147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches

McKenzie L. Kuhn[*]

ABSTRACT: The 2017 Equifax breach, which endangered the personal financial information of 147 million Americans, was one of the worst data breaches in U.S. history. In light of this catastrophe and the growing number of mass data breaches, many privacy advocates and U.S. consumers have begun to advocate for federal data protection legislation. However, companies that thrive off big data, such as Facebook, Amazon, Google, and Equifax, have spent millions lobbying against data protection laws. As a result, the United States has no universal, federal data protection law. Many states and specific sectors of the economy, such as healthcare and finance, have tried to bridge this gap in legislation with their own data protection laws. However, businesses continue to collect, store, and sell the personal information of consumers with few consumer protections. In comparison, the EU recently passed the General Data Protection Regulation ("GDPR"), which guarantees EU citizens the fundamental right to data protection and forces companies to implement data protection regulations and baseline security measures when collecting personal information. Because of the growing risks to consumers due to recent mass-data breaches and the growth of "big-data" companies, this Note asserts that Congress should enact a federal data protection law, similar to the GDPR, that will adequately protect consumers from future mass breaches like the 2017 Equifax.

[*] J.D. Candidate, The University of Iowa College of Law, 2019; B.A., Denison University, 2016.

I. INTRODUCTION

Have you ever searched your name on Google and immediately found your phone number and home address on the very first page? Have you noticed that as you scroll on Facebook, the ads you see are tailored to your favorite stores and items? Have you ever wondered why certain apps on your phone track your GPS location, even when the app is not in use? Have you questioned whom your email address will be shared with when you sign up for a coupon on a store's website? Consumers are beginning to ask these questions in light of recent mass data breaches, like UnderArmour's "MyFitnessPal" in 2018, Equifax in 2017, LinkedIn and Yahoo in 2016, and eBay in 2014, which affected hundreds of millions of Americans. [1]

Technology has enabled phones, smart watches, and computers to recognize an individual's face and voice, to track a person's average heart rate and hours of sleep, or even to collect internet search history, financial information, and sensitive medical history. [2] Additionally, 70% of smartphone

1. Nick Turner, *Under Armour Says 150 Million MyFitnessPal Accounts Hacked,* BLOOMBERG (Mar. 29, 2018, 5:09 PM), https://www.bloomberg.com/news/articles/2018-03-29/under-armour-says-150-million-myfitnesspal-accounts-were-hacked; Elizabeth Weise, *Equifax Breach: Is It the Biggest Data Breach?*, USA TODAY (Sept. 7, 2017, 7:54 PM), https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001.

2. *Big Data: Why Do Companies Collect and Store Personal Data*, LE VPN (May 26, 2017), https://www.le-vpn.com/why-companies-collect-big-data. Technology has made it so that "[e]very time you

apps share the personal information they collect with third-party companies such as Google Analytics and Facebook Graph API.[3] Data collection gives companies the power to tailor their products and services to specific individuals. For example, Cambridge Analytica collected the private information from more than 50 million Facebook users in order to identify American voter personalities and sway their behavior in the 2016 Presidential election.[4] Of the 50 million individual accounts harvested, only 270,000 Facebook users consented to having their data collected, after being told it was to be used solely for academic purposes.[5] While the mass collection of individuals' data is helpful for businesses and some consumers, the problem arises when businesses invade the privacy of individuals by storing and, sometimes, losing their information, exposing those consumers to harm.[6]

While other countries have extensive data protection laws to protect consumers' personal information, the United States lacks universal, federal data protection laws.[7] Instead of calling for a law that would protect consumers from the progression of technology and globalization, many companies are actively lobbying against U.S. data protection legislation.[8] Equifax, a company that suffered a data breach that affected over 147 million Americans in 2017,[9] has spent millions lobbying in Congress against such protections.[10] Many states have attempted to fill the void of data protection laws by passing their own laws; however, large companies that rely on the collection of consumer data for revenue have thwarted these efforts by urging state legislatures to vote against such data protections.[11]

---

log onto the web, log into a website, open a new account, fill out a survey, answer a questionnaire or provide information—it is being collected, often solely for the purposes of resale, and often with your name or other easily identifiable personal information attached. Even without your name, IP addresses and other markers can be used to tie what you do today to other information currently available on the web." *Id.*

3. Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCI. AM. (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services.

4. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

5. *Id.*

6. *Big Data: Why Do Companies Collect and Store Personal Data*, *supra* note 2.

7. *See infra* Section II.A (explaining the sectoral based approach for data protection legislation in the United States).

8. Michael Rapoport & AnnaMaria Andriotis, *Equifax Lobbied for Easier Regulation Before Data Breach*, WALL ST. J. (Sept. 11, 2017, 10:39 PM), https://www.wsj.com/articles/equifax-lobbied-for-easier-regulation-before-data-breach-1505169330.

9. Merrit Kennedy, *Equifax Says 2.4 Million More People Were Impacted by Huge 2017 Breach*, NPR (Mar. 1, 2018, 1:19 PM), https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach.

10. Rapoport & Andriotis, *supra* note 8.

11. Corban Rhodes & Ross Kamhi, *Efforts to Protect Consumer Data Face Corporate Pushback*, N.Y. L.J. (Oct. 12, 2017, 2:02 PM), https://www.law.com/newyorklawjournal/almID/12028002

As a result of the growing data protection problem, this Note argues Congress should implement data protection legislation to keep up with the rapidly advancing impact of technology on society and to protect consumers' privacy. First, in Part II, this Note compares the vastly different legal frameworks for data protection between the United States and the European Union ("EU"). Section II.A explores the current U.S. data protection framework, made up of sector-specific federal laws and state data protection laws. Section II.B discusses the development of data protection laws in the EU and contrasts its uniform regulatory framework with the U.S. approach. Finally, Section II.C provides a background on the General Data Protection Regulation ("GDPR"), which is a comprehensive data protection law passed by the European Parliament that will significantly affect how U.S. businesses collect the personal information of EU citizens. The GDPR establishes several rights for EU citizens regarding the right to control the processing of their personal information, such as the right to informed consent and the right to be forgotten.[12] When drafting a federal data protection law, Congress should use provisions of the GDPR as examples of the rights and critical protections that consumers need in order to be effectively protected from future mass data breaches.

After establishing both the U.S. and EU frameworks, this Note argues that the United States should implement its own data protection law to protect consumers and businesses from future data breaches. Part III argues that a federal data protection law is necessary to protect consumers. U.S. citizens are at risk of future mass data breaches, like those at Equifax and Yahoo. Currently, there is no universal, federal law that requires companies to disclose to consumers when their personal information has been compromised or to implement mandatory security measures. Additionally, there is no law limiting companies from selling the personal information of consumers to third parties for marketing purposes. Part IV argues that the appropriate first step is enacting a federal law that requires companies to implement basic protections when processing and storing personal information. This Note argues that Congress should model a federal data protection law after the GDPR and offers several protections that Congress should implement in future legislation: (1) data minimization; (2) notice of data breaches; (3) encryption; and (4) affirmative consent from consumers before collecting data. By implementing these basic requirements, Congress will drastically increase data protection for consumers.

72468/Efforts-to-Protect-Consumer-Data-Face-Corporate-Pushback (explaining the battle between state legislators, who are attempting to enact laws to protect consumer privacy rights, and data-driven companies who oppose such legislation).

12. *See Individual Rights*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights (last visited July 7, 2018).

II. BACKGROUND OF PRIVACY LAWS IN THE UNITED STATES AND EUROPEAN UNION

This Part provides background on the data protection frameworks of both the United States and the EU. The U.S. data protection framework is comprised of several sector-specific laws that regulate the processing of data in several industries, like healthcare, education, and finance.[13] As a result, companies create their own privacy and data processing policies, forcing consumers to self-regulate in order to protect their personal data from breach.[14] In comparison, the EU enacted the GDPR, a universal data protection law with which all member states and companies processing the data of EU citizens must comply.[15] The GDPR imposes strict obligations for companies that process the personal information of EU citizens and drastically increases the control and privacy that individuals have over their data.[16]

Overall, this Part explores the scope of the data protection laws in the United States and EU. Section II.A provides background on the U.S. legal framework for data protection by examining the development of the right to privacy in the United States and by providing examples of various federal sector-specific laws and several state laws that regulate data protection. Section II.B discusses the development of the fundamental right to data protection in the EU and describes the data protections afforded to EU citizens under Directive 95/46/EC. Section II.C examines the purpose, scope, and future effect of the GDPR, which took effect in May 2018.

A. U.S. DATA PROTECTION FRAMEWORK

Unlike the EU, the United States does not have a universal, federal data protection law.[17] Instead, the U.S. legislative framework "resembles a patchwork quilt"[18] of various sector-specific federal laws and hundreds of data protection laws enacted at the state level.[19] This sectoral approach to privacy prohibits specific actions and regulates certain commercial sectors, such as

13. *See infra* text accompanying notes 19–24.

14. *See* Aaron P. Simpson & Jenna N. Rode, *USA*, *in* THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: DATA PROTECTION 2017, 336, 336 (Suzie Levy & Rachel Williams eds., 2017).

15. 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 ("If you are deliberately providing goods or services to people in the EU (even if they only happen to be in the EU for a short period and they live elsewhere) then the GDPR applies.").

16. *See infra* Section II.C.1 (discussing the data protection rights individuals have against companies processing their data such as the right to be forgotten and the right to be informed).

17. Simpson & Rode, *supra* note 14, at 336.

18. Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION & PRIVACY 2015, 208, 208 (Rosemary P. Jay ed., 2015).

19. Simpson & Rode, *supra* note 14, at 336; *Data Protection Laws of the World*, DLA PIPER (last modified Jan. 25, 2017), https://www.dlapiperdataprotection.com/index.html?t=law&c=US.

those involving healthcare,[20] finance,[21] education,[22] national security,[23] and children's privacy.[24] Because there is no universal, federal data protection law, companies are able to develop their own privacy policies and data protection technologies, leaving individuals with the responsibility to protect themselves from having their personal information hacked or stolen.[25] The U.S. approach to data protection is enforced through federal agencies, such as the Federal Trade Commission, state attorneys general, and through individuals bringing suit when data breaches occur.[26] This Part studies the development of the right to privacy under U.S. law and explores various sector-specific federal laws, as well as the state data protection laws with which they overlap.

1. Development of the Right to Privacy Under U.S. Law

Unlike the EU, where there is a recognized fundamental right to privacy, there is no express guarantee of privacy in the U.S. under its Constitution.[27] Despite no explicit protection under U.S. law, the right to privacy has slowly developed over the past 130 years. The theoretical origin of the right to privacy in the United States was expressed in 1890 in an article co-written by Louis Brandeis stating, "[r]ecent inventions . . . call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[28] Seventy-five years later, the U.S.

---

20. *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d (2012) (establishing a framework for protecting an individual's identifiable health information and establishes civil and criminal penalties for violations); *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited June 2, 2018). HIPAA establishes a set of national standards that address the "use and disclosure of individuals' health information." *Id.*

21. Gramm–Leach–Bliley Act, 15 U.S.C. § 6801 (a)–(b) (requiring financial institutions to inform customers of their information-sharing practices and to protect the sensitive information of their customers).

22. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012) (protecting student educational records and allowing parents to examine the academic records of their children under the age of 18).

23. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, §§ 201–25, 115 Stat. 272, 278–96 (2001) (permitting the government to wiretap as long as foreign intelligence is a significant purpose of the investigation, allowing agencies to share acquired information with other federal departments, and giving ability to compel internet service providers to turn over personal email information).

24. *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–05 (2012) (regulating commercial websites that collect the personal information of children under the age of 13 and requiring parental consent before data collection).

25. Simpson & Rode, *supra* note 14, at 336.

26. Alan Charles Raul et al., *United States*, *in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 364, 365–67 (Alan Charles Raul ed., 4th ed. 2017).

27. *See infra* Section II.B.

28. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting COOLEY ON TORTS 29 (2d ed.)).

Supreme Court recognized the right to privacy in "penumbras" within the Bill of Rights.[29] The Court held that the First, Third, Fourth, Fifth, and Ninth Amendments "create a zone of privacy in which government may not force [an individual] to surrender to his [or her] detriment."[30] Additionally, in *Whalen v. Roe*, the Supreme Court held that individuals have a privacy interest in "avoiding disclosure of personal matters."[31] However, this recognized right to privacy only protects individuals from government intrusion into one's private life. Unlike the right to privacy, the right to freedom of speech in the United States is well-defined, highly valued, and often trumps other rights. As a result, when the right to freedom of speech and privacy come into conflict, the expressly protected right to free speech frequently triumphs over the vague right to privacy.[32] In contrast, the EU recognizes the right to privacy as a fundamental right that all individuals, private entities, and governments must uphold.[33] In addition to this limited right to privacy, the United States also has several sector-specific laws that regulate individuals' privacy and data protection.[34]

2. Examples of Sector-Specific Federal Laws

The Federal Trade Commission Act ("FTCA") and the Fair Credit Reporting Act ("FCRA") are two examples of these sector-specific laws that enjoin unfair business practices relating to personal information.[35] Unlike the

29. Griswold v. Connecticut, 381 U.S. 479, 483–84 (1965).

30. *Id.* at 484.

31. Whalen v. Roe, 429 U.S. 589, 599 (1977). The Court also held that individuals had the right to "keep[] personal facts away from the public eye." U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 769 (1989).

32. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1106–10 (2000). For an example of the U.S. upholding the right to free speech over the right to privacy, see Martin v. Hearst Corp., 777 F.3d 546 (2d Cir. 2015). Three newspapers published stories stating that police confiscated drugs from the house of Lorraine Martin. *Id.* at 548–49. After the stories were published, the state did not press charges and the case was dismissed. *Id.* at 549. After the newspapers refused to delete the articles describing her arrest, Martin sued for libel and invasion of privacy. *Id.* However, the Second Circuit dismissed the claim, holding that readers understand that people who are arrested are not always guilty. *Id.* at 553.

33. *See infra* Section II.B.

34. *See, e.g.*, 15 U.S.C. § 6502 (2012) (imposing heightened privacy and parental consent requirements on companies operating websites or services directed to children under 13 years old); *id.* § 6801 (requiring financial institutions to inform customers of their information-sharing practices and to protect the sensitive information of their customers); 18 U.S.C. § 2710(b)(2) (allowing service providers to release the video-tape rental records of a customer only in limited circumstances such as written consent from the customer or a valid search warrant); 47 U.S.C. § 222(c)(1)–(2) (requiring every telecommunication carrier to protect the confidentiality of information of their customers and requiring that carriers "shall only use, disclose, or permit access" to customer information when necessary or by request by the customer).

35. Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012); Fair Credit Reporting Act § 602, 15 U.S.C. § 1681 (requiring consumer reporting agencies to "adopt reasonable procedures

EU, which guarantees the fundamental right to data privacy through extensive laws,[36] the U.S. framework is not preventative or precautionary but instead allows individuals to bring suit to stop "unfair or deceptive acts or practices in or affecting commerce."[37]

Section 5 of the FTCA prohibits "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."[38] The Federal Commission ("FTC") has construed Section 5 to "prohibit certain privacy invasions based on deception."[39] Under Section 5, if a company fails to uphold its privacy policy on its website, the FTC may prosecute the company or individual for unfair and deceptive practices.[40] While this Act does afford consumers some protection for data processing, it does not require companies to give notice, receive consent for data processing, limit their use, securely store the data, or actually post a privacy policy.[41] Additionally, it is severely limited in its application and only enforced when there is a violation of an actual written agreement, such as a privacy policy.[42]

In addition to the FTCA, the FCRA was one of the first federal laws that created a framework of protections of personal information.[43] Congress enacted the FCRA in 1970 to protect against the misuse of an individual's credit information and to require consumer reporting agencies to have accurate information.[44] Under the FCRA, credit agencies may only share an individual's personal information for a valid purpose, such as a landlord

. . . which [are] fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information").

36. *See infra* Section II.B.

37. 15 U.S.C. § 45(a)(1).

38. *Id.* § 45(a)(2).

39. *Federal Trade Commission*, EPIC, https://epic.org/privacy/internet/ftc/Authority.html (last visited June 3, 2018).

40. *Id.* An example of enforcement by the FTC occurred in 2011 when Facebook "agreed to settle Federal Trade Commission charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public." *Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises*, FTC (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

41. *Federal Trade Commission, supra* note 39.

42. *Id.*

43. *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, EPIC, https://epic.org/privacy/fcra (last visited June 3, 2018) (ensuring "rights of data quality (right to access and correct), data security, use limitations, requirements for data destruction, notice, user participation (consent), and accountability").

44. *Id.*; *see also A Summary of Your Rights Under the Fair Credit Reporting Act*, CONSUMER FIN. PROTECTION BUREAU, http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf (last visited June 3, 2018) (protecting the right to be informed when an individual's information has been used to take adverse action against him or her, the right to obtain information a consumer reporting agency has in an individual's file, the right to request a credit score, and the right to report incomplete or false information in a file).

seeking to approve a lease.[45] Agencies are prohibited from sharing credit information with an individual's employer without the individual's written consent.[46]

3. State Data Protection Laws

In addition to many sector-specific federal laws, states also have enacted laws that regulate data processing and the right to privacy. Forty-eight states have enacted data-breach notifications laws, which require companies to notify individuals when their personal information is compromised.[47] Compared to the federal laws, state legislation is the "most aggressive" aspect of data protection in the U.S.; however, state laws still give far less protection to consumers than the EU.[48] California was the first state to enact such data protection legislation in 2002.[49] In 2015, California enacted a statute that requires companies to delete any information that a minor has posted if the minor requests the deletion of such information.[50] Another example of these various state laws is Massachusetts, which requires businesses to "insure the security and confidentiality" of a Massachusetts resident's personal information both in paper and electronic records,[51] regardless of whether the business is located in-state or out-of-state.[52] While these laws are a good first step towards protecting U.S. consumers, they also create an often conflicting patchwork of data protection legislation. These state data protection laws enact different and frequently discordant provisions about what kinds of personal information must be protected, what kinds of companies must

---

45. *Summary of Your Rights Under the Fair Credit Reporting Act*, *supra* note 44.

46. *See* 15 U.S.C. § 1681b(g)(1)(B)(ii) (2012).

47. 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. Alabama and South Dakota are the only U.S. states with no data protection law. *2017 Security Breach Legislation*, NAT'L CONF. ST. LEGISLATURES (Dec. 29, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/2017-security-breach-legislation.aspx.

48. Paul J. Watanabe, Note, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111, 1124 (2017).

49. Lothar Determann, *New California Data Security and Breach Notification Requirements for 2016*, BAKER MCKENZIE (Jan. 14, 2016), http://www.bakerinform.com/home/2016/1/13/new-california-data-security-and-breach-notification-requirements-for-2016; *see also* CAL. CIV. CODE § 1798.82(a) (West 2009) (requiring "any person or business that conducts business in California, and that owns . . . data that includes personal information, [to] disclose any breach of [a] security system . . . to any resident of California whose unencrypted personal information was . . . acquired by an unauthorized person").

50. CAL. BUS. & PROF. CODE § 22581(a)(1) (West 2016).

51. 201 MASS. CODE REGS. § 17.01(1) (2009) ("The objectives of 201 CMR 17.00 are to . . . protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information in a manner that may result in substantial harm or inconvenience to any consumer.").

52. 201 MASS. CODE REGS. § 17.05; Donovan Colbert, *The Future of IT Security Compliance: 201 CMR 17.00*, TECHREPUBLIC (Apr. 29, 2013, 11:00 PM), http://www.techrepublic.com/blog/it-security/the-future-of-it-security-compliance-201-cmr-1700.

comply with the requirements, and what constitutes a breach.[53] Additionally, the requirements for notification also vary state by state. For example, the data breach notification law in New Jersey requires companies to notify the state cybercrime unit,[54] while Maryland's law requires companies to notify the state attorney general before notifying the affected individuals.[55] In addition to these laws and in response to the 2017 Equifax breach, over 30 states have introduced additional security breach notification laws.[56] These state data protection laws are enforced by the state attorneys general and also the FTC.[57] The FTC has brought over 500 claims against companies such as Google, Twitter, and Facebook, enforcing laws that protect consumer privacy information.[58] In 2017, the FTC and 32 state attorneys general brought a suit against Lenovo for giving a third-party access to their customer's sensitive personal data, including Social Security numbers, financial information, medical records, and login credentials, "[w]ithout the consumers' knowledge or consent."[59]

B. EU DATA PROTECTION LAWS

Unlike the U.S. privacy laws, EU privacy laws serve to protect the "fundamental right to the protection of personal data."[60] Article 8 of the Charter of Fundamental Rights of the European Union explicitly protects the fundamental right to data protection.[61] Additionally, the Treaty on the Functioning of the European Union preserves the right to data protection, stating that individuals have "the right to the protection of personal data concerning them."[62]

---

53. *See* Colbert, *supra* note 52.

54. *Cyber Crimes Unit,* N.J. ST. POLICE, http://www.njsp.org/division/investigations/cyber-crimes.shtml (last visited June 3, 2018).

55. MD. CODE ANN. COM. LAW § 14-3504(h) (West 2013).

56. *2017 Security Breach Legislation*, *supra* note 47.

57. Raul et al., *supra* note 26, at 368–69.

58. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017, 2 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

59. *Id.*

60. *EU Data Protection Directive,* EPIC, https://epic.org/privacy/intl/eu_data_protection_directive.html (last visited June 17, 2018).

61. *See* Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10 ("Everyone has the right to the protection of personal data concerning him or her . . . . [D]ata must be processed fairly for specified purposes and on the basis of . . . consent . . . or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.").

62. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, May 9, 2008, 2008 O.J. (C 115) 55. This is one of the main treaties that establishes the functions and organization of the EU. *See Data Protection in the EU*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last visited July 7, 2018).

The development of privacy as a fundamental right began after World War II, in response to the authoritarian governments that used the personal information of European citizens for hateful and catastrophic purposes.[63] Post-war efforts began to prohibit the unchecked collection and use of personal information of individuals.[64] In 1950, Article 8 of the European Convention of Human Rights ("ECHR")[65] was the first step to protect personal information.[66]

In the 1970s, legislators in Europe began to see that Article 8 of the ECHR did not provide adequate protection in light of the growing use of technology and collection of personal data; it was not clear what was meant by "private life" in the document or how it should be applied to private businesses.[67] As a result, the Council of Europe[68] aimed to regulate how companies or other private sector organizations processed the personal data of EU citizens.[69] After four years of negotiations between member states, the Council of Europe ratified the Data Protection Convention.[70]

Despite this new legal framework for data protection, EU member states did not uphold it consistently.[71] Concerned that the inconsistency would hinder the development of business in areas where the processing of personal data was important, the European Commission proposed a new legal framework in order to unify European law on data protection.[72] In October of 1995, the European Parliament and the Council of Europe passed the Data

63. *See, e.g.*, GÖTZ ALY & KARL HEINZ ROTH, THE NAZI CENSUS: IDENTIFICATION AND CONTROL IN THE THIRD REICH 2–3 (Edwin Black & Assenka Oksiloff trans., 2004) (explaining how the Nazi regime used the 1939 census in Germany to collect the personal information of non-Aryans, Romani people, and individuals with hereditary illnesses).

64. HARVEY L. KAPLAN ET AL., SHOOK, HARDY & BACON L.L.P., A PRIMER FOR DATA-PROTECTION PRINCIPLES IN THE EUROPEAN UNION 39 (2009).

65. *See* Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 art. 8, Nov. 4, 1950, E.T.S. No. 5 ("Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except . . . in the interests of national security, public safety or the economic well-being of the country . . . or for the protection of the rights and freedoms of others.").

66. KAPLAN ET AL., *supra* note 64, at 39.

67. PETER HUSTINX, EU DATA PROTECTION LAW: THE REVIEW OF DIRECTIVE 95/46/EC AND THE PROPOSED DATA PROTECTION REGULATION 4 (2014), http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf.

68. The Council of Europe is an international organization of 47 countries that was established to promote human rights and democracy. *Id.*

69. *Id.*

70. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108; HUSTINX, *supra* note 67, at 4; *see also Do Not Get Confused*, COUNCIL OF EUROPE, https://www.coe.int/en/web/about-us/do-not-get-confused (last visited June 18, 2018) (explaining the key differences between the Council of Europe and the EU).

71. HUSTINX, *supra* note 67, at 9.

72. *Id.*

Protection Directive 95/46/EC ("Directive 95/46/EC").[73] It established a framework that guaranteed security for an individual's personal data passing between EU member states and set a standard of security for the storage, transfer, or processing of personal information.[74]

Directive 95/46/EC established several core principles: Companies had to give notice to individuals when their data was collected,[75] and had to tell individuals who was collecting their data;[76] data needed to be stored safely and secured from abuse, theft, or loss;[77] data was not to be disclosed or shared without consent;[78] subjects were allowed access to correct their data;[79] data was only to be used for the originally stated purposes, and companies collecting data were accountable for breaches.[80] Additionally, the Directive required each EU member state to establish a supervisory authority to ensure compliance with the regulations relating to processing personal data.[81] Each authority had the power to investigate, intervene, and engage in legal proceedings.[82] Finally, data transfers to countries outside of the EU were only permitted if the country guaranteed the required level of data protection and security.[83]

Directive 95/46/EC was the main source of data protection for fifteen years until 2009, when the European Commission announced that it would develop a new framework that would guarantee the fundamental right of data protection by addressing the impact of advances in technology and international data transfers.[84] The goal of the EU Commission was to ensure effective enforcement of the data protection rules and to create a "seamless, consistent and effective protection."[85]

---

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

74. *EU Data Protection Directive*, EPIC, https://epic.org/privacy/intl/eu_data_protection_directive.html (last visited May 14, 2018).

75. Council Directive 95/46/EC, art. 18, 1995 O.J. at 43–44.

76. *Id.* arts. 10, 11, at 41–42.

77. *Id.* art. 17, at 43.

78. *Id.* art. 8, at 40.

79. *Id.* art. 12, at 42.

80. *Id.* art. 6, at 40.

81. *Id.* art. 28, at 47–48.

82. *Id.* For more information on the Data Protection Authority for each EU member state, see *Data Protection Authorities*, EUR. COMMISSION, http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm (last visited June 18, 2018).

83. Council Directive 95/46/EC, art. 25, 1995 O.J. at 45.

84. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 3 (Nov. 4, 2010), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0609&from=EN.

85. *Id.* at 4.

The European Commission, the Council of Europe, the EU member states, and the European Parliament negotiated for four years.[86] The new legislation needed to respond to two problems created by the Directive.[87] First, the Directive 95/46/EC did not sufficiently address the technological developments and growth as a result of the Internet.[88] Second, the Directive 95/46/EC created a patchwork of rules enacted by each EU member state that did not adequately protect individuals' privacy.[89] In April 2016, the EU Commission ratified the GDPR, which replaced the existing Directive 95/46/EC when it became effective on May 25, 2018.[90]

C. GENERAL DATA PROTECTION REGULATION ("GDPR")

Like the previous Directive 95/46/EU, the GDPR also recognizes that the protection of personal information is a fundamental right under Article 8(1) of the Charter of Fundamental Rights of the European Union.[91] In light of the rapid development of technology over the past two decades and the immense increase of the collection and storage of data by private companies, the purpose of the regulation is to "facilitate the free flow of personal data within the Union and the transfer to third countries . . . while ensuring a high level of the protection of personal data."[92] Additionally, the GDPR increases the data protection obligations of organizations that process the personal data of EU citizens, strengthens the control and privacy that individuals have over their data, and enhances the enforcement of the Regulation in each member state.[93] Additionally, another goal of the GDPR is to drastically reduce transactional costs for companies by enacting a uniform law, essentially a "one-stop-shop" for data protection for all EU member states and companies processing the data of EU citizens.[94]

---

86. LK Shields, *Background and Introduction to the General Data Protection Regulation*, LEXOLOGY (Sept. 19, 2017), https://www.lexology.com/library/detail.aspx?g=d7f59709-4362-4155-ab6f-de55af4147a4.

87. Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 630 (2013).

88. *Id.*

89. *Id.*

90. Nate Lord, *What is GDPR (General Data Protection Regulation)? Understanding and Complying with GDPR Data Protection Requirements*, DIGITAL GUARDIAN (Jan. 23, 2017), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

91. Council Regulation 2016/679, 2016 O.J. (L 119) 1, 1.

92. *Id.* at 2.

93. Bridget Treacy & Anita Bapat, *All Change for Data Protection: The European Data Protection Regulation*, *in* THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: DATA PROTECTION 2017, 1, 1 (Suzie Levy & Rachel Williams eds., 4th ed. 2017).

94. Griffin Drake, Note, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 182 (2017).

The two main changes in the GDPR are its penalties for non-compliance and the scope of its reach, affecting companies operating outside of the EU.[95] To guarantee compliance, for each serious breach, the GDPR imposes fines of up to €20 million or 4% annual global turnover, whichever penalty is greater.[96] Examples of serious breaches include a company "not having sufficient . . . consent to process data or violating the core of Privacy by Design concepts."[97] A lesser fine of 2% annual global turnover will be issued when companies fail to notify an individual of a data breach or fail to keep their records in order.[98] These penalties apply not only to companies processing the data of EU citizens, but also to cloud service providers that store the personal data of EU citizens on behalf of the company.[99] However, unlike Directive 95/46/EU, which was limited solely to European entities, the GDPR applies to any entity providing goods and services to individuals in the EU, regardless of whether it physically operates within the EU.[100] Thus, many U.S. organizations will be required to comply with the GDPR if they process or store the data of EU citizens.

Another significant change is that the GDPR expands the definitions for personal information,[101] data controllers,[102] and data processors,[103] and enhances the security requirements for companies that store personal information.[104] Finally, the GDPR strengthens the rights of EU citizens by

95. *GDPR Key Changes*, EUGDPR.ORG, http://www.eugdpr.org/the-regulation.html (last visited June 18, 2018).

96. Nuria Pastor & Georgina Lawrence, *Getting to Know the GDPR, Part 10—Enforcement Under the GDPR—What Happens If You Get It Wrong?*, FIELDFISHER (Mar. 5, 2016, 4:45 PM), http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-10-enforcement-under-the-gdpr-what-happens-if-you-get-it-wrong. The supervisory authority from each EU member state has a wide variety of powers to enforce compliance with the GDPR. *Id.* The supervisory authorities have the power to investigate and audit companies processing the data of individuals and inform the companies of breach. *Id.* Additionally, they can issue warnings, bans, and reprimands and can impose fines as long as they are "effective, proportionate and dissuasive." *Id.*

97. *GDPR Key Changes*, *supra* note 95.

98. Pastor & Lawrence, *supra* note 96; *GDPR Key Changes*, *supra* note 95.

99. *GDPR Key Changes*, *supra* note 95.

100. *Who does the GDPR apply to?*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions (last visited June 18, 2018).

101. *GDPR FAQs*, EUGDPR.ORG, http://www.eugdpr.org/gdpr-faqs.html (last visited June 18, 2018) ("[Personally identifiable information is] any information relating to an identifiable person . . . . This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.").

102. *Id.* (defining data controller as an "entity that determines the purposes, conditions and means of the processing of personal data," such as a business collecting the data of customers for marketing purposes).

103. *Id.* (defining data processor as "an entity which processes personal data on behalf of the controller," such as a cloud storage company).

104. *GDPR Key Changes*, *supra* note 95 (explaining the expanded rights of data subjects under the GDPR, including informed consent, breach notification, and privacy by design).

requiring that companies receive informed consent before collecting personal information and guaranteeing several individual rights, such as the right to be informed, the right to be forgotten, and the right to object to the processing of their personal data.[105]

1. Strengthening Privacy Rights of EU Citizens: Affirmative Consent and Guaranteed Rights

The GDPR requires a heightened form of consent from individuals. While Directive 95/46/EC allowed companies to rely on implied consent or to use complicated privacy policies,[106] the GDPR requires that consent is "given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data."[107] While signing a privacy agreement electronically or checking a box is sufficient, silence or pre-checked boxes are not enough to show consent.[108] Additionally, when companies process the data of an individual for multiple purposes or multiple sets of data, the individual must consent each time.[109]

In addition to requiring a heightened form of consent, the GDPR creates new rights for EU citizens and strengthens some rights that existed under the original Directive.[110] Some of the fundamental rights protected under the GDPR include the right to be informed, the right to erasure, and the right to object.[111]

The right to be informed establishes what information the company must give to individuals before processing their data: the identity of who is collecting the data, the purpose of the collection of the data, the identity of any other recipient of the personal data, details of transfers to third countries, the retention period of the data, and the individual's right to withdraw consent at any time.[112] The company must provide this information before an individual gives consent.[113]

---

105. *See infra* Section II.C.1.

106. Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 3—Consent*, IAPP (Jan. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent.

107. Council Regulation 2016/679, 2016 O.J. (L 119) 1, 6.

108. *Id.*

109. *Id.*

110. *See Individual Rights*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights (last visited June 18, 2018).

111. *Id.*

112. *Right to Be Informed*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed (last visited June 18, 2018). For more information on the right to rectification, the right to access, the right to restrict processing, the right to portability, and the rights related to automated decision making and profiling, see *Individual Rights*, *supra* note 110.

113. *Right to Be Informed*, *supra* note 112.

In addition to the right to be informed, one of the most burdensome and broadest rights that companies must comply with under the GDPR is the right to erasure, also known as "the right to be forgotten."[114] Although the right to be forgotten is not absolute, individuals can request to have their data erased in specific circumstances such as when it is not needed for the reason it was originally collected.[115] This right allows a person to request a company to delete or remove their personal information when the company has no business justification to continue using it.[116] For example, companies often collect and store the personal information of employees, such as their name, email, home address, bank information, background check information, phone number, social security number, etc., for legitimate human resources or employment purposes. However, for example, if an employee leaves the company and requests that his or her data be deleted, the company must comply because it has no compelling reason to continue to store the personal information.

Before the GDPR was ratified, the European Court of Justice ("ECJ") had already firmly recognized the right to be forgotten in 2014.[117] In *Google v. Spain,* Mario Costeja González, a Spanish citizen, filed a complaint with the Spanish Data Protection Agency ("AEPD") against Google Spain.[118] Mr. González argued that auction notices from 1998, which contained detrimental information regarding his social security debts, were no longer relevant almost twenty years later.[119] He sought for Google to remove the pages so that the damaging personal information was no longer listed online.[120] After the AEPD ruled against Google, "Google appealed to Spain's high court, which" then referred the case to the ECJ.[121]

The ECJ established the right to be forgotten by holding that European citizens have the right to request that search engines remove their personal information from searches.[122] Under Article 12(b) of the previous Directive 95/46/EU, a company could not store or use any data that was "irrelevant or excessive" or keep personal information "longer than . . . necessary unless [the data is] required to be kept for historical, statistical or scientific

114. *See Right to Erasure*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure (last visited June 18, 2018).

115. *Id.* When a data subject withdraws consent or objects to the processing of their personal data, that person has a "right to have their personal data" deleted. *Id.*

116. *Id.* (explaining that individuals can request to have their data deleted if the "data is no longer necessary for the purpose [it was] originally collected or processed . . . for").

117. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317 (May 13, 2014) ¶¶ 20–21, 99, at 8–9, 20.

118. *See generally id.*

119. *Id.* ¶¶ 14–15, at 6.

120. *The Right to Be Forgotten (Google v. Spain)*, EPIC, https://epic.org/privacy/right-to-be-forgotten (last visited June 18, 2018).

121. *Id.*

122. *Id.*

purposes."[123] As a result of this decision, individuals in the EU have the right to request their data be removed from search engines.[124] The ECJ held that this fundamental right overrides the company's economic interest and general public's interest in accessing that information.[125]

After the ECJ's decision, Google claimed that the data should only be removed in the country where the person requesting its removal resides.[126] However, privacy experts criticized this position, arguing that it made little sense because the privacy problem would still exist elsewhere in other countries' domains.[127] To comply with the "right to be forgotten," Google created an online form[128] that allowed individuals to list their name, the URL they wanted to remove, and an explanation as to why they believed the information listed was "irrelevant, outdated or inappropriate."[129] On the same day the online request form was launched, Google received over 12,000 submissions from EU citizens to remove links from its search engine results,[130] and since 2014 Google has received over 2.3 million requests for deletion.[131] In 2016, the French data protection agency ("CNIL") fined Google €100,000 for not complying with the full scope of the Court's decision.[132] CNIL stated that when an EU citizen requests that Google remove his or her information from the search engine, Google must "de-list '*all extensions of the search engine*

123. *Google Spain SL*, ECLI:EU:C:2014:317, ¶ 92, at 19.

124. *Id.* ¶¶ 21, 99, at 9, 20.

125. *Id.* ¶ 99, at 20.

126. *See* Marc Rotenberg, *The Right to Privacy Is Global*, U.S. NEWS (Dec. 5, 2014, 1:50 PM), https://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-right-to-privacy-is-global.

127. *Id.*

128. Danny Sullivan, *Google's Right to Be Forgotten Form Gets 12,000 Submissions on First Day*, MARKETING LAND (May 30, 2014, 5:19 PM), https://marketingland.com/google-right-to-be-forgotten-first-day-8564.

129. Danny Sullivan, *How Google's New "Right to Be Forgotten" Form Works: An Explainer*, SEARCH ENGINE LAND (May 30, 2014, 2:54 AM), https://searchengineland.com/google-right-to-be-forgotten-form-192837 (explaining the process for applying for removing information from Google search engines); *EU Privacy Removal*, GOOGLE, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf (last visited June 18, 2018).

130. Sullivan, *supra* note 128.

131. THEO BERTRAM ET AL., THREE YEARS OF THE RIGHT TO BE FORGOTTEN 3 (2018), https://elie.net/static/files/three-years-of-the-right-to-be-forgotten/three-years-of-the-right-to-be-forgotten-paper.pdf; *see also* Michee Smith, *Updating Our "Right to Be Forgotten" Transparency Report*, GOOGLE (Feb. 26, 2018), https://www.blog.google/topics/google-europe/updating-our-right-be-forgotten-transparency-report (describing the steps Google has taken to comply with the right to be forgotten).

132. Commission Nationale de l'Informatique et des Libertés [CNIL] [National Commission of Computing & Freedoms] Mar. 10, 2016, 2016-054, at 9 (unofficial translation); *see also* Carol Umhoefer & Caroline Chancé, *French Data Protection Authority Orders Fine of 100,000 Euros Against Google Inc. for Violation of Right to Be Forgotten*, BLOOMBERG BNA (May 25, 2016), https://www.bna.com/french-data-protection-n57982072949 (explaining the reasoning of the court when it fined Google €100,000).

domain name.'"[133] As a result, when someone requests for a link to be deleted, Google now blocks access to links "from all of its domains" worldwide, "including the main United States one, Google.com" not just the domain of the country where the European citizen resides.[134] Because the right to be forgotten is a fundamental human right for all EU citizens, any business, whether located inside or outside of the EU, that processes the personal information of EU citizens is therefore required to have the technological capability to comply with this right and an individual's request of erasure.

Another fundamental right recognized under the GDPR is an individual's "right to object to the processing of their personal data," which may result in the processor having to erase all data relating to the individual.[135] For example, a company may use a person's name and email address to send marketing information or advertisements; however, as soon as the company receives an objection from the person for unnecessarily storing and using his or her personal information, the company must delete the information.[136]

2. Requirements for Data Processors and Controllers

The GDPR imposes several legal requirements upon data processors and controllers. Data processors and controllers are required to be transparent in the collection and processing of data, to hold data only for the minimum amount of time necessary, to implement up-to-date security measures such as the encryption of data, and to report breaches.[137]

When collecting and using information, companies must be transparent, stating how the data will be "collected, used, consulted or otherwise processed."[138] Companies must have privacy policies with clear language, stating their purpose for collecting the personal information, how it will be used, who it will be shared with, and where it will be stored.[139] This ensures

---

133. Commission Nationale de l'Informatique et des Libertés [CNIL] [National Commission of Computing & Freedoms] Mar. 10, 2016, 2016-054, at 8 (unofficial translation); *see also* Umhoefer & Chancé, *supra* note 132 (explaining that Google must delete all of its "[s]earch extensions globally, and unconditionally" not just from the country where the citizen resides).

134. Mark Scott, *Google Will Further Block Some European Search Results*, N.Y. TIMES (Feb. 11, 2016), https://www.nytimes.com/2016/02/12/technology/google-will-further-block-some-european-search-results.html.

135. *Right to Object*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object (last visited June 23, 2018).

136. *See id.* ("The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances . . . . Individuals have an absolute right to stop their data being used for direct marketing.").

137. Council Regulation 2016/679, 2016 O.J. (L 119) 1, 7, 14, 16.

138. *Id.* at 7.

139. *GDPR Privacy Policy*, TERMSFEED, https://termsfeed.com/blog/gdpr-privacy-policy (last visited June 30, 2018) (explaining what information companies should include in their privacy policies).

fair processing of the data of EU citizens and ensures their right to informed consent to how their data will be stored and processed.[140]

Another critical principal under the GDPR is data minimization, which requires companies to hold only personal data that is necessary for their business purposes[141] and limit the time period "to a strict minimum."[142] To ensure data minimization, the GDPR requires companies to establish time limits for erasure of data or periodically review the data they hold.[143]

Article 32 requires companies to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including . . . the pseudonymisation and encryption of personal data."[144] Pseudonymization is a security measure which protects the identity of the data subject by substituting "identifiable data with a reversible, consistent value" which is required to re-identify the data subject.[145] This security measure can reduce the risks of data breaches and help companies meet the required level of protection for personal data.[146]

The final critical requirement established by the GDPR is breach notification, which applies to all companies controlling or processing the data of EU citizens.[147] Under the GDPR, when a data breach occurs, an organization must notify the data protection authority immediately, and "not later than 72 hours after having become aware of [the breach]."[148] The GDPR created an exception to the notification requirement: Companies are exempt from reporting a breach when it "is unlikely to result in a risk to the rights and freedoms of natural persons."[149] This exemption incentivizes companies to encrypt the data they store or use pseudonymization to protect the identity and personal data of individuals after a breach because there will be very little risk that their identities will be compromised. However, when a breach does involve a high risk to the rights and freedoms of an individual, such as the leak of someone's medical information or social security number, the company must disclose the breach to the supervisory authority and to the compromised individual without delay.[150] Examples of high-risk breaches include breaches that result in "discrimination, identity theft or fraud,

140. Council Regulation 2016/679, 2016 O.J. at 6.

141. *Id.* at 29.

142. *Id.* at 7.

143. *Id.*

144. *Id.* art. 32, at 51.

145. Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help with GDPR*, PROTEGRITY BLOG (Jan. 5, 2017), http://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr.

146. Council Regulation 2016/679, 2016 O.J. at 5.

147. *Id.* art. 33, at 52.

148. *Id.*

149. *Id.*

150. *Id.*

financial loss, unauthorized reversal of pseudonymisation, damage to reputation, and loss of confidentiality . . . . [or] any other significant economic or social disadvantage."[151]

III. ADDITIONAL PRIVACY REGULATIONS WOULD PROTECT CONSUMERS FROM FUTURE DATA BREACHES

Congress should adopt a federal data protection law requiring a minimum standard of data protection to protect consumers against the rapid advances in technology and the effects of future mass data breaches, like the 2017 Equifax breach. Originally, the U.S. privacy framework was generally *laissez faire*, allowing companies to make their own privacy policies and allowing consumers to self-regulate the information they provided or choose the businesses that protected their data.[152] However, with globalization and digitalization driving U.S. companies forward, the amount of personal data consumers share with businesses has increased exponentially. Today, data brokers are able to collect all types of personal information, such as one's home address, name, annual income, internet history, and social media connections and accounts; they even collect information shared on social media platforms or websites and items looked at while online shopping.[153] Once data is collected, data brokers sell consumers' personal information to companies to use in targeted marketing to consumers[154] or to collect analytic data of demographics and personal preferences.[155] Because the United States has no online privacy laws, data brokers are free to use the personal information they collect for whatever purpose they choose.[156] Over the past decade, companies have begun to collect and transfer the personal data of individuals in vast amounts, and identity theft and data breaches have become the norm.[157] As a result of the 2017 Equifax hacks, arguably the worst data

151. ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON PERSONAL DATA BREACH NOTIFICATION UNDER REGULATION 2016/679, 9 (2017), http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827.

152. *See supra* Section II.A (noting the exception of sector-specific laws that protected certain kinds of information like sensitive health information, financial information, etc.).

153. Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016, 4:51 PM), http://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it.

154. *Id.*

155. Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012, 3:52 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html.

156. *Id.*

157. *Data Breaches 2017*, ITRC, https://www.idtheftcenter.org/2017-data-breaches (last visited June 23, 2018). There were 1,579 U.S. data breaches in 2017, which is a 44.7% increase from 2016. *Id.* Eight-hundred thirty data breaches involved Social Security numbers and resulted in 158 million Social Security numbers being exposed and stolen. *Id.* In late March 2018, over 150 million Under Armour "MyFitnessPal" accounts were breached, giving criminal hackers access to usernames, health data, hashed passwords, and email addresses. Turner, *supra* note 1. For a full

breach in U.S. history, a growing number of consumers, companies, politicians, and privacy experts are calling for stronger data protection laws.[158]

Equifax, a consumer credit reporting agency that collects the personal information of over 800 million individuals worldwide, discovered a massive data breach of the personal data of 147 million customers on July 29, 2017.[159] The company spent six weeks assessing what data had been compromised and patching its software before it alerted the affected customers or its shareholders of the hack.[160] The Equifax hack was particularly damaging because the breached data was the kind of personal information that companies use to verify consumers' sensitive financial and personal information.[161] This data included names, social security numbers, birthdates, home addresses, and even driver's license numbers, exposing over 147 million U.S. citizens to countless crimes, such as bank account theft, fraud, identity theft, and even crimes committed by using a victim's stolen identity.[162] In early 2018, Under Armour's "MyFitnessPal" application suffered a data breach of over 150 million users in 2018, exposing users' email addresses, hashed passwords, and usernames.[163] Another massive U.S. data breach was disclosed in 2016 when Yahoo discovered that in 2013, data from over one

report on the 2017 Data breaches see *2017 Breach List*, ITRC, https://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachReport2017i.pdf (last visited June 23, 2018).

158. *See* Joanne Dynak et al., *Two Data Breach Bills Introduced in US Senate*, MINTZ LEVIN (Dec. 11, 2017), https://www.privacyandsecuritymatters.com/2017/12/senators-re-introduce-bill-requiring-30-day-notification-of-company-data-breaches; Gloria Gonzalez, *Congress Urged to Adopt National Data Breach Standard*, BUS. INS. (Feb. 14, 2018, 2:07 PM), https://www.businessinsurance.com/article/20180214/NEWS06/912319215/Congress-urged-to-adopt-national-data-breach-standard (calling for data protection reform to protect consumers from ongoing data breaches and changes in technology); O'Connor, *supra* note 47.

159. Jackie Wattles & Selena Larson, *How the Equifax Data Breach Happened: What We Know Now*, CNN TECH (Sept. 16, 2017, 4:06 PM), http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html; *see also* Kennedy, *supra* note 9 (discussing an additional 2.4 million individuals who were impacted by the Equifax breach); Patrick Rucker & Angela Moon, *Equifax Avoids Fines in Deal with U.S. States Over Data Breach*, REUTERS (June 27, 2018, 3:06 PM), https://www.reuters.com/article/us-equifax-states-agreement/equifax-agrees-to-toughen-cyber-defenses-in-agreement-with-states-idUSKBN1JN2YH?il=0 (discussing the wide scope of data Equifax collects).

160. Hayley Tsukayama, *Why It Can Take So Long for Companies to Reveal Their Data Breaches*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches ("Equifax waited six weeks to disclose that sensitive information, such as Social Security numbers, birth dates and home addresses, of up to 143 million Americans were swept up in a data breach.").

161. *See id.*

162. *Id.*; Adam Levin, *Equifax Breach Shows the Need for Radical Overhaul in Privacy Laws*, HILL (Oct. 12, 2017, 11:20 AM), http://thehill.com/opinion/cybersecurity/355110-equifax-breach-shows-the-need-for-radical-overhaul-in-privacy-laws; *see also* Kennedy, *supra* note 9 (stating that an additional 2.4 million people were impacted by the Equifax breach).

163. Chloe Aiello, *Under Armour Says Data Breach Affected About 150 Million MyFitnessPal Accounts*, CNBC (Mar. 29, 2018, 4:38 PM), https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html.

billion accounts were breached.[164] In addition to these massive breaches, in 2016, hackers stole the personal information of over 57 million Uber users.[165] Instead of alerting Uber users of the breach, the company spent over $100,000 to cover it up.[166]

As a result of these massive breaches of personal information and the lack of timely notification to the affected victims, consumers have begun to ask why companies do not report breaches sooner.[167] Despite calls for prompt disclosure, there is no federal law mandating companies to report data breaches and each state has its own laws for how breaches are reported.[168] In absence of a federal law, the Federal Trade Commission can bring sanctions against companies that suffered data breaches for violating section 5 of the FTCA, which prohibits unfair business practices.[169] However, the FTC minimizes sanctions if the company cooperates with the investigation and has attempted to reduce the harm resulting from the breach.[170]

As a result of the limited protection of the FTC under section 5 of the FTCA, consumers are vulnerable and unable to protect themselves against identity theft. The problems arising from the United States' patchwork of data protection laws and the rise of data breaches also threaten the personal data of consumers. The U.S. framework for data protection laws is a patchwork of federal sector-by-sector legislation and individual state laws.[171] The federal sector-by-sector approach means that the financial, medical, and educational sectors all require different disclosures and set different breach reporting requirements.[172] This patchwork of legislation makes it difficult for companies with services that operate primarily through the internet or in multiple states and multiple sectors to determine their obligations to customers, especially customers located in multiple states other than the

164. Hayley Tsukayama, *It Took Three Years for Yahoo to Tell Us About Its Latest Breach. Why Does It Take So Long?*, WASH. POST (Dec. 19, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/12/16/it-took-three-years-for-yahoo-to-tell-us-about-its-latest-breach-why-does-it-take-so-long.

165. Selena Larson, *The Hacks that Left Us Exposed in 2017*, CNN TECH (Dec. 20, 2017, 9:11 AM), http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

166. *Id.*

167. Tsukayama, *supra* note 164.

168. *Id.*

169. *See supra* Section II.A (explaining the FTCA and the enforcement of unfair and deceptive business practices); *Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited June 23, 2018).

170. Ellen Nakashima, *Hacked U.S. Companies Have More Options, Departing Cybersecurity Official Says*, WASH. POST (Mar. 2, 2016), https://www.washingtonpost.com/world/national-security/hacked-us-companies-have-more-options-departing-cybersecurity-official-says/2016/03/02/f7cc2e20-d508-11e5-9823-02b905009f99_story.html.

171. Sotto & Simpson, *supra* note 18.

172. *See* Tsukayama, *supra* note 164.

company's headquarters.[173] Additionally, the Equifax, Yahoo, and Under Armour breaches serve "as a warning for what may lie ahead. Hacks will only grow more sophisticated and prevalent."[174]

Although higher security measures are needed in light of the rise in mass data breaches, companies are not incentivized to invest in higher security measures. In 2016, Equifax spent $1.1 million lobbying against data protection regulations, including the basic protections of data breach notification.[175] Without required data protection standards, consumers have few protections to safeguard their personal information from a data breach and few remedies after a data breach occurs.[176] Companies profiting from consumers' personal data must be held accountable for protecting it. However, this will not happen unless there are strictly enforced federal laws and penalties.[177]

To ensure companies implement sufficient security measures to protect consumers from future data breaches, Congress should pass a federal law that would regulate the way companies collect and store mass amounts of personal data[178] and implement mandatory security measures.[179] The proposed legislation should ensure that companies only collect the minimum amount of personal data necessary for legitimate purposes, require companies to give notice of data breaches, and require informed consent from consumers before collecting data.[180]

IV. RECOMMENDED LEGISLATION: HEIGHTENED REQUIREMENTS FOR DATA PROTECTION

In light of the growing number of mass data breaches, U.S. consumers are in need of a comprehensive data protection reform to protect themselves. When drafting a federal data protection law, Congress should look to other countries, such as the member states of the EU, which uphold data protection and an individual's right to privacy as fundamental rights that must be

173. *See id.*

174. Karen Turner, *The Equifax Hacks Are a Case Study in Why We Need Better Data Breach Laws*, VOX (Sept. 14, 2017, 10:17 AM), https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security.

175. *Id.*; Stacy Cowley et al., *Equifax Breach Prompts Scrutiny, but New Rules May Not Follow*, N.Y. TIMES (Sept. 15, 2017), https://www.nytimes.com/2017/09/15/business/equifax-data-breach-regulation.html.

176. *Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL ST. J. (Mar. 10, 2013, 4:00 PM), https://www.wsj.com/articles/SB10001424127887324338604578328393797127094.

177. Greg Mooney, *Equifax Data Breach—Does the US Need Its Own GDPR?*, IPSWITCH (Sept. 8, 2017), https://blog.ipswitch.com/equifax-data-breach-does-the-us-need-its-own-gdpr.

178. *See, e.g.*, Turner, *supra* note 174 (arguing that "[t]he only good way for these [breaches] to be stopped is for the giant organizations holding this information to be better regulated").

179. Tsukayama, *supra* note 164 ("The law should require, not just encourage, reasonable data security practices from companies that collect, process, and share personal information . . . .").

180. *See* Turner, *supra* note 174.

protected. Specifically, the GDPR requires informed, affirmative consent from consumers before companies can collect any information, and it requires that companies only collect the minimal amount of information necessary for their legitimate business purposes.[181] Additionally, the GDPR incentivizes companies to encrypt individuals' personal information and requires companies to inform consumers of data breaches within a short period of time after the breach occurs.[182] If Congress enacted similar basic protections afforded under the GDPR, consumers would be more protected against mass data breaches like Equifax in 2017. Not only would companies be forced to encrypt sensitive personal information like Social Security numbers and health information, but they would also only be allowed to store data if consumers affirmatively consented to the collection and only to the extent necessary for a legitimate business purpose. Additionally, unlike Equifax, which waited several months before disclosing the breach to the affected consumers, a federal data protection law that mirrors aspects of the GDPR would require companies to notify consumers within days after a data breach. This Note argues that there are several protections Congress should implement in a federal data protection law, including data minimization, data breach notice requirements, the encryption of data, and affirmative consent from consumers. This Part explores each one of these protections in turn.

A. DATA MINIMIZATION

The first feature that Congress should enact in a federal data protection law is a data minimization requirement. A data minimization policy would force companies to collect and store only the necessary amount of personal data to fulfill their legitimate business purposes and would require companies to delete such information after a maximum of three years.[183] As technology advances, companies will continue to collect mass amounts of data, including private data such as one's home address, cell-phone number, date of birth, and other personally identifiable information.[184] An FTC staff report warned that not only does storing mass amounts of data create a bigger target for data hackers, but it also increases the harm to consumers if a data breach does occur.[185]

Additionally, when a company collects and stores mass amounts of personal information, there is a higher chance "that the data will be used in

181. Council Regulation 2016/679, 2016 O.J. (L 119) 1, 6.

182. *Id.* at 7.

183. *See* Bernard Marr, *Why Data Minimization Is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data.

184. *See id.*

185. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, iv (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

a way that departs from consumers' reasonable expectations."[186] The GDPR requires companies to hold the minimum amount of data necessary for their business purpose,[187] and other countries outside of the EU have begun to follow this approach. In South Korea, mass data breaches occurring from 2004 to 2014 resulted in the theft of 80% of the country's national identification numbers.[188] The country was forced to replace its entire national identification system, which cost billions of dollars.[189] As a result, South Korea passed a law which requires companies processing the personal identification number of a citizen to delete it within two years.[190]

South Korea is an excellent example of a data minimization policy in practice. Congress should pass a law restricting companies to only collect personal information that is absolutely necessary to fulfill a legitimate business purpose and requiring companies to delete the information after three years. In other words, if a business does not require a consumer's social security number to provide a service, it should not request the social security number or other highly sensitive personal information online. If a company does require personal information for a legitimate business purpose, the company should only retain the information for the maximum amount of years allowed under the data protection law. For example, when updating its online privacy policy, an online clothes retailer should ask itself a few questions, like: Is collecting this data necessary for business purposes? Would collecting less of the information accomplish the same result? Companies should also determine how long data actually needs to be stored. Storing a customer's data that was collected from an online purchase five years ago, like their name, mailing address, billing address, email, birthday, phone number, etc., would not comply with the federal law requiring that data be only held for a maximum of three years. While changing the ways that companies collect information is a daunting task, the potential threat of future mass data breaches against American consumers outweigh these costs.[191] Identity theft cost U.S. citizens over $16 billion in 2016.[192] By limiting the amount and time that the personal information of consumers is stored, companies protect themselves and consumers from future data breaches and identity theft.

---

186. *Id.*

187. Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1, 35.

188. Mark Buell, *Post Equifax, We Need to Reconsider How to Identify People*, INTERNET SOC'Y (Sept. 26, 2017), https://www.internetsociety.org/blog/2017/09/post-equifax-need-reconsider-identify-people.

189. *Id.*

190. *Id.*; *see also* John Leitner, *Data Privacy in South Korea: Can Legislation Transform Protection of Personal Information?*, DIGITAL ASIA (Oct. 21, 2016), https://www.digitalasiahub.org/2016/10/21/data-privacy-in-south-korea-can-legislation-transform-protection-of-personal-information (describing the strict regulation of the processing of South Korean Resident Registration Numbers and requirement of data minimization for all companies processing this data).

191. Buell, *supra* note 188.

192. *Id.*

B. *DATA BREACH NOTICE REQUIREMENTS*

Congress should also require companies to notify consumers within a set amount of time when their personal information has been breached. For companies like Equifax and Yahoo, it took months or even years to report a data breach, likely in part because there is no universal, federal law requiring disclosure.[193] Additionally, companies do not want to damage their reputation or trust with customers by disclosing a mass data breach. As a result, consumers lose precious time they could have used to protect themselves from identity theft by changing their financial information or closing their bank accounts.

In a data protection law, Congress should include uniform data breach requirements in order to ensure that consumers are informed when their data is compromised and that companies follow the same standards, regardless of the state or industry. The federal data protection law should define the kinds of personal information required to trigger data breach notification, the definition of a data breach, the timing of the notification, the methods required to notify affected consumers, the penalties for non-compliance, and the possible exemptions to these provisions, such as using encrypted data. A breach notification requirement should give companies a set amount of time, such as two weeks, to discover the scope of the breach and the number of affected parties before disclosing, instead of allowing months to pass before notifying victims of the attack.[194] Not only would this law force companies to implement more data security and to protect their data, but it would also protect consumers from future identity theft and other harm resulting from disclosure of sensitive personal information.

C. *ENCRYPTION*

Congress should require a form of encryption as a safeguard against threats to sensitive personal information, such as health information, social security numbers, and bank account numbers. By requiring a form of encryption for sensitive types of personal data, companies ensure that even if a data breach occurs, the risk of personal harm or identity theft to consumers is eliminated because the personal data cannot be accessed without an encryption key.

The traditional form of encryption is very impractical and inefficient in the modern way companies do business. The traditional form of "wholesale

193. *See supra* note 17 and accompanying text.

194. For an example of a data breach notification requirement, Article 33 of the GDPR requires an organization "without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority." Council Regulation 2016/679, art. 33, 2016 O.J. (L 119) 1, 52. The GDPR also provides that if a company cannot provide notice within 72 hours, to give reasons for the delay and to provide the information as soon as possible. *See id.*

encryption" of personal information makes it practically impossible for employees to do work.[195] Because employees share and work on multiple files and sets of data at the same time, adding a password encryption to every single file is inefficient in the workplace and is extremely challenging to organize and manage.[196] However, pseudonymization is an advanced form of encryption that protects the data without the complex process of requiring passwords and encryption keys to access the data. Pseudonymization is a technique that essentially "replace[s] personal identifiers with a random code," instead of encrypting the entire file.[197] It is the same technique authors use when "using pseudonyms to hide their identities."[198] When a company first collects personal data, it needs a system that processes the personal information and converts it into special codes.[199]

Then, the company would have a "master table" stored in an inaccessible location that could turn the codes back into the actual personal information when the original information is needed.[200] As a result, employees of a company could work on pseudonymized files that protect the identity of the individuals, while allowing the rest of the file to be readable.[201] Pseudonymization substantially diminishes the risks of processing personal information, while also preserving the utility of the personal information and providing easier access to files than wholesale password encryption.[202]

Congress should look towards the GDPR and its use of encryption when drafting security requirements for data protection legislation. Although the GDPR does not require encryption, it incentivizes companies to implement it. Under the GDPR, when a company encrypts or pseudonymizes its data,[203] the companies are not required to disclose data breaches to the affected individuals because the breached information is rendered anonymous with no connection to individuals.[204] By pseudonymizing data, the risk of identity theft or financial harm for individuals is mitigated because the sensitive information is encrypted, with the key stored in a separate non-accessible

195. Andy Green, *GDPR: Pseudonymization as an Alternative to Encryption*, VARONIS (Mar. 22, 2018), https://blog.varonis.com/eu-gdpr-spotlight-pseudonymization-as-an-alternative-to-encryption.

196. *See id.*

197. *Id.*

198. *Id.*

199. *Id.*

200. *Id.*

201. *Id.*

202. Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 8- Pseudonymization*, IAPP (Feb. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization.

203. Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 33 ("'[P]seudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately . . . .").

204. *Id.* art. 34, at 52–53.

place—meaning it cannot be accessed by hackers.[205] Overall, the GDPR provides exceptions to the most burdensome parts of the regulation when companies take steps to "de-identify" personal information.[206] By making it impossible to connect the identity of an individual with the encrypted personal data, companies are allowed to use EU citizens' personal information in any way and for any reason, since there is no risk of harming an individual with that information.[207]

Like the GDPR, the data protection legislation should incentivize companies to pseudonymize consumers' personal data. Congress could make exceptions for these companies that encrypt their data using pseudonymization; the exceptions could allow companies to not comply with the data breach notice or data minimization requirements because the data would be rendered anonymous and the threat of harm resulting from breaches would be reduced. Additionally, because the threat of data breach for smaller companies or for individuals storing personal information physically is smaller, Congress could provide an exception to the requirement of pseudonymization for companies only processing the data of less than 200 people or individuals who only store hard copies of information securely. By requiring a form of encryption, Congress will protect consumers and companies from the harm caused by future mass data breaches.

D. AFFIRMATIVE CONSENT

This Note's final recommendation is that Congress should require that consumers give affirmative consent *before* companies can collect, store, or share their personal information. Under the GDPR, consent must "be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication" on the consumers' agreement to processing their personal information.[208] The GDPR also states that companies should receive in writing a "declaration of consent . . . in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms."[209] Additionally, the GDPR requires that the consumer must "be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."[210] Similar to the informed consent provisions of the GDPR, Congress should enact a federal law that requires companies that collect the personal information of consumers to receive informed, affirmative consent from consumers *before* collecting their data.

205. *Id.*

206. Matt Wes, *Looking to Comply with GDPR? Here's a Primer on Anonymization and Pseudonymization*, IAPP (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization.

207. *Id.*

208. Council Regulation 2016/679, 2016 O.J. at 6.

209. *Id.* at 8.

210. *Id.*

Also, the federal law should require that all companies and online organizations create a privacy policy and require that the privacy policy be easily accessible, use clear language, and be simple enough for consumers to understand what they are consenting to, rather than using "fine print" terms and conditions. Additionally, the law should require that the privacy policy states what information will be stored, for how long it will be stored, for what purpose it will be stored, etc.

Currently, while there are many sector-specific federal laws, none of them require companies to have a privacy policy. However, the FTC issued guidelines for companies to follow when writing a privacy policy.[211] The guidelines suggest that a company's privacy policy should be written in "easy-to-understand English and not 'legalese.'"[212] Additionally, it should state what data is being collected, how the data is being used, how the company protects the data, whether consumers have control over their information, and if a company shares the collected data, who is the third party receiving the personal information.[213] Making these guidelines mandatory for all companies collecting data would protect consumers by disclosing how their personal information would be used, before companies collect it in the first place.

V. CONCLUSION

As mass data breaches like Equifax and Yahoo become more and more common in today's world of globalization and digitalization, it is apparent that consumers can no longer protect themselves through self-regulation alone. Although the EU recognizes data protection as a fundamental right and has enacted the GDPR to guarantee data protection to all EU citizens, the United States has no universal, federal law regulating data protection. Instead, each state and various federal sectors, such as healthcare, finance, and education, have enacted their own data protection laws. This has resulted in a complex, yet ineffective patchwork of privacy legislation. This piecemeal approach to data protection is inadequate to protect consumers as technology progresses and the amount of personal information collected by companies grows. Congress must address these growing risks to consumer protection by adopting a federal data protection law that implements a risk management approach, forcing companies to strengthen their security measures through encryption, data minimization, and putting consumers back in control of their personal information.

211. *Privacy Policies Are Mandatory by Law*, TERMSFEED, https://termsfeed.com/blog/privacy-policy-mandatory-law/#In_United_States (last visited June 23, 2018).

212. *Id.*

213. *Id.*