VIII. Data Protection Law: The GDPR, CCPA, and U.S. Federal Regulation

A. Introduction

This article will outline current global developments in data protection law by analyzing the United States' current data privacy law framework as well as new regulations such as the European Union's General Data Privacy Regime (GDPR),[1] and the California Consumer Privacy Act (CCPA).[2]

Data protection encompasses both "data privacy"—how the collection and use of data is controlled—and "data security"—how personal information is safeguarded from theft.[3] Both the GDPR and the CCPA fuse these two concepts under a single umbrella of legislation by: (1) granting individuals statutory rights as to their personal information, and (2) imposing obligations on private parties which process personal information.[4]

This article analyzes how these regulations impact the U.S. financial and banking industries, as well as private corporations. Part B considers the risks and costs of data breaches. Part C explains the background, function, and requirements of the GDPR. Part D examines the current state of U.S. data protection law, and Part E considers California's new data protection regime. Part F analyzes potential avenues for future federal regulation, and Part G provides examples of how U.S. companies can, and should, respond to this type of legislation.

---

[1] Regulation (EU) 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).

[2] California Consumer Privacy Act of 2018, A.B. 375, Ch. 55, § 3 (2018), eff. Jan. 1, 2019.

[3] STEPHEN MULLIGAN ET AL., DATA PROTECTION LAW: AN OVERVIEW, CONGRESSIONAL RESEARCH SERVICE 54 (March 25, 2019) (comparing data protection and data security and detailing how various state laws may focus on one or the other).

[4] *Id.* ("Recent data protection laws such as the CCPA and GDPR appear to indicate a trend toward combining data privacy and security into unified legislative initiatives.").

B. Data Breaches

A tipping-point for the push for stricter data privacy standards in the United States was the 2018 Cambridge Analytica scandal, which saw eighty-seven million Facebook users' data improperly harvested during the 2016 presidential campaign.[5] Specifically, "Facebook gave researchers affiliated with British political consulting firm Cambridge Analytica access to information on millions of its users without the users' consent, which Cambridge Analytica then used to attempt to persuade users to vote for its clients."[6] Facebook covered up the breach instead of reporting it, yet there was no clear, automatic penalty from any U.S. federal regulator for this deception.[7] Conversely, even under its pre-GDPR framework, the United Kingdom imposed the maximum fine of £500,000 against Facebook for this breach.[8] However, with the GDPR in place, some believe Facebook could be liable for billions of dollars over the 2018 breach of 50 million users' data.[9] In practice, GDPR penalties have already been imposed for a range of smaller breaches, from a €4,800 fine to a small business in Austria for improper CCTV cameras to €300,000 in fines to a hospital in Portugal for its violation of data integrity and confidentiality principles.[10]

Companies may be advised to invest more heavily in data security regimes even if regulations like the GDPR and CCPA do not

---

[5] Melissa Quinn, *California data-privacy law may become the model for Congress*, WASH. EXAMINER (July 22, 2019, 12:01 AM) https://www.washingtonexaminer.com/news/california-data-privacy-law-may-become-the-model-for-congress [https://perma.cc/RE58-FY9R] (reporting that there is increasing support for regulation of the collection and use of consumer data).

[6] Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 76 (2019) [hereinafter *Confiding in Con Men*].

[7] *Id.* ("This is an enormous abuse of its users' trust, and yet the question of whether the company would be punished by the FTC was initially somehow still uncertain, despite the fact that the company was *already under a consent decree with the FTC for sharing user information with third parties without their consent*.").

[8] Margaret Reetz, *GDPR: Does Coverage Exist for Fines and Penalties for Noncompliance?*, 21 TORTSOURCE 8, 9 (2019) (detailing fines already levied under the GDPR for various types and levels of severity of breaches).

[9] *Id.* (stating that while Facebook was fined by EU privacy regulators in 2018, new GDPR fines could be in the billions due to the September 2018 data breach).

[10] *Id.* (providing examples of the fines already imposed under the GDPR).

yet apply to them. Businesses today are increasingly vulnerable to costly data breaches as data collection and processing becomes more central to corporate operations.[11] Regulatory fines are far from the only cost of a major security breach. For example, in 2017, Target settled with forty-seven states for $18.5 million dollars over a cyberattack that mined the credit card information of forty million customers.[12] However, Target estimated the total cost of that breach to be more than $200 million due to "a separate multimillion-dollar settlement in a class action brought by the merchant banks covering the alleged fraudulent activity on the credit card accounts; notification and credit monitoring costs; and the implementation of a comprehensive information security program."[13] Moreover, the 2017 Equifax breach forced the corporation's chief executive officer, chief information officer, and chief security officer to resign after the exposure of consumer information led to heavy criticism of management.[14] Even smaller-scale breaches can be costly and harmful, as a 2016 report estimated that data breaches of companies with less than 100,000 consumer records still resulted in an average cost of $7 million per breach.[15]

Banks and financial institutions are repositories of valuable personal information and thus are particularly vulnerable to data breaches.[16] These organizations must contend with, on average, eighty-

---

[11] Almudena Arcelus, Brian Ellman & Randal S. Milch, *How Much Is Data Security Worth*, 15 SCITECH LAW. 10, 11 (2019) ("In this era of big data and interconnectivity, critical information assets often are at the core of evolving business models, and the value of data is increasing daily. By the same token, data are making organizations more vulnerable. Those information assets, especially personal and financial customer data, expose their stewards to greater risk. . . .").

[12] *Id.* ("Four years [before the 2017 settlement], cyber attackers used stolen credentials and malware to access Target's customer service database.").

[13] *Id.*

[14] *Id.* ("Equifax's revelation that it had suffered a massive data breach of credit information led to widespread examination both of its response and its management.")

[15] *Id.* (citing Ponemon Institute, 2017 Cost of Data Breach Study: United States, June 2017).

[16] Zachary N. Layne, *The Modern Threat: Data Breaches, Security Measures, and a Call for Changes*, 23 N.C. BANKING INST. 159, 159 (2019) ("Of the 1,244 data breaches [in 2018], 135 (10.9%) fall into the banking/credit/financial category.").

five breach attempts per year.[17] The main problems with the current regulatory landscape are: (1) too many distinct regulatory agencies, and (2) a tension between federal and state laws.[18] Therefore, federal, comprehensive data privacy regulation implementing national, uniform standards across industries and institutions could reduce breaches by instituting a baseline defense, thereby stopping hackers from targeting companies with lax protections.[19]

C. Defining the GDPR

The European Parliament approved the GDPR on April 27, 2016 and the legislation went into effect on May 25, 2018.[20] Both before and since its enactment, the GDPR has impacted how corporations structure their data collection systems as companies both in and outside of Europe continuously work to understand and comply with the regulation.[21]

---

[17] *Id.* at 162 (adding that the cost of these breaches outstrips the average due to lost business as customers flee to institutions they feel will better safeguard their money) (citing Rocco Grillo, *Regulatory Compliance Does Not Equal Cybersecurity,* CLEARING HOUSE, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/regulatory-compliance-does-not-equal-cybersecurity (last visited Jan. 17, 2019)).

[18] *Id.* at 174 (listing some of the federal agencies empowered to make and enforce rules related to data security and explaining that in addition to these federal regulations, companies must contend with the "potentially conflicting requirements" of state data use and breach notification guidelines).

[19] *Id.* at 179 ("One potential explanation for the high number of breaches that occur today is the lack of uniform standards employed by various institutions. If every institution were monitored and required to employ at least a minimum baseline of protection, hackers would not be able to take advantage of institutions with suboptimal security requirements." (footnote omitted)).

[20] Regulation (EU) 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) at 87–88 [hereinafter GDPR] ("[The GDPR] shall apply from 25 May 2018. This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Brussels, 27 April 2016.").

[21] Rachel F. Fefer and Kristin Archick, *EU Data Protection Rules and U.S. Implications*, Congressional Research Service (Feb. 7, 2019) ("Many U.S. firms have made and are making changes to comply with the GDPR.").

The European concern for data privacy protection dates from the 1970s.[22] However, because the variety of standards across Europe threatened to limit the free flow of information across borders, the European Parliament enacted the 1995 Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Directive).[23] The goal of this directive was to "harmonize [] national privacy laws" across the European Union (EU).[24] However, because the 1995 Directive was not a regulation, individual member nations implemented the directive into their own national laws, resulting in a lack of uniformity.[25]

In an effort to remedy the shortcomings of the 1995 Directive, the GDPR "seeks to strengthen individual fundamental rights and facilitate business by ensuring more consistent implementation of data protection rules EU-wide."[26] It is a comprehensive approach to data privacy which "identifies what is a legitimate basis for data processing and sets out common rules for data retention, storage limitation, and record keeping."[27] Moreover, its reach is global as it applies not only to all organizations established in the EU which process personal data, irrespective of the physical location of the data processing, but also to all entities outside the EU offering goods or services, whether or not for profit, to individuals located in the EU, or which monitor the behavior of individuals located in the EU.[28]

The GDPR broadly defines personal data as encompassing "any information relating to and identified or identifiable natural person," including names, identification numbers, location data, online

---

[22] Mulligan, *supra* note 3, at 41 ("Beginning in the 1970s, individual European countries began enacting broad, omnibus national statutes concerning data protection, privacy, and information practices.").

[23] *Id.* (stating that due to different standards across Europe, the EU wanted to harmonize various national privacy laws and adopted the Data Protection Directive).

[24] *Id.*

[25] *Id.* at n.388 ("Directives apply to all EU countries, but EU law authorizes each nation to determine the 'form and methods' by which the directive is implemented into its national law. Regulations, by contrast, are binding as written and apply directly to all member states. Because the 1995 Data Protection Directive was a directive rather than a regulation, EU member states implemented its requirements somewhat differently." (footnotes omitted)).

[26] Fefer, *supra* note 21.

[27] *Id.*

[28] *Id.* (summarizing scope and requirements of GDPR).

identifiers, and other information specific to that person's identity.[29] Data processing is similarly broad in scope and means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means," and includes actions such as collecting, storing, organizing, disclosing, or destroying the data.[30] On the other hand, although the regulations apply to any organization with an "establishment" in the EU and which processes data in the context of that establishment, "establishment" is not precisely defined.[31] Still, the GDPR states an establishment "implies the effective and real exercise of activity through stable arrangements. . . . The legal form of such arrangements . . . is not the determining factor in that respect."[32]

Significantly, the GDPR requires a "lawful basis" for processing data and lists six possible such bases: (1) consent, (2) performance of contract, (3) compliance with a legal obligation, (4) protection of the "vital interests" (i.e., the life) of the data subject or another individual, (5) tasks carried out in the public interest (e.g., by a government entity), and (6) the "legitimate interests" of the data controller or third party where the data subject's fundamental rights do not override such interests.[33] The "legitimate interests" category is considered the most flexible, serving as a basis for common activities such as "processing carried out in the normal course of business, provided that the processing is not unethical, unlawful, or otherwise illegitimate."[34]

A common mistake companies have made when working to comply with the GDPR is an overreliance on consent, which must be "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,"[35] as a legal basis for data collection.[36] Some companies defaulted to asking for consent as the legal

---

[29] GDPR, 2016 O.J. (L. 119/1) at art. 4(1).
[30] *Id.* at art. 4(2).
[31] Mulligan, *supra* note 3, at 42 (examining the territorial reach of the GDPR).
[32] GDPR, 2016 O.J. (L. 119/1) at 22.
[33] Mulligan, *supra* note 3, at 43–44.
[34] *Id.* at 44.
[35] GDPR, *supra* note 32, at 32.
[36] Justin P. Webb & Sarah A. Sargent, *An American Perspective on the GDPR One Year in*, 11 LANDSLIDE 13, 14 (2019) (opining that of the six enumerated legal bases, "consent has the most pitfalls because individuals may always withdraw their consent and force the company to stop processing the data.").

basis for all data processing even though one of the other six bases would have sufficed.[37]

In addition, the GDPR places obligations on organizations subject to its regulation, including a duty to notify a designated data authority of a personal breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it," unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[38] For example, a breach which exposes customer data such as identification numbers or credit card information that could be used for identity fraud must be reported, whereas the exposure of an office's telephone number directory may not need to be.[39] Moreover, organizations must "implement a range of measures designed to ensure and demonstrate that they are in compliance . . . proportionate in relation to the processing activities."[40] This may mean implementing new data protection policies or working to implement compliance measures into all stages of data collection and processing, not just the final product.[41]

Lastly, perhaps the biggest headlines about the GDPR have been in regard to the heavy fines it authorizes each nation's data authority to levy for certain breaches, which ranges from (1) the greater of up to ten million Euros or 2% of global annual revenue, to (2) the greater of up to twenty million Euros or 4% of global annual revenue for more, the latter scale being applied to egregious violations involving negligent or intentional behavior.[42] EU residents also have a

---

[37] *Id.* (lamenting that companies pointlessly sent users "an avalanche of e-mails in May 2018 asking for consent to continue using personal data" because "[m]any of these e-mails were unnecessary because the companies either had already obtained consent or could have relied on another legal basis.").

[38] GDPR, *supra* note at 32, at recital 85.

[39] Mulligan, *supra* note 3, at 47 (continuing that there is also a duty to notify individuals if the breach poses a "high risk" to their individual rights and freedoms, though this is a higher threshold).

[40] *Id.* at 46.

[41] *Id.* (giving examples of other measures, including keeping records of data processing activities, assessing the likelihood of risks, appointing a data protection officer, and entering into contracts with data processors which take GDPR requirements into consideration).

[42] Catherine Barrett, *Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection?*, 15 SCITECH LAW. 24, 26 (2019) [hereinafter *De Facto Global Standards*] (giving as example Marriott International, which in 2018 suffered a breach which for

private right of action for breaches and can file complaints with their respective regulatory authority and pursue compensation in the form of damages.[43]

Despite these burdens, the EU hopes the GDPR will simplify compliance through uniformity and thereby strengthen the EU Digital Single Market.[44] Even when companies "engage in cross-border data processing" across the EU, they need only "liaise with the supervisory authority of the EU country where the firm is established (the 'lead' authority)."[45] Many U.S.-based companies that also operate within the EU have already made changes to comply with the GDPR, such as clarifying user terms of agreement and sending e-mails asking for affirmative user consent to data collection.[46] Despite the promise of a simple, unified system for compliance, U.S. firms are concerned about the potential costs of adhering to the requirements, which may be too high for smaller businesses to invest in, as well as the chilling effect limitations on data analysis could have for future innovations.[47]

---

four years had "exposed the personal data, such as names, passport numbers and credit card numbers, of up to 500 million customers. . . Under the GDPR, the American company could face fines of up to 4% of annual revenue. In 2017, Marriott International "generated approximately 22.9 billion U.S. dollars in revenue," so the fine could total US$916 million." (quoting Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, WASHING. POST (Nov. 30, 2018), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breachimpacting-million-guests/?utm_term=.b4048d495d06)).

[43] Mulligan, *supra* note 3, at 50 ("Individuals also have the right to an "effective judicial remedy" (i.e., to pursue a lawsuit) against the responsible data processor or controller, and individuals may obtain compensation for their damages from data processors or controllers." (quoting GDPR, art. 83(5))).

[44] Fefer, *supra* note 21 (explaining that the purpose of the EU Digital Single Market is to "increase[e] harmonization across the bloc on digital policies.").

[45] *Id.* (clarifying that companies are "still subject to oversight and enforcement by the supervisory authority of every country where [they] do business.").

[46] *Id.* ("While it creates more requirements on companies that collect or process data, some experts contend that the GDPR may simplify compliance for U.S. firms because the same set of data protection rules will apply across the EU.").

[47] *Id.* ("Some U.S. businesses, including several newspaper websites and digital advertising firms, opted to exit the EU market rather than confront the complexities of GDPR.").

D. Current U.S. Data Privacy Laws

The privacy laws of the United States are based on the fundamental idea that privacy is a good, as opposed to the European idea of privacy as an immutable, fundamental right.[48] U.S. common law does little to protect privacy, with only a handful of torts applicable to breaches of an individual's privacy by a private party.[49] Although the Bill of Rights provides a few narrow guarantees of privacy, it does not guard against invasion by private entities.[50] Even the most directly applicable amendment, the Fourth Amendment "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[51] like common law torts and other relevant Amendments, "focus[es] on the public disclosure of private facts."[52] Given the lack of constitutional protections, statutes must be the source for effective data protection standards.[53]

The U.S., however, lacks a comprehensive federal data privacy framework and instead relies on a "patchwork" of federal laws[54] supplemented by state statutes.[55] Federal regulations apply nationwide

---

[48] *Confiding in Con Men*, *supra* note 6, at 1059–60 ("The central goal of U.S. privacy law is to create an environment where industry experiments first and asks questions later, while privacy law that in any way hinders that ability is often criticized as paternalistic or retrogressive—or worse, European. In Europe, the conceptual and regulatory balance is reversed. As both privacy and data protection are considered fundamental human rights, legal protections for such rights are fulsome and tend to prioritize the protection of individual rights over ease of compliance for companies.").

[49] Mulligan, *supra* note 3, at 3 (Although common law had long protected against eavesdropping and trespass, these protections said little to nothing about individual rights to privacy, per se." (footnote omitted)).

[50] *Id.* at 5 ("[T]he Constitution's Bill of Rights protects individual privacy from government intrusion in a handful of ways and does little to protect from non-governmental actors.").

[51] U.S. Const. amend. XIV.

[52] Mulligan, *supra* note 3, at 7 ("This focus limits their potential influence on modern data privacy debates, which extends beyond the disclosure issue to more broadly concern how data is collected, protected, and used.").

[53] *Id.* (commenting that the state action doctrine prevents private conduct from being scrutinized under the Constitution).

[54] *Id.* (contrasting U.S. "patchwork" of statutes relating to data protection policies of private companies with the single, comprehensive laws of Europe and some other parts of the world).

[55] *Id.* at 54 ("[S]ome state laws focus solely on data security or address a particular security concern, such as data breach notifications. Other state laws

but "most impose data protection obligations on specific industry participants . . . or specific types of data."[56] For example, the Health Insurance Portability and Accountability Act (HIPAA) authorizes the Department of Health and Human Services to protect protected health information and applies to health care providers, health plans, and health care clearinghouses.[57] Similarly, the Gramm-Leach-Bliley Act (GLBA) imposes data protection obligations on financial institutions regarding consumer's information,[58] and the Children's Online Privacy Protection Act (COPPA) regulates the online collection and use of children's information.[59] Due to the fractured nature of these and similar state regulations, activity which does not fall under an enumerated category is practically unregulated,[60] theoretically incentivizing companies to innovate and experiment.[61]

---

isolate a single privacy-related issue, such as the transparency of data brokers-companies that aggregate and sell consumers' information, but that often do not have a direct commercial relationship with consumers." (footnotes omitted)).

[56] *Id.* at 7–8.

[57] *Id.* at 10–11 ("The HIPAA regulations generally speak to covered entities': (1) use or sharing of [protected health information], (2) disclosure of information to consumers, (3) safeguards for securing PHI, and (4) notification of consumers following a breach of PHI.").

[58] *Id.* at 8–9 ("These obligations are centered on a category of data called 'consumer' 'nonpublic personal information' (NPI), and generally relate to: (1) sharing NPI with third parties, (2) providing privacy notices to consumers, and (3) securing NPI from unauthorized access." (footnotes omitted)).

[59] *Id.* at 24 ("COPPA's requirements apply to: (1) any "operator" of a website or online service that is 'directed to children,' or (2) any operator that has any 'actual knowledge that it is collecting personal information from a child' (i.e., covered operators). Covered operators must comply with various requirements regarding data collection and use, privacy policy notifications, and data security." (footnotes omitted)).

[60] *Confiding in Con Men*, *supra* note 6, at 1069 (giving as example the limitations of HIPPA, "which protects health privacy, [but] only applies to information collected by a healthcare provider. *Any other collection or use* of health information, for instance, by a healthcare startup selling predictive judgments on patients to insurance companies, or a period-tracking app hawking assessments of the likelihood that its users will conceive to their employers, *is not covered by the law*." (emphasis added) (footnotes omitted)).

[61] *Id.* at 1081 (arguing that "the weaknesses of U.S. privacy law are heavily influenced by a policy approach that seeks to minimize the dangers of privacy violations, such that strong consumer protections are characterized as a barrier to innovation rather than a necessary safeguard.").

The most far-reaching federal legislation regarding data privacy and security is the Federal Trade Commission Act[62] (FTC Act), which grants the FTC jurisdiction over most organizations and broadly authorizes enforcement action against "unfair or deceptive acts or practices in or affecting commerce."[63] Although the FTC Act fills some of the gaps left by the patchwork of other regulations, in practice, its effects are starkly limited.[64] An act is "unfair" only if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[65] Additionally, the FTC Act includes broad exceptions for certain industries, restricting its current capacity to function as a general regulator for all data usage.[66]

E. The CCPA

The first truly expansive data privacy and protection act to surface in state legislation is the CCPA, approved on June 28, 2018 and enforced as of January 1, 2020.[67] The CCPA has rightfully drawn comparisons to the GDPR in that unlike current federal regulations, it is not limited by industry or types of data.[68] Rather, "the CCPA applies

---

[62] 15 U.S.C. §§ 41–58 (2018).

[63] 15 U.S.C. § 57a (2018).

[64] *Confiding in Con Men*, *supra* note 6, at 1074 ("[T]he [FTC]'s ability to police abusive privacy practices is severely curtailed by the limits of its statutory authority, its reactive rather than proactive approach to shaping privacy practices, and the sheer size of the job in comparison to the agency's available manpower, legal tools, and monetary resources. Reticence to enforce also seems to play a role." (footnotes omitted)).

[65] 15 U.S.C § 45n (2018).

[66] 15 U.S.C. § 45a(2) (2018) ("[The FTC] is hereby empowered and directed to prevent persons, partnerships, or corporations, *except banks, savings and loan institutions* . . . , *Federal credit unions* . . . , *common carriers* . . . , [and] *air carriers and foreign air carriers* . . . , from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." (emphasis added)).

[67] California Consumer Privacy Act of 2018, A.B. 375, Ch. 55 (2018), eff. Jan. 1, 2019.

[68] Mulligan, *supra* note 3, at 38 ("The CCPA also does not distinguish between the sources of the data that comes within its scope. Rather, the CCPA regulates all 'personal information,' which, by the CCPA's definition, covers nearly any information a business would collect from a consumer.").

to any company that collects the personal information of Californians, is for-profit, does business in California, and satisfies a basic set of thresholds."[69] These thresholds provide a low enough bar that even small companies will likely fall under the legislation's broad reach.[70] The "personal information" regulated by the CCPA includes almost any information a business could gather from its consumers, namely "information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[71]

Unlike the GDPR, which requires each member state to form a Data Protection Authority to enforce penalties, the CCPA is enforced via actions brought by the California Attorney General.[72] CCPA fines are based on the number of users violated, not the overall scope of the violation as in the GDPR, and provide for civil penalties of up to $7,500 per violation.[73] However, businesses which fail to provide adequate protections in violation of the act are generally given thirty days to cure their violation, although the CCPA does not elaborate on the precise meaning of "cure."[74] In addition, this statute authorizes private causes of action for breaches resulting from unreasonably lax security measures in the form of up to $750 per incident or actual damages, whichever is greater, in addition to other relief, such as an injunction, though these causes also require a thirty-day notice to allow a chance to cure the violation.[75] Actual monetary losses, however, do not require notice before filing suit.[76]

The CCPA has the potential to be a significant piece of legislation both on its own and as a model. With nearly forty million residents and the fifth largest economy in the world, California is the most populous and wealthy state in the United States.[77] Consequently,

---

[69] *Id.*

[70] *Id.* ("Analysts have suggested that . . . the law could reach a considerable number of even 'relatively small' businesses with websites accessible in California.").

[71] CCPA at § 1798.140(o)(1); *see also* Mulligan, *supra* note 3, at 38 ("The law does not require the presence of any individual identifier, such as a name or address, for data to fall within the meaning of personal information.").

[72] *Id.* at § 1798.135.

[73] *Id.* at § 1798.155.

[74] *Id.* at § 1798.150.

[75] *Id.*

[76] *Id.*

[77] Associated Press, *California is now the world's fifth-largest economy, surpassing United Kingdom*, L.A. TIMES (May 4, 2018, 1:50 PM) https://

legislation affecting businesses which interact with California residents has a national, and even global reach.[78] Thus, the CCPA could serve as a model for future state legislation and even for a potential future federal framework.[79]

F. Potential Federal Privacy Regulation

Congress is already risking falling behind in the sphere of data privacy.[80] Transatlantic trade between the United States and Europe encompasses $2.7 billion dollars in goods and services every day and the annual trade in digital services amounts to $260 billion.[81] Consequently, U.S. companies are already working to comply with the GDPR in an effort not to be locked out of the European market.[82] Therefore, many argue that without U.S. congressional legislation, the U.S. risks allowing the GDPR, instead of a U.S. federal privacy law, to

---

www.latimes.com/business/la-fi-california-economy-gdp-20180504-story.html [https://perma.cc/HQV6-7J6Z] (detailing that as of 2017, only China, Japan, Germany, and the rest of the United States outstrip California in terms of GDP).

[78] *De Facto Global Standards*, *supra* note 42, at 28 ("[G]iven California's large population and economy, and the fact that 'many (if not most) American companies service California consumers,' companies will need to comply with the CCPA, even if the company has no physical presence in California . . . Realistically, 'few companies are likely to devote the resources necessary to provide . . . opt-out options to a user visiting a Web site from an IP address in California, while providing a Web site without those features to residents of the other 49 states.'" (citations omitted)).

[79] Mulligan, *supra* note 3, at 3–40 ("Statements by some Members of Congress during Congressional hearings have already noted the CCPA's likely importance to future federal legislative efforts.")

[80] Fefer, *supra* note 21 ("With no multilateral rules on cross-border data flows, experts contend that the GDPR may effectively set new global data privacy standards, since companies and organizations will strive for compliance to avoid being shut out of the EU market or penalized, and other countries may introduce rules that imitate the GDPR. . . . Such developments could limit U.S. influence in future trade negotiations on issues related to digital trade and cross-border data flows.").

[81] *Id.* ("The transatlantic economy is the largest in the world. . . . The United States and [the] EU are each other's largest customers of digitally delivered services exports.").

[82] *Id.* ("Many U.S. firms have made and are making changes to comply with the GDPR, such as revising and clarifying user terms of agreement and asking for explicit consent.").

set global standards.[83] Other major nations are already following the EU's lead, such as China[84] and Japan.[85] However, officials in the Trump Administration criticize the GDPR as being too prescriptive and likely to stymie corporate innovation by burdening businesses with too many regulations.[86]

Despite the fears of the Trump Administration, there is already a significant amount of federal and state legislation affecting how corporations collect and use consumer data.[87] Therefore, enacting a comprehensive federal data protection law with new requirements would create a single set of rules all businesses would adhere to and likely preempt state laws on the same subject, resulting in a net *decrease* in regulations.[88] There remains some debate as to whether a GDPR-type federal statute would create blanket data protection requirements for all personal data in addition to the sector-specific requirements in the current patchwork of federal legislation, or rather, allow existing regulations such as HIPPA and GLBA to continue to

---

[83] *Id.* ("With no multilateral rules on cross-border data flows, experts contend that the GDPR may effectively set new global data privacy standards, since companies and organizations will strive for compliance to avoid being shut out of the EU market or penalized").

[84] Mulligan, *supra* note 3, at 50 ("[C]ommentators have described China's Personal Information Security Specification, which defines technical standards related to the collection, storage, use, transfer, and disclosure of personal information, as modeled on the GDPR.").

[85] Webb, *supra*, note 36, at 17 (citing Michihiro Nishi, *Japan: Data Protection in Japan to Align with GDPR*, Mondaq (Sept. 27, 2018)), http://www.mondaq.com/x/739986/Data+Protection+Privacy/Data+Protection+In+Japan+To+Align+With+GDPR).

[86] Mulligan, *supra* note 3, at 52 ("The Administration has argued that many comprehensive data privacy models have resulted in "long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users" (citing *Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018))).

[87] *See supra* Section D (analyzing the current "patchwork" of federal and state data privacy legislation).

[88] Zachary N. Layne, *The Modern Threat: Data Breaches, Security Measures, and a Call for Changes*, 23 N.C. BANKING INST. 159, 176 (2019) ("Under [a] scheme [in which a federal body promulgates regulations], state regulations should be preempted by the federal regulations, as the state regulations that were designed to 'plug gaps' will no longer be necessary.").

operate by specifying general data protection rules do not apply where federal enforcement already exists.[89]

Any federal law would have to contend with the multitude of state laws already in place by preempting them in whole or in part.[90] If the federal regulation is designed to function as comprehensive U.S. data protection law, Congress could express its intent in the language of the regulation to preempt all state law "related to" this matter.[91] Conversely, "Congress could alternatively take a more modest approach to state law . . . [which] would leave intact state schemes parallel to or narrower than the federal scheme."[92]

The CCPA is already serving as, at the very least, inspiration for other states.[93] Since its passage, more than twenty-five states have introduced bills addressing data privacy.[94] While most of this legislation failed, "[l]awmakers on both sides of the aisle have expressed interest in passing a federal privacy bill, with California's law and the GDPR possibly serving as models."[95] However, the impact of the

---

[89] Mulligan, *supra* note 3, at 57 (proposing two avenues for future federal comprehensive legislation vis-à-vis current federal regulations, namely either creating layers of federal rules composed of "(1) general data protection requirements for "personal" information and (2) sector-specific requirements for data regulated by the existing 'patchwork' of data protection laws" or "avoid[ing] dual layers of regulations by stating that the proposed data protection requirements would not apply to individuals or entities covered by certain existing federal privacy laws.").

[90] *Id.* at 62 (distinguishing three types of federal preemption of state law under the Constitution's Supremacy Clause: conflict, express, and field. Conflict preemption is the enforcement of federal law where federal and state laws are contradictory. Express preemption takes place when Congress explicitly states its intent to preempt state law in the text of the federal law. Field preemption takes effect when federal law has such broad scope that there is no room for state laws to operate in its sphere).

[91] *Id.* at 63 ("[Language expressing intent to preempt state law] can be used to displace all state laws in the digital data privacy sphere to promote a more uniform scheme.").

[92] *Id.*

[93] *See supra* section E (analyzing the CCPA's requirements and goals).

[94] Melissa Quinn, *California data-privacy law may become the model for Congress*, WASH. EXAMINER (July 22, 2019, 12:01 AM) https://www.washingtonexaminer.com/news/california-data-privacy-law-may-become-the-model-for-congress [https://perma.cc/RE58-FY9R] (adding that "Illinois and Washington took the most comprehensive approach, while others considered piecemeal measures.").

[95] *Id.*

CCPA has not yet been realized, so both states and Congress are hesitant to pass their own versions before seeing what the consequences are in California.[96]

Some argue that data constitutes speech and thus any regulation of it should be considered in light of First Amendment protections.[97] Others reason that "[t]he Supreme Court has never interpreted the First Amendment as prohibiting all regulation of communication,"[98] so expanding it to cover commercial data would stretch the Amendment beyond the scope of the Constitution and invite overly restrictive government regulation of ordinary commercial activity.[99]

As mentioned above, the FTC already has the most direct power to regulate data use[100] and would therefore likely be an appropriate enforcement agency for future federal regulations.[101] However, the FTC is statutorily limited in its authority: it generally cannot issue fines for first-time offenses; it lacks jurisdiction over banks, common carriers, and certain other types of entities; and it cannot utilize the usual federal agency "notice-and-comment" process to promulgate new regulations.[102] Additionally, though the FTC has authority to

---

[96] *Id.* ("While policymakers in other states looked to California's bill as an example, its delayed implementation may have caused some wariness since the effects weren't yet apparent. Instead, states like North Dakota approved studies to examine consumer personal data disclosures.").

[97] Mulligan, *supra* note 3, at 64 (arguing that forms of data can constitute speech, which require first amendment protections).

[98] *Id.*

[99] *Id.* ("As the Supreme Court has explained, simply because regulated activity involves 'communication' does not mean that it comes within the ambit of the First Amendment." (citing *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978))).

[100] *Confiding in Con Men*, *supra* note 6, at 1073 (contrasting other agencies, which are limited to enforcing certain industries' use of information as defined by the ambit of specific legislation, "any company in the FTC's jurisdiction that used the information in a way that would constitute an unfair or deceptive trade practice would be subject to the FTC's oversight.").

[101] Mulligan, *supra* note 3, at 57 ("Of [the] agencies [responsible for enforcing the patchwork of current federal data protection laws], the FTC is often viewed—by industry representatives, privacy advocates, and FTC commissioners themselves—as the appropriate primary enforcer of any future national data protection legislation, given its significant privacy experience." (citations omitted)).

[102] *See supra* notes 48–66 and accompanying text (describing extent of FTC authority over data protection policies); Mulligan, *supra* note 3, at 57–58

regulate both deceptive and unfair practices vis-à-vis data privacy, it "rarely relies on its unfairness authority, with the latter requiring the agency to reach the lofty threshold of 'a clear theory of substantial likelihood of harm to consumers that is not outweighed by any countervailing benefits.'"[103] Of course, these limitations could be lifted by new statutes,[104] empowering the FTC to enforce and maintain a theoretical, comprehensive federal framework.

Professor Jack Balkin of Yale Law School has proposed that instead of a comprehensive, GDPR-style piece of federal legislation, the United States should instead consider applying fiduciary duties of care, loyalty, and confidentiality to data-collecting entities.[105] Traditional fiduciary relationships such as between doctor-patient, lawyer-client, and investment advisor-client/customer involve circumstances where one party provides a specialized service to the other that involves sensitive information and thus, a monetary incentive to abuse the client's trust.[106] Such fiduciaries are thus "generally prohibited from benefitting from their clients' information in a way that could hurt the client."[107] Therefore, information fiduciaries would be barred from "inducing trust in their users to obtain their information, then

---

(listing the various ways in which the FTC's enforcement authority is restricted and limited).

[103] *Confiding in Con Men*, *supra* note 6, at 1075 (citing Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 522 (2018) (continuing that the FTC's overreliance on its deception authority means the agency focuses on whether companies are open about their practices, not whether those practices are actually harmful to users).

[104] Mulligan, *supra* note 3, at 58 ("While Congress may not be able to legislate around constitutional constraints, future legislation could address some of [the FTC's] limitations").

[105] *Confiding in Con Men*, *supra* note 6, at 1088 ("Like traditional fiduciaries, companies that collect enormous amounts of data on individuals have a strategic advantage over their clients due to the fact that they are trusted with the user's sensitive information, in addition to superior and specialized knowledge, lack of transparency, and the reliance of their users on the specialized services provided.").

[106] *Id.* at 1089 ("Traditional fiduciaries are generally prohibited from benefitting from their clients' information in a way that could hurt the client: using client information to enrich themselves in a way that disadvantages the client would violate the duty of loyalty, and sharing it beyond prescribed limits would violate the duty of confidentiality.").

[107] *Id.*

using that information to the benefit of the fiduciary and the detriment of the user, in violation of that trust."[108] Balkin argues that considering data collectors as information fiduciaries would recognize the legitimate professional interests of tech companies in collecting and analyzing data while "help[ing] to adjust the objective of U.S. privacy law to more heavily prioritize the rights of the user."[109]

G. How U.S. Companies Should Respond to and Prepare for New Data Privacy Legislation

It is important for companies to understand whether data privacy legislation applies to them.[110] The European Council published a set of Guidelines to clarify who is subject to GDPR regulation.[111] These Guidelines specify that non-EU entities must "actually direct activity" towards the EU to trigger the GDPR, meaning that "tangential interactions with the EU, standing alone, are unlikely to apply the GDPR to many U.S. companies."[112] In the initial days of the GDPR, the New York Times took the cautious route of assuming the regulation applies to them due to their extensive activity in the EU and thus made a permanent change to their advertising structure by removing automated, behavior-targeting ads in the EU.[113] Other companies, whose interactions with EU residents were more incidental, took a wait-and-see approach that often turned out to be prudent, as the European Council's Guidance later confirmed their activities did not

---

[108] *Id.* at 1094.
[109] *Id.* at 1088.
[110] Webb, *supra* note 36, at 14 (warning that misunderstanding applicability is one of the most common mistakes companies have made in the wake of GDPR's enforcement).
[111] Guidelines 3/2018 on the Territorial Scope of the GDP (Article 3) at 15–16 (providing a list of factors which could be taken into consideration in determining whether an entity is subject to GDPR regulation, including whether any member state is specifically named in reference to good or service, a search engine is paid to reference the site for EU residents' access, the activity is of an international nature, etc.).
[112] Webb, *supra* note 36, at 16.
[113] *Id.* (adding that despite the shift away from automated, behavioral-targeting ads, the company's digital advertising business in Europe actually improved).

subject them to regulation.[114] Another option for companies concerned they are subject to regulation is to mitigate GDPR compliance costs and risk of noncompliance by spinning off operations involving processing EU data to subsidiaries established in the EU, or building GDPR compliance into vendor contracts to shift the compliance burden.[115]

Like the GDPR, the CCPA is expansive in scope, covering many forms of data, broadly defining "sale" and "personal data," and providing for both governmental enforcement and private rights of action.[116] Even so, the law does not include a roadmap for compliance and does not include express requirements for new company data policies, risk management, or accountability standards.[117] Instead, it may be useful to consider the Department of Justice's 2019 guidance for white-collar prosecutors evaluating corporate compliance programs, which includes reviewing whether compliance programs are: (1) well-designed, (2) being applied effectively and in good faith, and (3) actually functioning as intended.[118] Corporations should consider what their overall data privacy and security strategy is in order to determine how many resources should be allocated to security and how risks should be assessed.[119] Some companies may find it

---

[114] *Id.* at 16–17 ("This approach proved fruitful for some, as the Territorial Guidance confirmed that companies must intentionally target individuals in the EU to satisfy the extraterritorial tests.").

[115] *Id.* at 17 ("In such a scenario, the vendor does not become subject to the GDPR legally, but merely contractually, which can lessen the burden of compliance.").

[116] *Data privacy enforcement on the rise in the US – California's CCPA setting the benchmark*, Dentons Insights 1 (Aug. 19, 2019) https://www.dentons.com/en/insights/articles/2019/august/20/data-privacy-enforcement-on-the-rise-in-the-us-californias-ccpa-setting-the-benchmark [https://perma.cc/U72W-T3QL] ("[T] the new regime signals a significant shift in US privacy law and will greatly impact how covered businesses collect, use, store and share the 'personal information' of all California residents, including non-consumers, job applicants, employees and business-to-business partners.").

[117] *Id.* ("From a compliance perspective, [the CCPA is] somewhat of a blank slate.").

[118] *Id.* at 4 (explaining that these guidelines are topics the Criminal Division of the U.S. Department of Justice considered relevant for prosecutors when evaluating "whether, and to what extent, a corporation's compliance program was effective at the time of a criminal offense.").

[119] *Id.* (adding that determining data security strategy also helps in designing a risk management program).

worthwhile to segregate data policies based on jurisdictional requirements whereas others may determine it is most cost-effective to apply the new data policy to all consumers, even though doing so may increase liability exposure.[120] Companies should also consider how much risk its third-party relationships introduce into their data security regime and conduct information security audits of their internal standards as well.[121]

H. Conclusion

The current patchwork of federal regulations is inadequate to deal with the growing threat and severity of data breaches.[122] State legislation such as the CCPA and foreign regulations like the GDPR are inevitable, and it is likely Congress will act to expand federal authority in this area.[123] Regardless of the regulatory environment, the risks and costs of data breaches are such that companies should take proactive steps now to update their data protection policies.[124]

Kellen Safreed[125]

---

[120] *Id.* (providing as an example the question of whether a business operating in 25 states should use a single privacy policy for all or carve out a separate policy for California residents in light of the new CCPA requirements).

[121] *Id.* at 5 ("Third-party risk management is especially important for CCPA compliance because the transfer of personal information to service providers is exempt from the opt-out rights.").

[122] *See supra* notes 5–19 and accompanying text (discussing the threats data breaches pose to modern companies).

[123] *See supra* notes 80–109 and accompanying text (analyzing possible models of federal legislation).

[124] *See supra* notes 1–4 and accompanying text (explaining the high costs and increasing danger of data breaches).

[125] Student, Boston University School of Law (J.D. 2021).