effects on international data transfers. According to the surveys within this study, conducted by Dell Software, "[a]bout 82 percent [of the 821 executives surveyed] said they are concerned about GDPR but knew little or nothing about its details, and 97 percent said their companies do not have a plan to come into compliance.").

205 *See Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: Joint Hearing Before the Subcomm. on Commerce, Mfg., and Trade and the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce*, 114th Cong. 21 (2015) (detailing figures about the transatlantic data economy between the European Union and the United States); *see also* Paul Merrion, *EU's New Privacy Reg. Will Require 75,000 Data Protection Officers Worldwide*, 2016 WL 6645854 (Nov. 10, 2016) (discussing the findings of a study conducted by the International Association of Privacy Professionals, which predicts that companies worldwide will need to hire at least 75,000 data protection officers to ensure that organizations stay in compliance with the GDPR's standards).

206 Weiss & Archick, *supra* note 16.

207 *See infra* Part III (discussing how privacy law in the United States is lagging behind with the rest of the world, which may impact future trade if the United States does not develop its data protection standards).

208 Chris Albers Denhart, *New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook*, FORBES (May 25, 2018, 10:27 AM), https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#46eb34ea4d36.

209 *See* Russell Brandon, *Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR*, THE VERGE (May 25, 2018), https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe (alleging that the new policies written by the companies in anticipation of the GDPR were insufficient to allow users a freedom of consent beyond an all-or-nothing choice).

company's terms.[210] Though both organizations had prepared for the GDPR's implementation, these suits indicate the lack of compliance and regulatory backing in the United States that leaves companies susceptible to GDPR violations. Facebook has received additional data security scrutiny for its failure to comply with the GDPR following two data breach incidents.[211] On September 25, 2018, Facebook experienced a data breach incident, which impacted 50 million accounts.[212] Though less than five million of the users effected were European citizens, the incident may still result in a fine up to $1.63 billion.[213] In a prior similar data breach incident, Facebook received only a £500,000 fine under the DPD.[214] While this occurrence affected 17 million European citizen accounts, this fine was the maximum amount allowed under the now outdated Data Protection Act.[215] Had the amount been calculated under the GDPR's provisions, this fine would have been roughly $22 million, or 4% of Facebook's global turnover at the time.[216] Though the GDPR's impact on United States companies has been minimal thus far, it has already reared its devastating potential.

III. SOMETIMES, SLOW AND STEADY DOES NOT WIN THE RACE

The United States must alter its mindset towards data privacy if it wishes to sustain its international data transfer market.[217] While the slowly developing

---

210 Denhart, *supra* note 208.

211 *Id.*

212 *See* Charlie Osborne, *Facebook could face $1.63bn fine under GDPR for latest data breach*, ZDNET (Oct. 2, 2018), https://www.zdnet.com/article/facebook-could-face-billions-in-fines-under-gdpr-over-latest-data-breach/.

213 *See id.* (stating that the GDPR's fine calculations of the greater of either €20 million or 4% of annual global turnover, applied to Facebook's recent financial results, may tops out at $1.63 billion).

214 *See* James Vincent, *UK data watchdog fines Facebook maximum legal amount for Cambridge Analytica scandal*, THE VERGE (Oct. 25, 2018), https://www.theverge.com/2018/10/25/18021900/facebook-cambridge-analytica-scandal-uk-data-watchdog-ico-fines-maximum-amount.

215 *See id.* (stating that even though the maximum fine was awarded, many believed that this was insufficient).

216 *See id.*

217 *See* Bennett, *supra* note 156, at 192-94 (explaining the constant developments in technology, business, and the Internet create a highly complex, changing legal landscape. Though a method for solution may not be clear, inaction is not a viable option to reconciling cultural differences and protecting either nation's privacy interests); *see also* Erika Morphy, *Staring Down the Intersection of ePrivacy, GDPR and Privacy Shield*, CMS WIRE (Aug. 29, 2018), https://www.cmswire.com/digital-experience/staring-down-the-intersection-of-eprivacy-gdpr-and-privacy-shield/ (discussing aspects of data-sharing not addressed by current regulations).

sectoral approach to privacy appeases the expectations of United States citizens and businesses, it is unsustainable in the long run.[218] The United States' approach is too slow to satisfy rapidly growing expectations at an international level.[219] At its core, the European Union's emphasis on privacy is a fundamental right and willingness to enforce its protection creates a much higher standard for privacy protection.[220] More countries are embracing this approach toward protecting consumer data and privacy by following the European Union's strict approach.[221] This rise of global standards complicates international data transfers because the United States must either adopt a similar stricter approach to privacy or rely on negotiated trade agreements similar to the Safe Harbor Agreement and Privacy Shield.[222] As evidenced by the Safe Harbor Agreement, the United States cannot reasonably rely on the negotiation of dozens of agreements to allow companies to safely participate in international data transfers because the international data policies will not withstand legal challenges.[223] Instead, the United States must embrace an omnibus approach, at the least, to govern all international data transferred into the United States and used by American companies.[224] Without a minimum standard in place,

---

218 *See* Brookman, *supra* note 11, at 371-74 (explaining the government is unlikely to place any significant importance on protecting privacy until pressured by American citizens. The difficulty in this is that while citizens can sense privacy concerns, they do not understand the full extent to which personal data collection, storage, processing, and transmitting occurs).

219 *See* Schwartz, *supra* note 21, at 2007-08 (2013) (describing new developments and stricter requirements will enlarge the privacy law gap between the European Union and the United States. Unless the United States government and companies operating between the European Union and the United States respond with increased privacy emphasizes, future legal challenges are certain to loom).

220 *See* Charter of Fundamental Rights of the European Union, 2000, art. 7 & 8, 2012 O.J. C 326/02; Fromholz, *supra* note 154; Streitfeld, *supra* note 156 (discussing the current approach to privacy law in the European Union).

221 *See* Schwartz, *supra* note 21, at 1978-79 (describing how the effects of more countries following the European Union's approach towards privacy makes the United States' privacy law lag further behind the regulations necessary to conduct in international data trades); *see also* Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Feb. 6, 2018, 4:50 AM), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ (describing how countries such as Japan, Israel, and South Africa recently conformed to data protection guidelines put forth by the European Union).

222 *See* Schwartz, *supra* note 21, at 1978-79; *see also* Bennett, *supra* note 156, at 192-94 (describing the importance for Unites States companies to reconcile with the European Union's data privacy regulations).

223 *See generally* U.S.-EU SAFE HARBOR FRAMEWORK DOCUMENTS, https://2016.export.gov/safeharbor/eu/ (last visited Sept. 19, 2019); *see generally* Tourkochoriti, *supra* note 33, at 162 (discussing the impact that the disparity between data privacy standards in the United States and the European Union has on international data transfer relations and negotiations).

224 O'Connor, *supra* note 115; *see* Seita, *supra* note 35, at 472-73 (discussing the

subsequent international agreements regarding international data transfers are likely to fail.[225]

A. The United States Must Adopt an Omnibus Approach to Privacy

Companies and industries operating within the United States are reluctant to give Congress a reason to enact overarching privacy regulations.[226] Although there have been numerous attempts to pass federal privacy regulations through Congress, none have successfully passed through.[227] The United States' only recent significant change in privacy law is the Judicial Redress Act, which addresses international concern over data sharing in the context of criminal and terrorism investigations.[228] This has been the United States' only major privacy

---

globalization of trade and how the United States should adopt a comprehensive data privacy and protection regime, similar to the direction taken by that the majority of the world).

225 *See* Mehreen Khan & Jim Brunsden, *EU to Demand Tough Data-Protection Rules with Future Trade Deals*, FIN. TIMES (Feb. 9, 2018), https://www.ft.com/content/e489abba-0dc5-11e8-8eb7-42f857ea9f09 (describing that as the EU's regulatory guidelines expand globally, the United States' influence in international trade will diminish); *see* Tourkochoriti, *surpa* note 33, at 161-62(discussing current negotiations between the European Union and the United States on the Transatlantic Trade and Investment Partnership (T-TIP), which aims to increase foreign trade and investment between the U.S. and the E.U.); *see also* Eric Shimp, *Data Privacy in the Transatlantic Trade Agreement? US-EU Ponder the Way Forward*, ALSTON & BIRD: PRIVACY & DATA SEC. BLOG (Apr. 10, 2013), http://www.alstonprivacy.com/data-privacy-in-the-transatlantic-trade-agreement-us-eu-ponder-the-way-forward/ (discussing how data protection and privacy concerns have impacted recent trade negotiations and how they are likely to continue to stall progress of agreements between the United States and countries with greater data security standards).

226 Neema Singh Guilani & Jay Stanley, *The Landmark European Law That Could Change Facebook and Improve Privacy in America*, ACLU (Apr. 14, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/landmark-european-law-could-change-facebook-and-improve; *contra* Cameron F. Kerry, *Why protecting privacy is a losing game today–and how to change the game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game (stating that "a number of companies have been increasingly open to discussion of a basic federal privacy law," because they see "value in a common baseline that can provide people reassurance about how their data is handled.").

227 *See* Boggs & Donoghue, *supra* note 58; Ashley Baker, *Congress must act to protect privacy before courts make surveillance even easier*, THE HILL (Aug. 7, 2017), http://thehill.com/blogs/pundits-blog/technology/345559-congress-must-act-to-protect-data-privacy-before-courts-make.

228 5 U.S.C. § 522a(g)(1)(A)-(B), (D) (2014); Judicial Redress Act of 2015, Pub. L. No. 114-126, Feb. 24, 2016, 130 Stat 282 (2016); *see also* Eric Geller, *Everything You Need to Know about the Big New Data-Privacy Big in Congress*, THE DAILY DOT (Feb. 4, 2016, 5:28 PM), http://www.dailydot.com/layer8/what-is-the-judicial-redress-act-europe-data-privacy-bill/ (describing the significance of the Judicial Redress Act and its impact on the European Union and the United States' international data relations).

law advancement since the Safe Harbor Agreement's invalidation.[229] Though important to sustaining international data privacy relations, government uses of personal data for criminal cases does not address the European Union's concerns for protecting individual's data as a standard practice.[230]

The United States government must take further precautions to protect the personal information of its own citizens; otherwise the European Union and other third-party countries will take further precautions when conducting international data transfers.[231] The invalidation of the Safe Harbor Agreement proves that the United States' privacy laws governing consumer data are not on par with the European Union.[232] However, the United States' domestic federal privacy law landscape remains unchanged since the invalidation.[233] With the rest of the world adopting privacy approaches similar to the European Union, the United States lags further behind.[234] Agreements like the Privacy Shield, which will attempt to bridge even larger privacy policy gaps than its predecessor, is set up for failure from the outset, unless change occurs within the United States.[235] Without the development of consumer data protections in the United States, corporations will likely experience exponential increases in costs for

---

229 European Commission Press Release, Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama (Feb. 24, 2016).

230 *See* Weiss & Archick, *supra* note 16, at 13.

231 *See* Tourkochoriti, *supra* note 33, at 161 (indicating that while the United States is a valuable trade partner because of its economy's strength, countries are not willing to compromise on their fundamental rights to privacy. Instead, more hurdles to trade negotiations arise, prolonging the negotiation process); Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.231190111.1146412004.1535386038-1536309635.1535386038.

232 *See European Court of Justice Invalidates U.S.-EU Safe Harbor Agreement*, *supra* note 26, at 1-2 (discussing the impact and reasoning behind the invalidation of the Safe Harbor Agreement).

233 Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2016); Amy C. Pimentel, *Safe Harbor update: House votes to pass Judicial Redress Act*, LEXOLOGY (Oct. 22, 2015), https://www.lexology.com/library/detail.aspx?g=89cf6033-8252-4e78-85d6-a93acc97a65e (describing the Judicial Redress Act as a means of redressing the invalidation of the Safe Harbor Agreement).

234 *See* Gallego et al., *supra* note 178, at 57 (describing the territorial scope of the GDPR and its bolstering effect on international data privacy standards); *Business Without Borders: The Importance of Cross-Border Data Transfers of Global Prosperity*, U.S. CHAMBER OF COMMERCE (2014) (explaining that nearly 100 countries are enacting laws that will protect both citizens and non-citizens, when data is being transferred through limitations on where certain data may be transferred, unlike the United States).

235 *See* Schwartz, *supra* note 21, at 1978-79 (detailing the effect that rising global privacy standards will have on future international data transfer negotiations); Natasha Lomas, *EU-US Privacy Shield Now Officially Adopted but Criticisms Linger*, TECHCRUNCH (2016), https://techcrunch.com/2016/07/12/eu-us-privacy-shield-now-officially-adopted-but-criticisms-linger/.

negotiations; insurance; and time delays, among other things.[236] In response, Apple and Facebook have both advocated for the United States to adopt privacy laws in a similar manner to the European Union.[237]

While some scholars have correctly noted that the FTC operates as a de facto common law and promotes this structure of privacy law development,[238] this is insufficient to sustain increased international data protection and privacy standards. Under the FTC, nearly all cases end in settlement agreements, thereby setting no legal binding precedent.[239] This practice is unsustainable and lacks the function of creating legally binding precedent necessary to develop privacy law in the United States.[240] Though settlements resolve disputes and hold companies accountable, the development of privacy law remains stagnant.[241] Additionally, the rise of legal threats adversely impacts the government's motivation to increase international data transfers due to high transactional costs and threats.[242] Instead, third-party countries are shaping privacy law in a way that significantly impacts U.S. businesses.[243]

The advocates for a common law approach to develop privacy law in the United States neglect to take into account the significance of data as a global commodity.[244] For example, while the courts in the United States have been reluctant to grant standing for privacy claims absent actual pecuniary harm,

---

236 *See* Tourkochoriti, *supra* note 33, at 161-64 (2014); *see also* Shimp, *supra* note 225.

237 *See* Mehreen Khan, *Apple and Facebook call for EU-style privacy laws in US*, FINANCIAL TIMES (Oct. 24, 2018), https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713.

238 *See* Solove & Hartzog, *supra* note 86, at 600, 602, 605-07 (analyzing how the FTC has emerged as the most influential privacy and data protection authority in the United States with an increasingly expanding jurisprudence. The FTC has led to the development of industry standards and best practices that companies are liable to comply with).

239 *See id. at* 620-21 (explaining that though the FTC has led to greater enforcement of privacy policies, the majority of its cases end as settlements).

240 *See* Serwin, *supra* note 48, at 842-44 (discussing some of the drawbacks to the FTC's structure of privacy enforcement and suggestions on how it must develop to remain effective); United States v. ITT Cont'l Baking Co., 420 U.S. 223, 238 (1975) (reasoning how the Court did not need to determine whether 15 U.S.C. §§21(l) and 45(l) "permit the imposition of daily penalties.").

241 *See* Serwin, *supra* note 48, at 842-43 (explaining that confidential terms through private settlements limit available guidance on how to develop U.S. privacy law).

242 *See* Coase, *supra* note 125 (detailing the adverse impact on overall wealth due to unnecessary wealth allocation deterrents that minimize the efficiency of economic decision-making).

243 *See* Ashford, *supra* note 169.

244 *Contra* Hartzog & Solove, *supra* note 44, at 2294 (promoting the bottoms-up approach to developing privacy law in the United States, which consists of a slow, common law approach); *The New Data Protection Laws*, ISLE OF MAN INFO. COMMISSIONER (June 2017), https://www.inforights.im/media/1389/new-data-protection-laws-summary-june-2017.pdf.

international courts are willing to use long arm statutes to pursue international privacy claims.[245] Though these rulings do not directly impact privacy law in the United States, the FTC's common law approach to privacy cannot remain in its current state due to the increasing international expectations.[246] Instead, Congress should lower the hurdles that the FTC must overcome in promulgating nationwide and industry wide rules governing data privacy and protection.[247]

B. The FTC: The United States' DPD

As the de facto governing body for consumer data in the United States, the FTC has entrenched itself as the nation's regulatory body for consumer data.[248] The FTC was originally given authority based on the necessity to regulate technology at a time of exponential technological innovation.[249] However, as technology has evolved, the FTC's scope of power has also evolved.[250] The FTC sets a floor for data protection by aligning corporate practices with industry norms and expectations.[251] This approach allows the FTC to expand its authority, but it is still limited in the ways in which it may pursue a company for its practices.[252] The impetus for change revolves around Congress' willingness to amend the Magnuson-Moss rules to allow the FTC greater jurisdiction, increased control over consumer data protection, and additional rulemaking authority within this capacity.[253] While Section 5 of the FTC Act grants the FTC's broad jurisdiction, its jurisdiction and practical ability to make rules remains severely restrained in the data privacy context.[254]

---

245 *See* Fram et. al., *supra* note 135 (discussing the elements looked at by U.S. courts to determine whether data privacy and breach claims have standing); *see, e.g.*, Drinkwater, *supra* note 142 (speculating on the significance of *Google v. Vidal-Hall* and how it may allow for more, successful international actions for data privacy and breach).

246 *Contra* Hartzog & Solove, *supra* note 44, at 2294, 2297-99; Jules Polonetsky & Christopher Wolf, FUTURE OF PRIVACY FORUM, *The US-EU Safe Harbor: An Analysis of the Framework's Effectiveness in Protecting Personal Privacy* 1-2 (2013).

247 *Contra* Gathani, *supra* note 66, at 33 (positing that the FTC's rulemaking authority should reduce rather than expand); James C. Cooper et. al., *Theory and Practice of Competition Advocacy at the FTC*, ANTITRUST L.J., 1091, 1101, 1104, 1110-11 (2005).

248 *See* Serwin, *supra* note 48, at 811.

249 *See* Berin Szoka & Geoffrey Manne, *Now in its 100th year, the FTC has become the Federal Technology Commission*, TECHFREEDOM (Sept. 26, 2013), http://techfreedom.org/post/62344465210/now-in-its-100th-year-the-ftc-has-become-the/.

250 *See* Hartzog & Solove, *supra* note 44, at 2246.

251 *See id.* at 2266.

252 *See id.* at 2265-75; *but see* SOLOVE & SCHWARTZ, *supra* note 53.

253 *See* Hartzog & Solove, *supra* note 44, at 2263, 2266 (arguing that the FTC has only scratched the surface of its powers' reach and should continue to stretch its bounds. The FTC must keep pace with the constantly evolving issues of data protection and technological innovation).

254 *See id.* at 2289; *see* 15 U.S.C. § 45(a)(2).

Scholars have compared the FTC's current development to that of a common law system, but this is too slow and incremental to keep pace with the ever-changing technological environment.[255] Perhaps in more stagnant areas of law this would suffice, but data privacy law is best assessed in an international context rather than as an issue confined within the bounds of the United States.[256] While advocates for the FTC to develop its authority in a manner similar to the common law cite compelling rationales, it would be an unnecessary effort.[257] Additionally, the milder penalties and shorter probationary timeframes for Section 5 violations suggested by the authors do not entice companies to remain diligent in their efforts to continuously amplify their data protection procedures.[258] Especially for companies who may incidentally fall subject to the GDPR's provisions, preemptive actions by the FTC, rather than just reactions to Section 5 violations, would quickly develop U.S. data privacy law standards before international conflicts and suits can emerge.[259] Accordingly, a slow developing common-law approach is an ineffective solution to close the vast privacy protection gap between the United States and the rest of the developing world; mainly, the European Union.[260]

The ability for the European Union to quickly institute broad privacy protections across all of its Member States has stemmed from its recognition of the fundamental right to privacy.[261] Though the United States' Constitution does not explicitly address personal data privacy as a fundamental right in the way that the European Union's Charter of Rights has evolved, Congress has the authority to create a regulatory agency.[262] But rather than create a new agency, Congress should simply amend the FTC Act to authorize explicit authority to

---

255 *But cf.* Hartzog & Solove, *supra* note 44, at 2294 (agreeing that the FTC must expand and develop its jurisprudence and their bottom-up approach needs to be more transparent to benefit companies).

256 *See generally A Global Standard for Data Protection Law*, PRIVACY INT'L, https://privacyinternational.org/impact/global-standard-data-protection-law (last visited Nov. 14, 2018).

257 *See generally* Hartzog & Solove, *supra* note 44, at 2265, 2294 (describing that the rapid growth of the data privacy law field far outpaces that of most areas of law that found a common law approach effective).

258 *See generally id.* at 2298.

259 *Contra id.* at 2299 (explaining that because the development of global data privacy law far outpaces that in the United States, even though persons in the U.S. remain subject to its provisions, the area of law must develop at a rate compatible to the rest of the developing world).

260 *See generally id.* at 2270.

261 *See* Charter of Fundamental Rights of the European Union, 2000, arts. 7, 8, 2012, O.J. C 326/02; *see also* Fromholz, *supra* note 154, at 462.

262 U.S. CONST. art. I §§ I, VII.

the FTC over the field of data privacy.[263] Additionally, there should be an amendment of the Magnuson-Moss rulemaking standards, within the data privacy context. Such an amendment would expedite the FTC's rulemaking process, such as through simple notice-and-comment procedures.[264] This would allow the FTC to quickly implement a plan to strengthen data protection across a vast number of industries, much like how the DPD raised its standards for all of the E.U. Member States, based on industry input and concerns.[265] Rather than continuing to state best practices or issue consent decrees, which do not create any substantive law, the FTC would be able to more easily promulgate legally enforceable data protection standards that best serve industry practices.[266] If the FTC adopts a similar hybrid of DPD and GDPR, standards of uniformity can begin to develop across multiple industries across the entire United States.[267]

Broadly, the FTC could implement a uniform rule that would require every company processing consumer data to create, maintain, and implement data protection measures throughout all their business operations.[268] The FTC should provide additional specifications which could then be further defined to raise data protection and quality requirements in response to the developing world.[269] By the end of an allotted compliance period, data protection in the United States will have risen to a level that reduces the growing gap between U.S. and E.U. data privacy and security laws.[270] While not ideal, the GDPR's approach is the

---

263 *See* Solove & Hartzog, *supra* note 44, at 606 (stating that in the FTC, the United States has the basic framework in place for a data privacy and protection regulatory regime; however, limitations on its effectiveness occurs through a lack of express power to occupy the field and to develop rules).

264 *Contra* Gathani, *supra* note 66 (criticizing the FTC's use of its best practices power as a way to circumvent the procedural guidelines for promulgating binding rules under the Magnuson-Moss Act).

265 Council Directive 95/46, 1995 O.J. (L 281) 31, 32 (EC); Fromholz, *supra* note 154, at 469.

266 Solove & Hartzog, *supra* note 86, at 604-06 (describing the FTC's current regulatory authority).

267 *See* Fromholz, *supra* note 154, at 467-70 (illustrating that the DPD creates a blanket coverage of privacy law over the E.U. Member States, without heed towards specific industries and use).

268 Council Directive 95/46 art. 6, 1995 O.J. (L 281) 31 (EC) (identifying data quality requirements for data processors to abide by when processing personal data. Similar provisions would provide adequate instruction for data protection standards required by companies irrespective of their industries); *see also* Lawrence J. Spiwak, *Insight: Digital Privacy Requires a Cohesive Federal Solution*, BLOOMBERG L. (June 13, 2018), https://www.bna.com/insight-digital-privacy-n73014476440 (calling for cohesive privacy and data legislation).

269 *See* Hartzog & Solove, *supra* note 44, at 2271 (explaining that because the development of technology and third country data standards are unpredictable, rulemaking authority would allow the FTC to take an active role in ensuring data protection instead of only being able to respond to unfair and deceptive practices).

270 *See id.* at 2271.

new global standard given the uniformity it creates, and the United States must further develop its privacy laws.[271] The United States must quickly progress by beginning with increased FTC authority and rulemaking capabilities.[272]

The importance of privacy protection in the developing world has become more vital in ensuring international trade relations.[273] Because personal data privacy is a fundamental right in many countries, the United States cannot remain ignorant to this fact by simply attempting to contract around it.[274] Instead, Congress must explicitly grant the FTC authority over data processing entities in the United States and the rights to promulgate rules.[275] Once the FTC becomes a more significant authoritative body in the data protection field, then the United States can begin to develop its privacy laws in a fashion similar to the European Union.[276] Because United States privacy law should develop in an international context, Congress should allow the FTC to more easily promulgate rules that encapsulate the international aspects of data.[277] Even if the burden is not

---

271 Council Regulation 2016/679, 2016 (EU) (General Data Protection Regulation); *see, e.g.*, Kerry, *supra* note 148 (mentioning proposals to Congress to adapt the Consumer Privacy Bill of Rights developed in the Obama administration as a starting point for comprehensive privacy legislation).

272 *See* Hartzog & Solove, *supra* note 44, at 2289-99; *see also* Fred Donovan, *FTC Wants Expanded Authority in Data Security, Privacy*, HEALTHIT SECURITY (July 19, 2018), https://healthitsecurity.com/news/ftc-wants-expanded-authority-in-data-security-privacy (FTC Chairman Joseph Simons explaining the House Energy and Commerce Committee's digital commerce and consumer protection subcommittee that FTC "wants the ability to impose civil penalties in privacy and data security cases, authority over nonprofits and common carriers, and authority to issue implementing rules under the Administrative Procedure Act (APA)").

273 *See* Brookman, *supra* note 11, at 355-56; O'Connor, *supra* note 115 (describing how current U.S. privacy and data laws "put U.S. companies at a disadvantage globally as emerging economies adopt simpler, and often more-EU style, comprehensive approaches.").

274 Tan, *supra* note 22, at 662-63 (comparing the level of emphasis and significance countries around the world place on data privacy as a fundamental right and how the United States lags behind many countries in this respect).

275 *Cf.* Hartzog & Solove, *supra* note 44, at 2289-300 (supporting the expansion of the FTC's authority and jurisdiction, but in a common law manner, as previously discussed in this Note); *see also* Donovan, *supra* note 272 (FTC Commissioners advocating FTC needs "greater authority in the privacy and data security area," and Congress needs "to give the agency the ability to impose financial penalties and develop 'sensible safeguards that can evolve with the marketplace.").

276 *Cf. id.* at 2289-99 (discussing areas of regulatory improvement for the FTC and agreeing the impetus for privacy law development within the United States is more power and action by the FTC); *see also Oversight Of The Federal Trade Commission Before the Subcomm. on Digital Commerce and Consumer Protection on Energy and Commerce*, 115th Cong. 9 (2018) (statement of Rep. Bob Latta) (discussing how "it's time to look at ways to reduce barriers to FTC consumer protection" in relation to data privacy by helping it move forward with rulemaking).

277 *See* Robert Bond, *Data Privacy is going Global*, LEXOLOGY (Sept. 10, 2018), https://www.lexology.com/library/detail.aspx?g=430e4aa4-8120-4444-9fe5-d8d525ecf362

lessened, the FTC must still promulgate a rule to shape United States privacy law.[278] Raising global privacy standards require nations, not just individual companies, to have adequate data protections in place.[279] Irrespective of if Congress eases the burden on the FTC's rulemaking authority, the FTC must create a privacy rule to govern data privacy and protection within the United States.[280] The existence of this rule will help absolve potential organizational liability for inadequate data protection practices, especially when no data transfer agreement exists between the United States and the foreign country.[281] The need for a rule is apparent, but first the FTC must address two issues. First, whether data standards should follow a DPD approach or a GDPR approach and second, how to ease the burden on companies when implementing this FTC rule.[282]

1. The GDPR Approach: A Shortcut to FTC Success

The FTC should follow the GDPR's approach in creating a uniform standard for data privacy and protection to be adhered to by all the states.[283] Currently, states are acting on their own to create minimum data privacy standards and rights.[284] Like common law, interpretation of privacy law and applicable

(explaining that data protection laws in South Africa, the Middle East, Canada, and much of Asia are heavily influenced as a result of the British Commonwealth and former British rule).

278 *Contra* Gathani, *supra* note 66, at 31 (calling for a restraint in rulemaking so that the free market can develop practices on its own); *see* Donovan, *supra* note 272 (FTC Commissioner Rohit Chopra urging Congress that the FTC needs rulemaking authority so that it can confront the risk to the economy, society, and national security of inadequate data security and privacy.").

279 *See* THE PRIVACY, *supra* note 61, at 280-81 (discussing how international data transfer agreements, such as the Safe Harbor Agreement, are more successful when each country's individual standards adequately comply with the others).

280 *See* Solove & Hartzog, *supra* note 86, at 604-06 (calling for an increase in the FTC's power and presence within the field of data privacy and protection).

281 *See* McCormac, *supra* note 27 (outlining proactive steps that companies should, but do not always, take in conducting international data transfers without the protection of a trade agreement); *see also* Olorunnipa et al., *supra* note 31 (detailing how the current executive administration has enveloped an inward protection approach to foreign policies, which may result in an absence of international data transfer agreements to protect companies).

282 *See* Gilbert, *supra* note 27 (discussing the impact that the GDPR will have on businesses globally and what steps companies should take to prepare for its impact).

283 *But cf.* Jolly, *supra* note 40 (discussing how individual states within the United States have set their own data privacy and protection standards); *see* Spiwak, *supra* note 268 (calling for cohesive privacy and data legislation).

284 *Privacy Protections in State Constitutions*, *supra* note 109 (providing a list of the ten states who have incorporated privacy rights within their constitutions); Aaron Mak, *Vermont, California Charging Ahead of Congress on Data Privacy Laws*, SLATE (May 29,

standards leads to inconsistencies across jurisdictions.[285] This situation resembles that of the European Union prior to its enactment of the DPD.[286] The DPD became outdated with the development of technology and as Member States adapted their policies at varying degrees.[287] This complicated trade amongst Member States, spurring the movement for a uniform standard.[288] Rather than repeat the European Union's efforts, the United States should forego the intermediary DPD-like-structure and instead adopt the uniformity approach set forth by the GDPR.[289]

The easiest way for the United States to develop its privacy law and to comply more effectively with rising global standards is for the FTC to make a rule setting a uniform standard across the country.[290] The DPD became obsolete because European Union Member States set varying standards above and beyond the minimum prescribed by the DPD; therefore, impeding trade amongst the Member States.[291] At this point, the United States has not set any sort of

---

2018, 2:40 PM), https://slate.com/technology/2018/05/state-level-data-privacy-laws-are-leapfrogging-congress.html (discussing how Vermont implemented the first data broker law in the country).

285 Fromholz, *supra* note 154, at 470 (stating that in the United States, privacy refers to a variety of contexts, resulting in a broad understanding of privacy as a general concept rather than in the specific context of data privacy); Amy Talbott, *Privacy Laws: How the US, EU and others protect IoT data (or don't)*, ZDNET (Mar. 7, 2016, 4:11 PM), https://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/ (describing that privacy laws vary by state).

286 *See* Fromholz, *supra* note 154, at 468-69 (explaining that prior to the DPD, the European Union allowed its Member States to govern their own privacy laws, which complicated data transfers and trade amongst one another); *see also* Bowman, *supra* note 11 (detailing the structure of privacy law in the European Union prior to the enactment of the DPD and GDPR).

287 Bowman, *supra* note 11 (describing the need for data privacy law reform with changing technology).

288 *Id.*

289 Nick Ismail, *Should the US adopt GDPR?* INFORMATION-AGE (Nov. 7, 2017), https://www.information-age.com/us-adopt-gdpr-123469401/ (arguing that cybercrime demands protection similar to GDPR with strict penalties to engender compliance); *but see IBM Executives Press U.S. Lawmakers Not to Adopt EU Privacy Law*, ITPROTODAY (May 15, 2018), https://www.itprotoday.com/risk-and-compliance/ibm-executives-press-us-lawmakers-not-adopt-eu-privacy-law (arguing the U.S. should have privacy law tailored to its needs and not adopt GDPR).

290 *See* Bowman, *supra* note 11 (illustrating the perpetual increase in technology signals that global data privacy and protection standards are going to increase for the foreseeable future, with the GDPR setting the bar); Emilio Iasiello, *Will the U.S. Adopt Similar GDPR Privacy Concerns??*, CYBERDB, https://www.cyberdb.co/will-u-s-adopt-similar-gdpr-privacy-concerns/ (last visited Sept. 15, 2018) (arguing for security standards in the U.S. supervised by the FTC).

291 *The data protection directive versus the GDPR: understanding key changes*, GDPR REPORT (Mar. 6, 2018), https://gdpr.report/news/2018/03/06/data-protection-directive-versus-gdpr-understanding-key-changes/ (describing data breach notification laws which

standard; therefore, states are free to develop this area of law creating inconsistencies.[292] While critics argue that this organic development of the law better serves the purpose of developing the law and gaining industry acceptance, it is an unsustainable practice because data transcends the borders of the United States.[293] By taking the initiative to develop privacy law on its own, the United States can avoid international lobbying for a global standard, or governing agency for data privacy and protection.[294]

Data flows freely throughout the world, and the United States cannot be complacent in its non-development as global standards continue to increase.[295] If the GDPR does not create a global standard, scholars have posited that the United Nations should establish an international data privacy organization to govern global data privacy standards.[296] This would even further complicate the United States' efforts to flip the script on its data privacy standards in a zero to sixty fashion.[297] To avoid this scenario, the FTC does not need to raise U.S. data standards to the height of global best practices; instead, standards must simply be set to an acceptable level that is compatible for international trade absent separate trade agreements.[298] By following the path of the GDPR at a national level rather than through a global organization, the FTC can promulgate a rule outlining a uniform standard for data privacy without having to idly wait decades for privacy law to develop on its own or succumb to abide by stringent global

---

vary by member states, became uniform under GDPR).

292 *See* Jolly, *supra* note 40 (comparing how states have chosen to approach data privacy law and how California has set the standard among the states).

293 *Compare* Gathani, *supra* note 66, at 27 (calling for a decrease in the FTC's issuance of best practices standards so that industries can develop themselves), *and* Hartzog & Solove, *supra* note 44, at 2289, 2293-94, 2296-97, 2299-300 (promoting a common law style of privacy law development in the United States), *with* Gilbert, *supra* note 27 (explaining the global impact of the GDPR on businesses and international transactions), *and see* Gallego et al., *supra* note 178 (discussing the implications of the GDPR on business practices and the stringent data transfer, use, and maintenance requirements that will be imposed).

294 De Hert & Papakonstantinou, *supra* note 173, at 315, 318-22 (advocating for an international agency to govern global data privacy if the GDPR is not universally adopted as the standard for countries to comply with).

295 Solove & Schwartz, *supra* note 116, at 897, 900, 902 (contending that the United States' current privacy law regime is unequipped to remain viable in international data transfers).

296 De Hert & Papakonstantinou, *supra* note 173, at 315, 318-22.

297 *See id.* at 316-19 (noting complications that a global organization would face in its development, and the burden it would have on countries, such as the United States, that would have to significantly amend its privacy law framework to adhere to any standard established).

298 *See* Schwartz, *supra* note 21, at 1974-75; Graham Greenleaf, *International Data Privacy Agreements after the GDPR and Schrems*, 139 PRIVACY LAWS & BUS. INT'L REP. 1, 2, 5-6, 8 (2016) (describing how the U.S. can shape trade agreements; however, the E.U. may not negotiate away privacy rights).

standards.[299] An FTC rule to effectively meet global data privacy standards would significantly lessen the burden on industries to comply.[300]

2. Easing the Burden of Implementation for an FTC Rule

While certain aspects of an FTC rule should be roughly based on the standards set by the GDPR, the FTC must decide how to best implement a rule without overburdening companies and industries.[301] The GDPR's standards for data privacy and protection are burdensome to implement, especially in the United States where the existing standards are far inferior.[302] While the GDPR limits liability for non-compliance in third-party countries to only those organizations that collect or process the personal data of E.U. citizens, the continual globalization of information and data threatens to envelop nearly all businesses across the globe.[303] The FTC does not need to emulate such a burdensome standard; instead, the FTC only needs to set its standards at a level adequate to comply with, and protect those effected by, the GDPR.[304]

Currently, most organizations lack information about the GDPR's expansive and stringent provisions.[305] On one hand, many companies that operated under the Safe Harbor Agreement have already prepared for international data trade absent a negotiated agreement between the United States and the European

---

299 Solove & Hartzog, *supra* note 86, at 586, 589-90 (arguing that the FTC has developed a common law that can serve as a basis for a data privacy regulatory regime).

300 *Id.* at 669, 672-73, 675-76 (arguing that the FTC is well poised to make meaningful data privacy regulation).

301 Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1185-86, 1226 (arguing that FTC guidance is needed for the rapidly progressing Internet of Things industries).

302 Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65, 92 (2017); Griffin Drake, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 164, 178, 184-85 (2017).

303 *See* Gallego et al., *supra* note 178 (discussing how the GDPR only applies to United States organizations when they process the personal data of E.U. citizens, yet the constant spread of information projects that every business will cross paths with this sort of data at some point); *see also* Gilbert, *supra* note 27 (stating "[t]hus, any website or mobile application that promotes goods or services and is available for access by EU/EEA based individuals is within the scope of the GDPR").

304 *See* Gallego et al., *supra* note 178; *see* Foley Hoag LLP, *FTC Seeks to Hold Companies to GDPR Promises*, JDSUPRA (July 11, 2018), https://www.jdsupra.com/legalnews/ftc-seeks-to-hold-companies-to-gdpr-60206/ (discussing the FTC's role in making sure that U.S. companies live up to GDPR standards).

305 Merrion, *supra* note 204 (noting how the majority of businesses throughout the world lack preparation for the GDPR and uninformed of its implications and potential impacts on international business dealings).

Union.[306] However, with uncertainty surrounding the viability of the Privacy Shield, companies are left to prepare for trade in compliance with the GDPR's heightened standards absent negotiated international trade agreements.[307] Alternatively, companies that have not worried about international trade compliance and who were not affected by the Safe Harbor Agreement and the DPD may soon find themselves within the GDPR's scope.[308] Even though an FTC rule prior to the GDPR's implementation is not feasible, the FTC should set a timeframe for compliance soon after to prevent companies from being subject to harsh non-compliance liability.[309] While the burden of implementing new policies required under an FTC rule may seem staggering to companies, it is slight in comparison to the GDPR's penalties and potential economic benefits.[310] To ease the burden of implementing more stringent standards, an FTC rule should require the creation of data privacy organizations and compliance units at an industry-wide level rather than on a per business basis.[311]

Proponents for allowing individual businesses to create their own data privacy compliance programs fail to take into account cost feasibility for smaller organizations, and the effects of varying industry practices.[312] Only larger firms

---

306 McCormac, *supra* note 27 (explaining how the "Safe Harbor" framework provided companies with a "simplified process for the transfer of personal information from Europe to the U.S.").

307 *See* Scott, *supra* note 32; *see generally* Nancy Harris, *A practical guide to the European Union's GDPR for American businesses*, RECODE (May 16, 2018), https://www.recode.net/2018/5/16/17360944/gdpr-us-business-eu-european-union-data-protection-privacy (discussing the various methods companies are using to prepare for the extensive GDPR regulations).

308 *See* Gallego et al., *supra* note 178; *see also* Gilbert, *supra* note 27 (discussing the global impact of the GDPR, both on businesses expecting the GDPR's effects and on those unaware of its provisions).

309 *See* Merrion, *supra* note 204 (explaining that outside of Europe only 22 percent of firms said they were prepared for the GDPR and that there is a lack of awareness when it comes to the impacts of noncompliance); *see also* Council Regulation 2016/679, art. 83(6), 2016 O.J. (L 119) 83 (EU) (stating that fines for non-compliance and violations of the GDPR can range from the greater of 20,000,000 EUR, or 4% of annual worldwide turnover for violations of basic GDPR principles, to the greater of 10,000,000 EUR or 2% of turnover for other lesser violations).

310 *See* Council Regulation 2016/679, art. 84, 2016 O.J. (L 119) 83 (EU) Regulation (EU).

311 *See* Gilbert, *supra* note 27 (explaining that implementation of the GDPR will require "close collaboration between the industry on one end, and governments and their agencies on the other.").

312 Dana Simberkoff, *GDPR Affects Small Businesses Too*, CMSWIRE (Feb. 20, 2018), https://www.cmswire.com/information-management/gdpr-affects-small-businesses-too/ (explaining that while GDPR compliance is difficult for all organizations, small businesses face greater challenges as they "simply may not have the money to put a detailed, high-tech security program into place"); *see, e.g.*, *How the GDPR impacts and suffocates small and medium businesses*, I-SCOOP (2016), https://www.i-scoop.eu/gdpr/gdpr-small-medium-businesses/ (explaining the unintended negative impacts of the GDPR specifically on small

have the capital necessary to quickly establish the requisite data protection departments and to hire the necessary personnel.[313] Expected costs attributed to increased data protection requirements, especially for companies without preexisting standards, are quite high, making it nearly impossible for smaller businesses to comply in their own in a timely manner.[314] Additionally, compliance by only a portion of the industry complicates domestic dealings within the industry due to the inability to ensure equal levels of data privacy and protection between companies.[315] A lack of standard policies would either inadvertently lead to GDPR violations or create numerous data screening obstacles to ensure adequate protection throughout its life cycle.[316] Instead, the FTC's rule creating data protection agencies would spread the costs so that more businesses could guarantee compliance, establish industry data standards, and be relieved of the burden of tracking developments in international privacy law.[317]

Not all companies were subjected to the GDPR upon its implementation.[318]

---

businesses and how those businesses can prepare for GDPR regulations).

313 *See* Ray Schultz, *The Price of Compliance: Study Uncovers GDPR Costs*, MEDIAPOST (Oct. 26, 2017), https://www.mediapost.com/publications/article/309342/the-price-of-compliance-study-uncovers-gdpr-costs.html (explaining how new hires that will help with GDPR compliance will cost firms hundreds of thousands of dollars).

314 *See* Simberkoff , *supra* note 312 ("GDPR compliance is certainly no small undertaking, and it will require a major shift for many companies, particularly for smaller organizations that may not have privacy programs in place."); *see also* Coase, *supra* note 125 (discussing the impact of heavy burdens and transactional costs on effective, and efficient, financial decision-making).

315 *See* Daniel Mikkelsen et al., *Tackling GDPR compliance before time runs out*, MCKINSEY & CO. (Aug. 2017), https://www.mckinsey.com/business-functions/risk/our-insights/tackling-gdpr-compliance before-time-runs-out (explaining how "many aspects of GDPR will be gradually resolved through industry practices and codes of conduct."); *see also* Allen Pogorzelski, *GDPR Coping Strategies: Keeping Calm and Working Toward Compliance*, FORBES (Aug. 23, 2018, 9:00 AM), https://www.forbes.com/sites/forbescommunicationscouncil/2018/08/23/gdpr-coping-strategies-keeping-calm-and-working-toward-compliance/#31d07f3e1a02 (stating that 15% of companies are completely ignorant to GDPR standards, whereas 15% are strategically choosing not to comply).

316 *See* Sara Degli-Esposti & Maureen Meadows, *GDPR: 10 easy steps all organisations should follow*, SILICON REPUBLIC (Mar. 16, 2018), https://www.siliconrepublic.com/enterprise/gdpr-coventry-university (explaining how the GDPR "is about improving industry standards" and ensuring organizations are "not alone" in their compliance efforts).

317 Gilbert, *supra* note 27 ("In the next two years, we hope to have the opportunity to receive and analyze guidelines and comments from the various bodies responsible for the interpretation and enforcement of the GDPR to assist with the transition to the new data protection regime of the EU/EEA. In the meantime, it will continue to be a challenge to comprehend and interpret the new rules created by the GDPR.").

318 *See id.*

However, businesses must approach GDPR compliance as if it will affect them within the next few years.[319] The FTC should ease the burden of implementation by using its promulgated rule to address GDPR compliance at the industry level rather than by attempting to distinguish between which individual business will be affected and when.[320] This approach would ease compliance with the GDPR because appropriate safeguards of data involved in transfers between countries can rely upon the approval of codes of conduct.[321] Industry standards for data protection and GDPR compliance industry agencies will better protect all United States businesses from GDPR violations.[322] The FTC already publishes industry best practices; therefore, a rule creating industry agencies to monitor data protection and compliance standards is not far beyond the FTC's current operations and is vital to the development of the United States' privacy law.[323]

IV. CONCLUSION

Technological developments continue to ease and increase the collection, maintenance, storage, and transmission of data.[324] Within seconds, companies can collect and transmit data all across the globe.[325] However, with large data comes immense liability as more countries and their citizens become concerned

---

319 *Id.*

320 *See* Nate Lord, *What is GDPR (General Data Protection Regulation)? Understanding and Complying with GDPR Data Protection Requirements*, DIGITAL GUARDIAN (Sept. 19, 2018), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection; *see generally* Merrion, *supra* note 204 (explaining how the GDPR affects all industries and compliance efforts need to account for this fact).

321 *See* Council Regulation 2016/679, art. 49, 2016 O.J. (L 119) 64 (EU); *see also* Myers, *supra* note 182 (explaining that though not contained in the DPD, the GDPR allows the use of codes of conduct to demonstrate GDPR compliance while still allowing for a self-regulated structure. To qualify, codes of conduct "may be prepared by associations or other bodies representing controllers or processors, and may be drawn up to address many aspects of the GDPR including international data transfers.").

322 *See* Myers, *supra* note 182 ("Adherence to these codes of conduct by controllers or processors not otherwise subject to the regulation, but involved in the transfer of personal data outside the EU, will help a regulated controller demonstrate adequate safeguards.").

323 *See What We Do*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do (last visited Sept. 12, 2018) (outlining what the FTC does to protect and educate consumers).

324 *See* Shangquan, *supra* note 2 (discussing economic globalization through the rise of big data); James Wickes, *Why Life Under GDPR will Encourage Technological Innovation*, INFO SEC. (June 21, 2018), https://www.infosecurity-magazine.com/opinions/gdpr-encourage-technology/.

325 *See* Pologeorgis, *supra* note 2 (discussing the rise of international trade in correlation with the continuous development of the use of technology in everyday business); *see* Cory, *supra* note 231 (explaining that the "increased digitalization of organizations . . . has increased the importance of data as an input to commerce" in the modern global economy).

with personal data privacy and protection.[326] Leading the pack is the European Union, which strengthened its stance on data privacy and protection through its enactment of the GDPR.[327] The GDPR is the new global standard that affects any and all nations that involve the controlling or processing of personal data for E.U. citizens.[328] Nations must prepare to comply with these strengthened standards; otherwise, their business can be held liable.[329]

When it comes to data privacy law, the United States is inept because, unlike the rest of the world, it fails to approach this rapidly expanding legal field.[330] Rather than stay on top of data privacy law, Congress continues to allow the FTC, a regulatory body not designed to develop law, to serve as the United States' primary data privacy and protection authority.[331] This structure will likely soon fail as the rapid growth of international regulations threatens to adversely impact international data transfers and trade.[332] Growth in the United States' protectionist policies could further frustrate efforts to negotiate compromises that allow for an assortment of international trade industries.[333] As the predominant data privacy authority in the United States, the FTC must promulgate a rule to spur increased United States data protection standards to prevent U.S. companies from falling behind within the global economy.[334]

---

326 *See* Brookman, *supra* note 11, at 356 (explaining how consumers are calling for stronger limitations on commercial data collection).

327 *The EU General Data Protection Regulation Questions and Answers*, HUMAN RIGHTS WATCH (June 6, 2018, 5:00 AM), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation; *See Data Protection in the EU*, EUROPEAN COMM'N (2018), https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (explaining that "the regulation is an essential step to strengthen individuals' fundamental rights in the digital age," such as the fundamental right to data protection).

328 *See* Gallego et al., *supra* note 178 (discussing the territorial scope of the GDPR and how it affects businesses located outside of the European Union).

329 *See id.*

330 *See* Brookman, *supra* note 11, at 367 (explaining how "Congress has failed to make meaningful progress on statutory data privacy reform in recent years").

331 *See id.* at 359 (explaining that despite the FTC's vigilance, Congress must act in certain areas of privacy law); O'Connor, *supra* note 115 (discussing how the FTC has "attempted to establish a data-security baseline through over sixty different enforcement actions").

332 *See* McCormac, *supra* note 27 (discussing how "the different approaches of the EU and the US toward data privacy have created compliance challenges for businesses seeking to transfer personal information about customers and employees from Europe to the US").

333 *See, e.g.*, Toluse Olorunnipa et al., *supra* note 31 (speculating on current protectionist approaches towards foreign relations and how it may affect the negotiation of future international trade agreements).

334 *See* Hartzog & Solove, *supra* note 44, at 2289 (agreeing that the development of privacy law within the United States is dependent upon the scope of the FTC's authority and its jurisdiction); *FTC Releases Annual Privacy and Data Security Update*, FED. TRADE COMM'N (Jan. 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-releases-annual-privacy-data-security-update ("The Commission is the nation's primary

Absent Congress passing a federal data privacy law, or easing the Magnuson-Moss rules, the FTC must face the burden of promulgating a rule governing data privacy and protection.[335] The implementation of uniform data standards across the states would ease domestic trade because businesses and industries would all need to remain compliant with one national standard.[336] Additionally, the creation of industry agencies would allow industries to adapt beyond the set general standards needed to comply with international trade inherent within the industry.[337] It is evident that the United States must improve its data privacy laws to keep pace with the rest of the world, and through the FTC, it is possible.[338]

---

privacy and data security enforcer.").

335 *See* 15 U.S.C. § 1455(b) (stating that regulations promulgated by the Federal Trade Commission are subject to hearings and judicial review); *see generally Understanding the Magnuson-Moss Warranty Act*, MLM LAW, https://www.mlmlaw.com/library/guides/ftc/warranties/undermag.htm (last visited Sept. 15, 2018).

336 *See* John M. Culbertson, *The Folly of Free Trade*, HARV. BUS. REV. (Sept. 1986), https://hbr.org/1986/09/the-folly-of-free-trade (explaining that free exchange only occurs when there is a uniform framework of laws and regulations); Hartzog & Solove, *supra* note 44, at 2248 (agreeing that the development of privacy law within the United States is dependent upon the scope of the FTC's authority and its jurisdiction).

337 *See generally EU Compliance: General Data Protection Regulation (GDPR)*, GEMALTO, https://safenet.gemalto.com/data-protection/data-compliance/european-union-eu-compliance/ (last visited Sept. 12, 2018) (discussing the effect that the GDPR will have on U.S. companies); *see* Jeff John Roberts, *The GDPR Is in Effect: Should U.S. Companies be Afraid?*, FORTUNE (May 25, 2018), http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/ (explaining the "Brussels Effect" which involves the EU creating its own regulations and other states around the world eventually raising their standards to match that of the E.U.'s).

338 *See* Hartzog & Solove, *supra* note 44, at 2294 (advocating for greater FTC presence within the field of data privacy law to raise U.S. data protection standards); Harris, *supra* note 307 (explaining that the GDPR impacts companies around the world and has become the data protection law that has received the greatest attention).