Washington University Global Studies Law Review

Volume 17 | Issue 3

2018

Post-Digital Era Reconciliation Between United States and European Union Privacy Law Enforcement

Nidhi Narielwala
Washington University School of Law

POST- DIGITAL ERA RECONCILIATION BETWEEN UNITED STATES AND EUROPEAN UNION PRIVACY LAW ENFORCEMENT

INTRODUCTION

The concept of privacy rights for citizens is not unique to the twenty-first century. Though modern privacy law deals largely with the privacy in one's digital presence, its origins date back to the Bill of Rights.[1] The founding fathers recognized that citizens have a right to privacy from government intrusion in certain spheres of their lives.[2] The ransacking of colonial homes in the eighteenth century by the English government spurred the drafting of the Fourth Amendment.[3] The privacy barriers provided by the Fourth Amendment included protections within safe spaces, such as the home, as well as the requirement of warrants to enter locked areas.[4] The universality of privacy intrusions, however, developed after the Digital Revolution; the rise of technology has eroded the previously established barriers, creating new gaps in privacy protections.[5]

---

1 *See* Elliot's Debates, *infra* note 26 (explaining that Patrick Henry in 1788 argues for a Bill of Rights that restrains the government from searching citizens' homes).

2 *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 117-18 (2015).

3 Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 54-55 (1996) (discussing the impact of the Fourth Amendment on the British colonies). *See also Writ of Assistance*, ENCYCLOPÆDIA BRITANNICA, https://www.britannica.com/topic/writ-of-assistance (last visited Feb. 17, 2018). A writ of assistance was a search warrant in the 1700s where the British colonies in America were subject to general searches of their homes for contraband. *Id.* The practice was very controversial and the colonies fought back in court on the legality of the writs. *Id.* "When similar warrants were expressly reauthorized by the Townshend Acts (1767), they were challenged for five years in every superior court in the 13 colonies and refused outright in 8 of them." *Id.*

4 *The Bill of Rights: A Brief History*, ACLU, https://www.aclu.org/other/bill-rights-brief-history (last visited Mar. 4, 2018). The United States' Bill of Rights was a direct response to the lack of privacy felt by colonies under British rule in the eighteenth century. *Id.* The Fourth Amendment created a right to privacy from governmental intrusions into one's "persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. CONST. amend. IV. The requirement of a warrant issued by a judge made sure that the government was unable to abuse their power of policing.

5 Riley v. California, 134 S. Ct. 2473, 2495 (2014). U.S. Supreme Court Chief Justice John Roberts wrote in *Riley* that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* Roberts understood the importance of privacy and boundaries in a world where technology does not. Technology has no concept of boundaries and barriers; it is pervasive in

Implementing comprehensive privacy laws to prevent intrusions or seek legal recourse is paramount given the ease of digital access to personal information.

The Federal Trade Commission (FTC) was founded in 1914 to help regulate businesses with the specific goal of consumer protection.[6] When the issue of privacy in a consumer context was brought to the public's attention, alongside the rapid development of sophisticated technology, there was a consumer-driven campaign for privacy regulation.[7] As a response, the FTC was put in charge of data privacy regulation in addition to its role as a consumer protection agency.[8] The FTC has passed numerous regulations in an effort to control data collection, use, and transfer by private companies and government entities, but these are not sufficient to combat the growing risk of data breaches by hackers.[9]

The United States (U.S.) needs an independent agency that oversees data protection, such as those set up in the European Union (EU) by the General Data Protection Regulation (GDPR).[10] The GDPR encompasses a

---

everyday life.

6 *Our History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/our-history (last visited Mar. 4, 2018).

7 *See* ROBERT GELLMAN & PAM DIXON, MANY FAILURES: A BRIEF HISTORY OF PRIVACY SELF-REGULATION IN THE UNITED STATES 5 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf. Robert Gellman is a privacy and information policy consultant, and Pam Dixon is the Executive Director of the World Privacy forum. *Id.* at 2. Together they wrote a report on the self-regulation of privacy rules by companies in various industries due to the increase demand from consumers. They discuss the positives to self-regulating industries but also touch on the many shortcomings of this model. *Id.* The issue with self-regulation is that the standards created by the industries quickly become obsolete as technology changes.

> The standards promulgated by the self-regulatory programs were often general and quickly became outdated because of technology and other changes. It appears that audits or reviews of compliance with self-regulatory standards were often not attempted, not completed, not credible, or not transparent. Finding original documents is often difficult or impossible now.

Id. at 9. Now that data is no longer kept in file cabinets, the traditional lock and key privacy enforcement is obsolete. Also, the FTC is lacking in authority due to its statutory limitations. *Id.* at 5. The need to create a feasible self-regulatory standard is more important than ever.

8 *Id.* at 17.

9 *Id.* Regulations such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and Children's Online Privacy Protection Act (COPPA) are all industry-specific privacy laws that the FTC enforces. *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE, *infra* note 60, at 1, 5.

10 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter "GDPR"], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en. The European Parliament passed this regulation on April 27, 2016 and stated that natural persons have a fundamental right in the protection of the processing of personal data. *Id.* The GDPR was set in motion by Commissioner Viviane Reding, who was the European Commission's Vice President from 2010 to 2014. *The EU General Data Protection Regulation*, ALLEN & OVERY, http://www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx (last visited Mar. 4, 2018). She published proposals to reform

variety of protections for entities with data privacy needs across the EU. Unlike the U.S., the EU has specific provisions when it comes to the enforcement of its privacy regulations, specifically the requirement of a Data Protection Officer for any entity that controls or processes personal data.[11] This across-the-board requirement differs from the privacy regulations in the U.S., which are dependent on the industry and type of personal information.[12] For example, information collected in the health care industry is more closely regulated due to the sensitive nature of patient-specific data.[13] The GDPR, however, requires each entity that deals with consumer data to appoint a Data Protection Officer.[14] The tasks of a Data Protection Officer are described in further detail in Article 39 of the GDPR.[15] The GDPR also includes provisions on how Data Protection Officers will be regulated, including provisions that delineate the consequences for violating the Regulation.[16] These consequences mostly consist of imposing administrative fines or penalties.[17] Companies may be

---

European data protection regulations in January of 2012. *Id.* The GDPR was finalized and agreed to on December 17, 2015 and will go into effect on May 25, 2018. *Id.*

11 *The Data Protection Officer (DPO)*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (last visited Mar. 4, 2018). The GDPR is unique because it requires companies to either hire a Data Protection Officer or have one working for the company on a contract basis. *General Data Protection Regulation*, CGE, https://www.cgerisk.com/2017/07/ (last visited Mar. 4, 2018). This individual's sole job description is to make sure consumer's data, as well as other confidential data, held by the company is well-protected. *Id.*

> A DPO reports to management but is expected to work independently and without direction. His primary concern is protecting data and enabling compliance, not facilitating shortcuts or finding legal loopholes in the Regulation. The organization he is working with is expected to provide any necessary resources the DPO requires to perform his tasks, such as office space, staff, equipment, and any other necessary resources. He must be involved in all areas of data protection within the organization he works with and must be notified of all data processing and protection issues or concerns in a timely manner.

Id. Since this is mandated by a regulation, the DPO will not be subject to management politics; he will work separately as to make sure his reports aren't swayed by other officers. *Id.*

12 O'Connor, *infra* note 126.

13 INST. OF MED. COMM. ON HEALTH RESEARCH & PRIVACY OF HEALTH INFO., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 158 (Sharyl J. Nass et al., eds. 2009), https://www.ncbi.nlm.nih.gov/books/NBK9573/.

14 GDPR, *supra* note 10, art. 37 (outlining the designation of a Data Protection Officer by controllers and processors).

15 *Id.* art. 39. The European Parliament passed this regulation on April 27, 2016 and stated that natural persons have a fundamental right in the protection of the processing of personal data. GDPR. *Id.*

16 *Id.* arts. 83-84.

17 *Id.* at 83. *See also* Courtney Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER ROSE PRIVACY LAW BLOG (Dec. 23, 2015), http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ (outlining the fines and penalties listed in the GDPR). Article 79 has raised eyebrows due to its stringent policies on violations. There is a possibility of incurring fines up to "4% of the

subject to a fine of 4% of the company's worldwide annual turnover, which may not seem significant, but can potentially make a significant impact for large companies.[18] These fines can be levied for a variety of noncompliance reasons, such as failing to implement basic processing principles or misapplying the rules to cross-border data transfers.[19] Higher fines will be imposed for egregious violations, such as the violation of the data subjects' rights.[20]

Technology plays an important role in the international economy and has made it easier for companies to operate on a global level. However, these companies have access and control over their consumers' sensitive personal data and have yet to perfect the protection of that data from outside intruders and governmental entities.[21] Because world is quickly shrinking as the development, use, and abuse of technology grows on a global scale, it is more important than ever to create parallels between EU and U.S. privacy laws. While the FTC's enforcement is stern, its power is limited in its reach due to the lack of wholly encompassing privacy laws.[22] Comparatively, the EU's privacy laws are extensive, but they lack in enforcement of those laws. As the Dutch Data Protection Authority Chairman, Jacob Kohnstamm, stated in a privacy panel about global privacy policies, "[T]he EU legislation and U.S. enforcement together is hell." [23] A thorough analysis of the differences between the U.S. and the

company's total worldwide annual turnover" for violating GDPR provisions, such as rules on cross-border data transfers. *Id.* Bowman expresses concerns of companies on Article 79 since 4% of some companies may mean millions of dollars in fines. *Id.*

18 *Id.*

19 *Id. See also* ALLEN & OVERY, THE EU GENERAL DATA PROTECTION REGULATION 5 ((2017), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf).

20 GDPR, *supra* note 10, art. 83 (listing factors that are taken into account when deciding the amount of an administrative fine).

21 GELLMAN & DIXON, *supra* note 7, at 26-27.

22 *Id.* at 27. The FTC's lacking enforcement and limited power have led to holes in the US's privacy law.

> The Federal Trade Commission has no effective means of issuing privacy regulations because of current limits on its statutory authority. This is a structural problem that essentially compels the agency to look favorably at self-regulation because it has no alternative to offer. The FTC can always recommend legislation, but it is not clear that an FTC recommendation will be influential, that privacy legislation can pass the Congress, or that the FTC can manage to support any legislative recommendation.

Id. If the FTC is unable to correctly influence privacy-related legislation, then consumers have no choice but to demand better privacy self-regulation from companies.

23 Allison Grande, *Google Working To Fix Privacy Policy, Dutch Regulator Says*, LAW 360 (Mar. 6, 2015), http://www.law360.com/articles/628844/google-working-to-fix-privacy-policy-dutch-regulator-says. In March 2015, Dutch Data Protection Authority Chairman Jacob Kohnstamm spoke at the International Association of Privacy Professionals' annual global privacy summit in Washington. *Id.* He discussed Google's privacy policies and also commented on the EU's plans to propose a unified data protection regulation, referring to the GDPR. *Id.* In that context, he stated "Someone said at a

EU's privacy laws and enforcement tactics is required to determine what approach is best going forward. Reconciliation between the U.S. and the EU's privacy laws is ultimately inevitable, but a timely resolution is essential to prevent potentially catastrophic global data breaches.

Part I of this Note will give a broad overview of the conception and development of contemporary privacy law. Part II will discuss the rise of U.S. and EU enforcement agencies and the differences of enforcement tactics between the two entities. Part III will incorporate the impact of developing technology on privacy rights and why technology plays an important role in our understanding and enforcement of privacy rights. Part IV will demonstrate the usefulness of reconciling differences between U.S. and EU enforcement tactics and privacy rights. Finally, Part V will propose possible avenues of reconciliation, based on the current state of privacy law. Overall, the aim of this Note is to lay out the differences in privacy right enforcement between the EU and the U.S. and to push for an integrated enforcement effort as technology increases the risk of privacy violations on a global scale.

I. DEVELOPMENT OF PRIVACY LAW

This section covers the chronological progression of privacy law in both the U.S. and the EU. In the U.S., the Fourth Amendment serves as the foundation for recognizing privacy rights for citizens, while in the EU, the passing of a French data protection law functioned as an introduction to privacy law. Though modern society requires some variances to accommodate for advancements in technology, the initial framework presented by these privacy law precursors remain relevant.

A. U.S. Privacy Law

Privacy law, being a relatively novel idea, developed at a similar pace in the U.S. and Europe. In the U.S., the Fourth Amendment was ratified in 1791 to protect citizens from governmental intrusions.[24] The framers of the Constitution recognized this right after incidents of the British government intruding upon colonial homes.[25] As Patrick Henry stated in 1788 when

certain point that the EU legislation and U.S. enforcement together is hell, and that's what it's going to be I guess." *Id.*

24 U.S. CONST. amend. IV.

25 The Bill of Rights (1688), 1 Will. & Mary, sess.2 c.2, http://www.legislation.gov.uk/aep/WillandMarSess2/1/2#reference-c2144673 (last visited Mar. 4, 2018). The British Bill of Rights of 1689 did not have a Fourth Amendment equivalent. Instead, it

advocating for the Bill of Rights, "[t]hey may, unless the general government be restrained by a bill of rights, or some similar restriction, go into your cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear. They ought to be restrained Within proper bounds."[26] The Bill of Rights, in general, was the founders' response to the colonials' lack of privacy within their homes.[27] However, many American privacy scholars will argue that the conversation of privacy rights within a legal context dates directly back to the 1890 Harvard Law Review article written by Samuel Warren and Louis Brandeis called "The Right to Privacy."[28] It was written as a direct response to the invention and widespread use of Kodak cameras in 1888, which changed the manner in which society was able to view and disseminate the intimate details of a stranger's life.[29] This article is most remembered for the section below:

Then the "right to life" served only to protect the subject from

---

narrowed down basic civil rights recognized over past centuries. These rights included (1) the requirement of authorization by Parliament before passing a law, (2) right the petition the monarch free of fear of retribution, or (3) freedom of speech. *Id.* The British Bill of Rights of 1688 also addressed topics such as excessive bail, standing armies during peace time, and election guidelines for Parliament, but there was no protection against governmental intrusions into your home. *Id.*

26 Patrick Henry, *Speech at the Convention of the Commonwealth of Virginia on the Adoption of the Federal Constitution (June 14, 1788)*, *in* 3 THE DEBATES IN THE SEVERAL STATE CONVENTIONS OF THE ADOPTION OF THE FEDERAL CONSTITUTION, 448–49 (Jonathan Elliot ed., 1827) [hereinafter "Elliot's Debates"]. Patrick Henry gave multiple speeches before the Virginia Ratifying Convention in June of 1788, passionately expressing his belief that a Bill of Rights in the Constitution was necessary to explicitly reserve rights for citizens. Gordon Lloyd, *Ratification of the Constitution*, TEACHINGAMERICANHISTORY.ORG, http://teachingamericanhistory.org/ratification/virginia/ (last visited Mar. 4, 2018). Henry opposed the adoption of the Constitution and argued that certain clauses of the Constitution could lead to "impending tyranny and doom." *Id.* Henry was extremely vocal about his belief that the Constitution, as written, should have amendments and a Bill of Rights so that Congress cannot use the necessary and proper clause to abuse Congressional power. *Id. See also* U.S. CONST. art. I, § 8, cl. 18 ("[Congress shall have Power] [t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.").

27 Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY, PLI 4-5 (2006).

> At the time of the Revolutionary War, the central privacy issue was freedom from government intrusion. The Founders detested the use of general warrants and writs of assistance. Writs of assistance authorized ''sweeping searches and seizures without any evidentiary basis' and general warrants ''resulted in "ransacking" and seizure of the personal papers of political dissenters, authors, and printers of seditious libel.

Id.

28 Samuel Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 205 (1890).

29 RICHARDS, *supra* note 2, at 17 (noting that the invention of the Kodak camera and the camera's invasive impact on the elite started the discussion about privacy law). Before the instant camera, there was no worry about a private moment being captured and disseminated throughout society. When elites felt that their social status was threatened by the new wave of newspaper reporters armed with Kodak cameras, Robert Warren sought out Brandeis to write an article about limiting the press and the "need for a legal right to privacy." *Id.*

> battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, — the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession — intangible, as well as tangible . . . . But if privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting.[30]

This section of text from the article serves as the foundational basis of the current tort of "invasion of privacy."[31] Warren and Brandeis' argued that the right of privacy was already 'recognized' by the common law by using a branch of cases that protected the injury of emotional harm from unwanted action or attention to demonstrate that the common law already protects privacy.[32]

Though the argument made by Warren and Brandeis is not incorrect in its conclusion that privacy has been historically protected by common law, their article failed to take into consideration future advancements in technology and the resulting impact of said technology on privacy rights. Currently, the privacy law framework consists of industry-specific legislation that requires a piecemeal approach to privacy law enforcement within the U.S.[33]

B. European Privacy Law

Alternatively, the European development of privacy law started in France. France was the first European country to enact a privacy law specifically addressing data protection in 1978.[34] The French Parliament placed penalties such as imprisonment and maximum fines for any

30 Warren & Brandeis, *supra* note 28.

31 *Id.* at 218 (explaining that invasion of privacy is viewed as a tortious, intentional wrong by an individual).

32 *Id.* at 198.

33 Asay*, infra* note 48, at 17.

34 Molly Guinness, *France Maintains Long Tradition of Data Protection*, DEUTSCHE WELLE (Jan. 26, 2011), http://dw.com/p/105Yl. In the 1800s, the right of privacy in France was limited to very specific situations, such as limiting the press, interfering with mail, and "violating a 'professional secret' by 'physicians, surgeons and other health officers, as well as pharmicists, midwives and all other persons . . . .'" Wenceslas J. Wagner, *The Development of the Theory of the Right to Privacy in France*, 1971 WASH. U. L. Q. 45, 48-49 (1971).

individual, company, or government agency that collected or processed personal data without explicit authorization.[35] This significantly contributed to the creation of the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," which was enacted by the Council of Europe in 1981.[36] This document was the first major international privacy law policy addressing protection of personally identifiable data.[37] Shortly thereafter, in 1993, the EU was formed, consisting of six founding countries: Belgium, France, West Germany, Italy, Luxembourg, and the Netherlands.[38] By 1995, there were a total of fifteen member countries,[39] and they voted in "The European Union Directive on Data Protection of 1995."[40] This Directive "mandated that each EU nation pass a national privacy law and create a Data Protection Authority to protect citizens' privacy and investigate attacks on it."[41]

This Data Protection Directive was the overarching data protection regulation within the EU until the passing of the General Data Protection

---

35 *Id.*

36 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108 [hereinafter "Protection of Personal Data Convention"], https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

37 *Details of Treaty No. 108*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (last visited Mar. 5, 2018) ("The Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.").

38 *Inner Six*, WIKIPEDIA, https://en.wikipedia.org/wiki/Inner_Six (last visited Mar. 5, 2018). Eventually, more countries acceded to the European Union to create the current twenty-eight-member countries: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. *Member State of the European Union*, WIKIPEDIA, https://en.wikipedia.org/wiki/Member_state_of_the_European_Union (last visited Mar. 5, 2018). However, the UK voted to leave the European Union on June 23, 2016. *Brexit*, WIKIPEDIA, https://en.wikipedia.org/wiki/Brexit#2016_referendum (last visited Mar. 5, 2018).

39 *Europe Without Frontiers*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/history/1990-1999_en (last visited Mar. 5, 2018). The fifteen countries are as follows: Germany, France, Italy, the Netherlands, Belgium, Luxembourg, Denmark, Ireland, United Kingdom, Greece, Spain, Portugal, Austria, Finland and Sweden. *Id.* This information is available on the European Union's official website, which is managed by the Communication Department of the European Commission. *Id.*

40 Directive 95/46/EC of the European Parliament and 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), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012 [hereinafter "Data Protection Directive"].

41 Bob Sullivan, '*La Difference' is Stark in EU, U.S. Privacy Laws*, NBC NEWS (Oct. 19, 2006, 11:19 AM), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.WCDCWOErLfY.

Regulation (GDPR) in May of 2016.[42] The European Commission, the drafters of the GDPR, believed that "[t]he principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."[43] This comprehensive initiative by the EU creates an umbrella of privacy protections across all member states. The European Commission "intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."[44] The GDPR was meant to govern any European-based 'data controller,' controller,' which includes any corporation or government agency that collects and/or processes personal data.[45] The European Commission, in their press release about the GDPR, defines "personal data" as "any information relating to an individual, whether it relates to his or her private, professional or public life.[46] It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address."[47] With this background of privacy law in mind, the question of enforcement of these laws arises.

II. THE RISE OF ENFORCEMENT AGENCIES

Although the concept of privacy law developed at a similar pace in the U.S. and EU, the current application and enforcement of such laws are vastly different. The following section follows the US and the EU's efforts to regulate privacy.

A. United States

Over the years, the U.S. developed a piecemeal approach to privacy law, operating under a combination of "industry-specific and state laws, ad

42 GDPR, *supra* note 10.
43 *Id.* at art. 2.
44 *Id.*
45 *See* GDPR, *supra* note 10, art. 4.
46 Press Release, European Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.
47 *Id.*

hoc FTC enforcement, and self-regulation."[48] This makes it extremely difficult for entities that collect and use personal data to know exactly how the law applies in their situation. Privacy law in the U.S. differs by industry: Fair Credit Reporting Act (FCRA) covers consumer reporting agencies;[49] The Gramm-Leach-Bliley Act (GLBA) monitors financial institutions;[50] Health Insurance Portability and Accountability Act (HIPAA)[51] regulates covered entities that have access to an individual's personal health information;[52] Telecommunications Act of 1996 covers communications businesses, such as television stations and cable services;[53] and Children's Online Privacy Protection Act (COPPA) governs online commercial websites or services directed to children thirteen years old or under.[54] These are just a few examples of the piecemeal regulation of privacy in the United States. However, both the Senate and House of Representatives have recently introduced the Consumer Privacy Protection Act of 2017. In the Senate, Senator Patrick Leahy from Vermont introduced the bill on November 14, 2017.[55] In the House, Representative David Cicilline introduced the bill on October 19, 2017.[56] The above bills are an attempt to consolidate the current piecemeal

---

48 Clark D. Asay, *Consumers: The Missing Piece in a Piecemeal Approach to Privacy*, AAAI PUBL'NS, Spring 2010, at 17.

> By contrast, the information privacy landscape in the United States was more of a tabula rasa. Its patchwork system reflected no deep commitment to a specific implementation framework and no institutional authority vested in defending a specific approach. Against this backdrop, the expression of privacy's value in terms of promoting consumer trust proved influential in the United States in a way that rights-based arguments had not. Historically, successful legislative efforts, with a few notable exceptions, were mounted in response to specific and egregious harms or to protect highly sensitive information.

KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 185 (2015).

49 Fair Credit Reporting Act, 15 U.S.C. §§ 1681(b)-1681a(f) (Supp. IV 2016).

50 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, §§ 6821-6827 (1999).

51 Asay, *supra* note 48, at 18.

52 Covered entities include: health plans, health care providers, health care clearinghouses and, in some cases, business associates of the same. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

53 Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

54 15 U.S.C. § 6502 (Supp. II 2014); *see also* Asay, *supra* note 48, at 18.

55 Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. (2017). The bill states that "Congress finds that . . . it is important for business entities that own, use, store, or license sensitive personally identifiable information to adopt reasonable policies and procedures to help ensure the security and privacy of sensitive personally identifiable information . . . ." *Id.* § 2. There was a previous version of this bill introduced in the Senate back in April of 2015, but it was not enacted. Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015).

56 Consumer Privacy Protection Act of 2017, H.R. 4081, 115th Cong. (2017). There was a previous version of this bill introduced in the House of Representatives back in July of 205, but it was not enacted. Consumer Privacy Protection Act of 2015, H.R. 2977, 114th Cong. (2015).

approach within the US.[57] Due to the lack of support, however, the chances of either bill advancing are slim.[58] If either Bill is passed, business entities that collect, use, transfer or store personal consumer information would be required to "implement a comprehensive consumer privacy and data security program."[59] Until that day comes, industry-specific piecemeal regulations will continue to govern the collection and use of personal data.

The above industry-specific regulations are all governed by different enforcement agencies. For example, the FTC regulates FCRA, GLB, and COPPA.[60] The FTC was first created in 1914 to protect consumers from unfair competition tactics between businesses.[61] It then took on the enforcement of consumer privacy rights in the 1970s, when FCRA was passed.[62] The FTC employs various methods of enforcement, which are dependent on the outcome of its investigations into violations.[63] The most common and well known is an FTC Consent Order issued under Section 5 of the Federal Trade Commission Act.[64] The consent order is an opportunity for companies who have violated the Federal Trade Commission Act to avoid litigation and settle the issue with the FTC.[65] The consent orders generally require the companies to immediately stop any practices or acts that the FTC has found to be a violation.[66] These consent orders normally have a term of twenty years during which the

57 Consumer Privacy Protection Act of 2017, *supra* notes 55-56 and accompanying text.

58 For a prognosis on both bills, see *H.R. 4081: Consumer Privacy Protection Act of 2017*, Govtrack, https://www.govtrack.us/congress/bills/115/s2124 and https://www.govtrack.us/congress/bills/115/hr4081 (last visited Mar. 5, 2017).

59 Consumer Privacy Protection Act of 2017, *supra* notes 55-56, § 202(a)(1). This consumer privacy and data security program would be designed to protect the privacy and the security of personal consumer information. *Id.* § 202(a)(2).

60 Fed. Trade Comm'n, Privacy & Data Security Update 5, at 7 (2017), https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.

61 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Mar. 5, 2018).

62 *Protecting Consumer Privacy*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited Mar. 5, 2018).

63 Federal Trade Commission Act, 15 U.S.C. § 45(b) (West 2006) [hereinafter "FTCA"].

64 *Id.* § 45(m)(1)(B) (West 2006).

65 *Id.* § 45(m)(3) (noting that the Commission may settle any action so long as it is followed by a public statement and receives Court approval). *See also A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, Fed. Trade Comm'n, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last revised July 2008).

66 Christie Grymes Thompson et al., *FTC Consumer Protection Investigations and Enforcement*, Practical Law (2014), https://www.kelleydrye.com/getattachment/9f51cc0b-540a-4c26-8e75-12be6282b42b/attachment.aspx.

FTC will monitor company practices for compliance.[67] The FTC has investigated and uncovered data security violations in more than fifty companies in the last thirteen years,[68] each of which settled with consent orders.[69]

If a settlement is not reached through a consent order, litigation becomes unavoidable. Since the FTC is a federal agency, it is bound by administrative law and procedure. The FTC has the "authority to direct and supervise the implementation of particular legislative acts."[70] Like many other administrative agencies, the FTC functions as a rule-maker, investigator, enforcer, and adjudicator. Due to potential conflicts of interest between each of these roles, the FTC must follow stringent procedures, such as appointing an independent decision maker to preside over the FTC's complaint proceedings.[71] The process for FTC investigations is outlined below.

First, the FTC files a complaint under 15 U.S.C. § 45(b) when it has, "'reason to believe' that a party is 'using an[] unfair method of competition or unfair or deceptive act or practice.'"[72] Next, an administrative law judge (ALJ) is assigned to the matter, hears the case, and makes a decision.[73] However, the ALJ decision is not absolute because

---

67 *See* Policy Statement Regarding Duration of Competition and Consumer Protection Orders, 16 C.F.R. § 3 (1995). *See generally* Duration of Existing Competition and Consumer Protection Orders, 60 Fed. Reg. 58,514 (Nov. 28, 1995). Based on the "Sunset Rule" issued by the FTC back in 1995, consent orders generally terminate within twenty years. *Id.*

68 Ryan T. Bergsieker et al., *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 The Colo. Law. 39, 40 (2015), https://www.gibsondunn.com/wp-content/uploads/documents/publications/Bergsieker-Cunningham-Young-FTC-Data-Security-Enforcement-06.2015.pdf.

69 *Id.*

70 Administrative Agency, FREE DICTIONARY, http://legal-dictionary.thefreedictionary.com/Administrative+Agency (last visited Mar. 5, 2018). The Federal Trade Commission Act gives the FTC the authority to both legislate and enforce the governing law. See FTCA, supra note 63, § 45(a) (2).

71 *Office of Administrative Law Judges*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/office-administrative-law-judges (last visited Mar. 5, 2018). *See also* Administrative Procedure Act, 5 U.S.C. § 3105 (1946) [hereinafter "APA"].

72 Todd N. Hutchison, *Understanding the Differences Between the DOJ and the FTC*, AMERICAN BAR ASS'N, www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/understanding_differences.html (last visited Mar. 5, 2018).

73 *Id.*

> The FTC files a complaint when it has "reason to believe" that a party is "using an[] unfair method of competition or unfair or deceptive act or practice." 15 U.S.C. § 45(b). An administrative law judge (ALJ) hears the matter, and either party may appeal the ALJ's decision to the full Commission. This process may result in a cease-and-desist order, which the FTC can enforce by pursuing an injunction or civil penalties in federal court.

Id.

either party has the right to appeal the decision to the FTC Board; once the appeal process is complete and a company is found to have violated trade practices, the company will receive a cease-and-desist order.[74] This order can be enforced by the FTC "by pursuing an injunction or civil penalties in federal court."[75]

An example of such an order used for privacy purposes was in 2012 when the FTC investigated Google for violating the privacy of its consumers when launching a program called Google Buzz.[76] The investigation started in February of 2011 when a public interest group based out of Washington, D.C., the Electronic Privacy Information Center (EPIC), filed a complaint with the FTC against Google.[77] EPIC claimed Google attempted to "convert the private, personal information of Gmail subscribers into public information for the company's social network service Google Buzz."[78] Based off of these allegations, the FTC opened an investigation into the matter, charging Google for violating the Federal Trade Commission Act of 1914.[79] The FTC's Complaint for Civil Penalties and Other Relief outlined the allegations it made against Google, stating that:

> Google misrepresented to users of its Gmail email service that: (1) Google would not use their information for any purpose other than to provide that email service; (2) users would not be automatically enrolled in the Buzz network; and (3) users could control what information would be public on their Buzz profiles.[80]

Google eventually settled with the FTC via a consent order, which went into effect on October 13, 2011.[81] The consent order obligated

---

74 Id.

75 Id.

76 EPIC v. FTC (Enforcement of the Google Consent Order), EPIC, https://epic.org/privacy/ftc/google/consent-order.html#background (last visited Mar. 5, 2018).

77 Id.

78 Complaint at 1, In re Google, Inc., (2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.

> This change in business practices and service terms violated user privacy expectations, diminished user privacy, contradicted Google's own privacy policy, and may have also violated federal wiretap laws. In some instances, there were clear harms to service subscribers. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

Id.

79 *Id.* at 13.

80 Complaint at 2, United States v. Google, Inc., No. CV12-04177, (N.D. Cal. 2012).

81 Order at 7, *In re* Google, Inc., No. C-4336, (2011).

Google to create a comprehensive privacy program to ensure Google's customer data is protected.[82] Google also agreed to privacy audits by an independent party over the course of twenty years.[83] Additionally, Google agreed to be transparent with its customers by not misrepresenting

> [T]he extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including but not limited to, misrepresentations related to: (1) the purpose for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.[84]

This 2011 consent order was imperative to industry-regulated privacy rights because it set a much-needed bar for companies collecting customer personal data.

The following year in 2012, Google was fined $22.5 million in civil penalties for violating this consent order.[85] This is the highest fine to date, which serves as a demonstration of the lengths to which the FTC will go to protect consumer data.[86]

B. European Union

The General Data Protection Regulation recently entered into force on May 24, 2016 and shall apply from May 25, 2018 onwards.[87] The GDPR

---

82 *Id.*

> IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information.

83 *Id.*

84 *Id.*

85 Statement of the Comm'n, United States of America v. Google Inc. (United States District Court for the Northern District of California) In the Matter of Google Inc., FTC Docket No. C-4336, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlestatement.pdf.

> The Federal Trade Commission has approved a proposed federal court consent order imposing a $22.5 million civil penalty on Google Inc., the highest fine ever levied for violation of a Commission consent order. That the violations alleged in the Commission's federal court complaint have warranted so significant a penalty signals to Google and other companies that the Commission will vigorously enforce its orders.

Id.

86 *Id.*

87 GDPR, *supra* note 10, art. 99.

is only applicable to personal data processed by data controllers within the EU or personal data that pertains to a data subject whose "behaviour takes place within the [European] Union."[88] The GDPR requires any such entity to have systems in place to protect the data. One of these systems requires the company to either internally create the role of a Data Protection Officer or to hire a consultant; either option should monitor internal practices and ensure the company complies with the standards set by the GDPR.[89] If a company opts to internally create the role, their Data Protection Officer is required to have expert knowledge about data protection law, but the actual level of knowledge depends on the data controller's "data processing operations . . . and the protection required for the personal data processed by the [data] controller or the processor." [90] This requirement needs to be implemented by May 25, 2018, after which companies will be held accountable for noncompliance.[91]

Each of these Data Protection Officers will have to report to a supervisory authority[92] provided by each member state.[93] Article 51 of the GDPR requires each member state to appoint an agency to monitor controllers and processors of personal data.[94] The European Commission strongly believes this to be an "essential component of the protection of natural persons with regard to the processing of their personal data," as explained in Article 117 of the GDPR.[95]

---

88 GDPR, *supra* note 10, pmbl. para. 24.

89 *Id.*

> The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Id.

90 GDPR, *supra* note 10, pmbl. para 97.

91 GDPR, *supra* note 10, art. 99.

92 GDPR, *supra* note 10, art. 4, para. 21 (defining "'supervisory authority' [to mean] an independent public authority which is established by a Member State pursuant to Article 51").

93 GDPR, *supra* note 10, art. 51, para. 1.

> Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Id.

94 *See generally* Bowman, *supra* note 17.

95 GDPR, *supra* note 10, pmbl. para 117.

> The establishment of supervisory authorities in Member States, empowered to perform their

Since the GDPR requires an officer within the company to help oversee the company's privacy practices, it also shifts the cost of providing the officer onto the company. This pushes the cost of complying with the regulation to the consumer, by making the service or product higher to offset any net profit. Although consumers will have to bear a portion of the cost for better privacy practices, their investment will be returned in the form of stronger protections for their personal data.

C. Differences in Enforcement Tactics between the United States and the European Union

This section analyzes the key differences in enforcement tactics for privacy laws between the U.S. and the EU. While the former uses a piecemeal approach to regulate through the FTC, the latter takes a collective approach to regulating the data collection and use of their constituents.[96]

From the above analysis, it is clear that the EU has a different approach to the enforcement of privacy laws from the U.S. Whereas the FTC is charged with investigating different types of data protection violations in separate industries with varying standards, the EU created a privacy law umbrella by holding all entities that collect and process personal data to the same standard.[97] Even though the FTC is thorough with its investigations, the current piecemeal regulations leave gaps in the law that are growing daily as technology advances.[98]

> tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

Id.

96 Asay, *supra* note 48, at 17. *See also* Ustaran, *infra* note 97.

97 Eduardo Ustaran, *Is EU Privacy Law Enforcement About to Become a Team Effort?*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (June 27, 2014), www.hldataprotection.com/2014/06/articles/international-eu-privacy/eu-privacy-law-enforcement-a-team-effort/.

98 Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

> The gaps in privacy laws have grown exponentially since then. There is a public outcry today—as there should be—about NSA surveillance, but the breadth of that surveillance pales in comparison to the data that Google, Apple, Facebook, and legions of app developers are collecting. Our smartphones track our movements and habits. Our Web searches reveal our thoughts. With the wearable devices and medical sensors that are being connected to our smartphones, information about our physiology and health is also coming into the public domain. Where do we draw the line on what is legal—and ethical?

Id.

Today, most companies that collect, use, transfer, and store consumer personal data have an international consumer base. When considering personal data, most consumers place less significance on the specific location of the data than on the methods by which this data is protected. It is important to note that there is a cultural component behind this campaign for better data protection regulations. The U.S. has a history of distrust with centralized governments[99] which led to the creation of the Fourth Amendment.[100]

Comparatively, the EU has not shown a similar level of distrust of their governments nor have they had major issues with centralized governments.[101] Having a general social expectation of privacy, France was at the forefront of privacy law enactment in the EU.[102] A French law professor at Parris II University, Emmanuel Derieux, was interviewed about his view on French cultural sensibilities and their impact on the development of privacy law in France.[103] He stated, "It wasn't that the French authorities were a particular threat . . . Perhaps it's more of a sensitivity or sensibility. French people worried about the protection of their private life and their independence."[104] This notion dates back to the nineteenth century, where there was an article on the French Napoleonic code that recognized a right for individuals within society to live a private life.[105]

---

99 Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 UNIV. OTTAWA L. & TECH. J. 362, 357-95 (2005).

> On the whole, the US legislation we discuss provides citizens with greater protection against the collection and use of personal information by government, as opposed to the private sector. It is significant, as we shall see, that the EU Privacy Directive imposes limits on interactions in the market place. The US has been less willing to impose government restrictions on the private sector, and chooses to rely on market constraints, possibly reflecting Americans' traditional distrust of a centralized government.

Id.

100 PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 153 (1998).

> Americans historically have a strong suspicion of government and a relatively strong esteem for markets and technology, while Europeans have given government a more prominent role in fostering social welfare but have placed more limits on unfettered development of markets and technology. European governments regulate themselves less strictly with respect to open meetings and freedom of information laws, whereas they are stricter with respect to regulating the press and other private sector users of information.

Id.

101 *Id.*

102 *See generally* Guinness, *supra* note 34.

103 *Id.*

104 *Id.*

105 *Id.*

Although the concept of privacy has different origins and cultural backgrounds, its importance globally is paramount. As such, it may be these cultural differences that have led to the lack of parallels between privacy enforcement within the U.S. and the EU.[106]

III. IMPACT OF CHANGING TECHNOLOGY ON PRIVACY RIGHTS

This section covers the risks of technological advancements in data privacy, and how those risks have contributed to the development of privacy law.

Technology plays a huge role in the development of privacy law in the digital age. As barriers to accessing personal information become insignificant due to increased connectivity between users, the chances of abuse of personal information elevates with the increased risks and consequences. Every day there are new data points, as data collectors are requesting personal information from users. With the amount of space that technology has taken up in daily lives, "risks of harm, inequality, discrimination, and loss of autonomy easily emerge" on a day-to-day basis.[107] There are risks associated with any technology that purports to be making life easier. These risks include giving out personal information to unknown parties in exchange for access to a particular online program or service.[108] As an article in the Stanford Encyclopedia of Philosophy titled "Privacy and Information Technology" accurately stated, "your enemies may have less difficulty finding out where you are, [and] users may be tempted to give up privacy for perceived benefits in online environments . . . ."[109]

The risk increases even more as the Internet creates a global environment that can put distance between the victim and the perpetrator. When the Internet was first created, it was not designed to operate on a global scale between users who were strangers to one another. It was initially designed to connect a "community of people who knew each other

---

106 SWIRE & LITAN, *supra* note 100.

107 Jeroen van den Hoven et al., *Privacy and Information Technology*, STAN. ENCYCLOPEDIA OF PHIL., Spring 2016, § 2.1; *see generally id.* § 1.2.

> An important aspect of this conception of having privacy is that it is seen as a relation with three argument places: a subject (*S*), a set of propositions (*P*) and a set of individuals (*I*). Here *S* is the subject who has (a certain degree of) privacy. *P* is composed of those propositions the subject wants to keep private (call the propositions in this set 'personal propositions'), and *I* is composed of those individuals with respect to whom *S* wants to keep the personal propositions private. (internal citation omitted)

Id.

108 Van den Hoven, *supra* note 107.

109 *Id.*

in real life . . . ."[110] So the issue of privacy arose after the fact, which required developers or engineers to add privacy notices. Anyone who has used the Internet has accessed data and information that is stored on foreign servers. Since data is now being transferred across nations every day, the need for a global approach to privacy enforcement is more important than ever.[111] The personal sensitive data currently saved on servers across the world is not governed by an overarching privacy regulation. Thus, complete compliance with the data processing laws within each jurisdiction cannot be guaranteed.[112]

Big data also plays a role in the advancement of technology and the implementation of privacy rights.[113] The term "big data" refers to the collection of diverse data points, from numeric data to emails and videos, that are stored under one big data set.[114] Due to the sheer amount of data it contains, a big data set can be key in detecting patterns and trends.[115] A big data set allows companies to collect performance information to identify risks and increase productivity, while providing opportunities to make key business adjustments by forecasting future trends.[116] Big data is important in a privacy context because companies have been using consumer personal data and activities to track and monitor their actions.

---

110 *Id.* at § 2.2.

111 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 254 (2010).

> This research, as this Article's Conclusion describes, suggests ways that the prevailing debate over the adequacy of U.S. information privacy law ''on the books' might be diversified, just as Congress, the Obama Administration, and international organizations are revisiting national and global approaches to privacy. While bolstered procedural mechanisms for enhancing informational self-determination might be needed, pursuing that goal in a way that eclipses broader normatively grounded protections, or constrains the regulatory flexibility that permits their evolution, may destroy important tools for overcoming corporate overreaching, consumer manipulation, and the collective action problems raised by ceding privacy protection exclusively to the realm of individual choice.

Id.

112 Van den Hoven, *supra* note 107, § 1.5.

113 *Big Data What it is and Why it Matters*, SAS INST., http://www.sas.com/en_us/insights/big-data/what-is-big-data.html#dmimportance (last visited Mar. 5, 2018).

> The importance of big data doesn't revolve around how much data you have, but what you do with it. You can take data from any source and analyze it to find answers that enable 1) cost reductions, 2) time reductions, 3) new product development and optimized offerings, and 4) smart decision making.

Id.

114 *Id.*

115 JAMES MANYIKA ET AL., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY, MCKINSEY GLOBAL INST. (2011), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

116 *Id. See also* Athanassios M. Kintsakis et al., *Data-Aware Optimization of Bioinformatics Workflows in Hybrid Clouds*, J. BIG DATA, 2016, at 1, 16.

Companies can then compile all the information they have on a particular individual to predict or skew that individual's actions. This use of consumer data to essentially manipulate consumer actions is a violation of consumer privacy rights. Not only that, but governmental agencies have been asking companies over the past several years to release their data for national security reasons.

There are serious consequences to company and governmental use of data in this manner. If customers were aware of the fact that their purchases on Amazon, for example, were being used by the government to hunt for terrorists, there would be a societal uproar. It is becoming easier for companies to evade detection as they infringe upon privacy rights of their consumers because of the ever-changing and evolving technology that is readily available.

IV. ETHICAL IMPLICATIONS OF VIOLATING CONSUMER PRIVACY RIGHTS

As stated earlier, the culture of a community impacts the rules and laws governing that community. There are ethical implications for lacking privacy enforcement that cannot be overlooked. The government should be an ethical entity that protects the rights of its citizens and does not exploit their governmental authority. The most pertinent example that comes to mind is the National Security Agency (NSA) leak by Edward Snowden.[117] Back in June of 2013, an NSA intelligence contractor, Edward Snowden, leaked classified information regarding the NSA's tracking of millions of Americans.[118] The NSA was collecting telephone records of tens of millions of American citizens without their knowledge or consent, with the excuse of a national security risk.[119]

There are two sides to this discussion. On the one hand, the government is tasked with the job of protecting its citizens from terrorist attacks. With that goal in mind, the NSA, after the 9/11 attacks, created a domestic surveillance program that sifted through records of millions of Americans to find possible threats.[120] This program gave the U.S. government access, without a warrant, to call records and emails of U.S. citizens.[121] The average citizen who had no need to worry if the

117 *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964.

118 *Id.*

119 *Id.*

120 *How It Works*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/nsa-spying/how-it-works (last visited Mar. 5, 2018) (explaining how the NSA's domestic surveillance program was created and used to access calls and emails of US citizens).

121 *Id.*

government was listening was monitored through this program. Even though an individual that is abiding by the law in all respects has no need to worry about being watched, the mere presence of government affects our freedom. This is similar to how drivers tend to slow down, even if they are not speeding, when they see a police car around. Edward Snowden, in his own words, discussed his role in this leak:

> You know, everybody who is involved with this debate has been struggling over me and my personality and how to describe me. But when I think about it, this isn't the question that we should be struggling with. Who I am really doesn't matter at all. If I'm the worst person in the world, you can hate me and move on. What really matters here are the issues. What really matters here is the kind of government we want, the kind of Internet we want, the kind of relationship between people and societies. And that's what I'm hoping the debate will move towards, and we've seen that increasing over time. If I had to describe myself, I wouldn't use words like 'hero.' I wouldn't use 'patriot,' and I wouldn't use "traitor." I'd say I'm an American and I'm a citizen, just like everyone else.[122]

Snowden's leak mobilized organizations to rein in the NSA's spying abilities, and there was a clear shift in the policy landscape.[123] Organizations such as the Electronic Frontier Foundation worked together with coalition partners to pass the USA Freedom Act, which put limits on the NSA's surveillance capabilities.[124] This Act would not have passed without Snowden's leak.[125] The American people are now aware of the issues and are able to keep the U.S. government accountable for their actions.

The same ethical analysis can be applied to companies that store their consumers' personal data. Companies ought to be held responsible for protecting the data of their consumers from outside hackers. Consumers are relying on companies to do so because identity theft is a real threat now that information is so readily transferable. The difficulty for

---

122 Edward Snowden, *Here's How We Take Back The Internet*, TED TALKS, https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript?language=en (last visited Mar. 5, 2017).

123 Rainey Reitman, *3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance*, ELECTRONIC FRONTIER FOUND. (June 5, 2016), https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

124 *Id*. *See also* USA FREEDOM Act of 2015, H.R. 2048, 114th Cong. (2015).

125 Reitman, *supra* note 123.

companies is the lack of wholly-encompassing legislation that outlines the standards necessary for consumer privacy protection, regardless of the industry.

V. HOW TO RECONCILE GLOBAL PRIVACY LAW ENFORCEMENT DIFFERENCES

This section outlines the three different approaches available to the U.S. in regulating citizens' personal data as technological advancements increase: industry self-regulation, passing the Consumer Privacy Protection Act of 2017, or joining forces with the EU to create a regulation similar to the GDPR. While each approach has pros and cons, the ultimate goal is to protect the personal information of consumers.

There is a need for a more connective legal approach to data privacy between continents. The U.S. needs "a single comprehensive data-protection framework" that applies to all companies, regardless of sector or types of personal information.[126] Other countries, such as Japan and Canada, have shifted their focus to creating comprehensive privacy regimes that are congruent with the GDPR.[127]

There are three different solutions to the problem set forth above. The first solution is to let the industry regulate itself.[128] This approach may be more efficient than mandatory regulation.[129] While government regulations cannot be amended quickly to account for changing technology, a self-regulation approach can quickly adapt to technological innovations.[130]

The second solution is waiting for Congress to pass the Consumer Privacy Protection Act of 2017,[131] which would require business entities processing big data to implement reasonable policies and procedures to protect the privacy of personal consumer information.[132] The Consumer Privacy Protection Act is the closest piece of legislation that the U.S. has to the EU's GDPR. This would bridge the gaps that currently exist due to the backdoor piecemeal regulations that are in place today. However, given the long and arduous democratic process of getting a bill to become

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

127 *Id*.

128 Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 15, 17 (2015).

129 *Id*. at 17.

130 *Id*. at 16.

131 Consumer Privacy Protection Act of 2017, *supra* notes 55-56.

132 *Id*.

a law, especially one that would require companies to invest money in protecting their consumers' data, the probability of this option is low.

Finally, the third solution would be to join forces with the EU in creating a similar regulation to the GDPR within the US. This would not only include the drafting of the regulation itself but also the enforcement tactics of the FTC, which have proven to be firmer than those within Europe. If this is possible, we will be able to reconcile the differences in enforcement tactics and avoid global differences in privacy law and privacy enforcement. As stated in the Stanford Encyclopedia of Philosophy's article on *Privacy and Information Technology*, "[t]he challenge with respect to privacy in the twenty-first century is to assure that technology is designed in such a way that it incorporates privacy requirements in the software, architecture, infrastructure, and work processes in a way that makes privacy violations unlikely to occur."[133] The goal for the future of privacy law is to create a system of global privacy policies that can keep up with the rapidly emerging technology without compromising personal data.[134]

CONCLUSION

Based off the research outlined above and the analysis done on both domestic and foreign policies of privacy right enforcement tactics, it is clear that there is no one proper solution to the problem. The choice is between efficient or thorough enforcement of personal privacy rights. It also includes a democratic struggle between governmental oversight for national security and constitutional rights of private citizens. However, if the goal is to reconcile these differences on a global scale, it is best to join forces with the EU in creating a similar regulation to the GDPR where U.S. companies are held accountable for the safekeeping of consumer personal data.[135] It is no longer an option to let consumers bear the cost of protecting their data because technology has become such a big part of our lives. It is unreasonable to ask a customer to agree to risk their personal information just to access a product or service. The only other option would be to not use the product or service at all, which is, in all likelihood, not an option at all. Consumer personal information must be protected by those who collect, use, and store it, regardless of where in the world the company operates. To make sure of this, a comprehensive program must

133 Van den Hoven, *supra* note 107, § 1.5.
134 O'Connor, *supra* note 126.
135 Ustaran, *supra* note 97.

be put in place between the U.S. and the EU.

Nidhi Narielwala*

---

* Associate Editor, Washington University Global Studies Law Review; J.D. Candidate (2018), Washington University School of Law; B.S. cum laude, Business Administration (2014), Saint Louis University. I would like to thank all of the editors of the Global Studies Law Review for their hard work in preparing this Note for publication. I would also like to thank my parents and my brother for their continuous support and guidance throughout law school.