DATA PROTECTION IN THE WAKE OF THE GDPR: CALIFORNIA'S SOLUTION FOR PROTECTING "THE WORLD'S MOST VALUABLE RESOURCE"

JOANNA KESSLER*

TABLE OF CONTENTS

INTRODUCTION

The concept of privacy has gradually evolved with the development of new technology.[1] An increasing number of businesses and organizations

*. Executive Senior Editor, Southern California Law Review, Volume 93; J.D. Candidate 2020, University of Southern California Gould School of Law; B.A., Sociology 2013, Kenyon College.

1. Keith Johnson, *What Is Consumer Data Privacy, and Where Is It Headed?*, FORBES (July 9, 2018, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#4a2da3131bc1 [https://perma.cc/AR68-XZ3K].

utilize technology to gather information about consumers.[2] This extensive collection of data prompts serious concerns about data privacy and security as devices and internet services collect a significant amount of personal information, which can be vulnerable to data breaches if not properly secured.[3] Many consumers are unaware of both the amount of information they are providing to businesses and the ways in which companies are using this data, although recent data-breach scandals have helped propel this issue to greater prominence in the political arena and the eyes of the public.[4]

Personal data has been described as surpassing oil as the world's most valuable resource.[5] While consumers may believe they are reaping the benefits of a particular service for free, they often do not realize that they are paying currency in the form of their personal data.[6] Companies routinely "collect, analyze, share, and sell" consumers' personal information.[7] Marketers are willing to pay for this data, which they typically analyze to facilitate their advertising efforts.[8] Thus, those who are willing to pay for data end up footing the bill for our favorite "free" online services.[9] However, consumers often do not fully comprehend the tradeoff they are making by virtue of the opportunity to use these services for free because these caveats are contained within complicated and lengthy privacy policies that consumers are unable to—or choose not to—read.[10]

Data-breach scandals in recent years have contributed to a greater awareness of what consumers are relinquishing when they take advantage of certain internet resources. For example, in March 2018, news broke that a political consulting firm called Cambridge Analytica misused the personal data of tens of millions of Facebook users for political purposes.[11]

2. Debra J. Farber, *Foresight Is 20/20: How to Prepare for the California Consumer Privacy Act Now*, CMSWIRE (Oct. 18, 2018), https://www.cmswire.com/information-management/foresight-is-2020-how-to-prepare-for-the-california-consumer-privacy-act-now [https://perma.cc/TU3A-JA54].

3. S. JUDICIARY COMM., 2017–2018 REG. SESS., REP. ON INTERNET SERVICE PROVIDERS: CUSTOMER PRIVACY 1–2 (June 25, 2018), *available at* https://digitalcommons.law.scu.edu/historical/1748 [https://perma.cc/8L4E-6GD3] [hereinafter SENATE JUDICIARY COMMITTEE REPORT].

4. *Id.* at 1.

5. *Id.*

6. Johnson, *supra* note 1.

7. SENATE JUDICIARY COMMITTEE REPORT, *supra* note 3, at 1.

8. Johnson, *supra* note 1.

9. *Id.*

10. *Id.*

11. Joseph Damon et al., *The New California Consumer Privacy Act of 2018: A Practical Analysis*, JD SUPRA (July 9, 2018), https://www.jdsupra.com/legalnews/the-new-california-consumer-privacy-act-33874 [https://perma.cc/9UA4-NVHB]; Heather Kelly, *California Passes Strictest Online Privacy Law in the Country*, CNN (June 29, 2018, 12:03 PM), https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html [https://perma.cc/DE39-XJY4].

Additionally, in October 2018, Google faced extensive backlash after it came to light that the company chose not to notify the public of a breach that exposed the private data of five-hundred thousand users of the Google+ social media platform back in March 2018.[12] These revelations sparked public support for greater protection of consumer data, as well as a debate about the level of control consumers are entitled to maintain over their data.[13] This controversial issue remains unresolved, and different countries take disparate approaches to regulating practices related to personal-data privacy.[14]

Europeans have long recognized the importance of data protection and privacy.[15] Privacy has been established as a fundamental right in The Charter of Fundamental Rights of the European Union.[16] Article 8 of the Charter explicitly recognizes the right to protection of personal data.[17] Therefore, it is unsurprising that the European Union ("EU") has enacted expansive data privacy laws. In May 2018, one such expansive law, the General Data Protection Regulation ("GDPR"), went into effect.[18] The GDPR is described as "the most contested law in the [EU]'s history, the product of years of intense negotiation and thousands of proposed amendments, despite its building blocks having been present in European law for decades."[19] The law aims to provide individuals with control over their own personal data.[20]

On the other hand, the United States does not recognize a fundamental right to privacy.[21] Academics have argued that the United States "has a weak tradition of data privacy that is diametrically opposed to the EU's expansive

12. Allison Grande, *Google Data Leak Exposes Breach Disclosure Conundrums*, LAW360 (Oct. 12, 2018, 9:47 PM), https://www.law360.com/articles/1091877/google-data-leak-exposes-breach-disclosure-conundrums [https://perma.cc/9UA4-NVHB].

13. Johnson, *supra* note 1; Kelly, *supra* note 11.

14. *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 369–70 (2019).

15. *Id.* at 372.

16. *Id.* at 373.

17. *Id.*

18. *Id.* at 375.

19. Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, NEW YORKER (May 25, 2018), https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy [https://perma.cc/54GL-9LH9].

20. Giuseppe Colangelo & Mariateresa Maggiolino, *Fragile or Smart Consumers? Suggestions for the US from the EU*, COMPUTER L. & SECURITY REV. (forthcoming 2019) (manuscript at 8) (on file with author).

21. Griffin Drake, Note, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 176 (2017).

data protection laws."[22] Certain states have begun taking measures to enact their own data privacy regulations. In July 2018, the California Legislature passed the "most far-reaching privacy measure ever to be enacted" in the United States, the California Consumer Privacy Act of 2018 ("CCPA").[23] The law, which takes effect in January 2020, will require companies to overhaul the way they manage their consumers' personal data.[24] Much remains to be seen about the impact of the CCPA, including how the law will continue to evolve after it goes into effect and how other states and the federal government will react to it.

This Note will argue that although the CCPA was imperfectly drafted, much of the world seems to be moving toward a standard that embraces data privacy protection, and the CCPA is a positive step in that direction. However, the CCPA does contain several ambiguous and potentially problematic provisions, including possible First Amendment and Dormant Commerce Clause challenges, that should be addressed by the California Legislature. While a federal standard for data privacy would make compliance considerably easier, if such a law is enacted in the near future, it is unlikely to offer as significant data privacy protections as the CCPA and would instead be a watered-down version of the CCPA that preempts attempts by California and other states to establish strong, comprehensive data privacy regimes. Ultimately, the United States should adopt a federal standard that offers consumers similarly strong protections as the GDPR or the CCPA. Part I of this Note will describe the elements of GDPR and the CCPA and will offer a comparative analysis of the regulations. Part II of this Note will address potential shortcomings of the CCPA, including a constitutional analysis of the law and its problematic provisions. Part III of this Note will discuss the debate between consumer privacy advocates and technology companies regarding federal preemption of strict laws like the CCPA. It will also make predictions about, and offer solutions for, the future of the CCPA and United States data privacy legislation based on a discussion of global data privacy trends and possible federal government actions.

22. Rustad & Koenig, *supra* note 14, at 370 (footnote omitted).

23. Grant Davis-Denny et al., *The California Consumer Privacy Act: 3 Early Questions*, LAW360 (July 2, 2018, 4:28 PM), https://www.law360.com/articles/1059403/the-california-consumer-privacy-act-3-early-questions [https://perma.cc/V3EN-GG64].

24. Allison Grande, *Calif. Privacy Law to Spark GDPR-Like Compliance Efforts*, LAW360 (July 3, 2018, 10:13 PM), https://www.law360.com/articles/1059877/calif-privacy-law-to-spark-gdpr-like-compliance-efforts [https://perma.cc/R7K4-WR8S].

I. THE GDPR AND THE CCPA

A. THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

The EU's GDPR went into effect on May 25, 2018.[25] The legislation replaced the Data Protection Directive, Directive 95/46/EC, which was adopted in 1995.[26] The Directive protected the fundamental right to data protection and aimed to guarantee the free flow of personal data between EU Member States.[27] Both the GDPR and the Data Protection Directive are based on an older set of principles, the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which laid out various recommendations to protect personal data and privacy.[28] EU directives are nonbinding, as they merely set out objectives for EU countries to achieve.[29] Given that Directive 95/46/EC was not binding on EU member states and the data landscape was frequently changing, the EU needed additional regulatory guidance.[30] The GDPR was first proposed by the European Commission in January 2012.[31] After several amendments, the GDPR was approved by the EU Parliament in April 2016. It then underwent a two-year grace period and went into effect in May 2018.[32] The legislation intends to protect EU citizens from privacy and data breaches.[33] Under the GDPR, all "natural persons" enjoy a "fundamental right[]" to personal-data protection.[34] Within the GDPR, personal data is any information that is related to an "identified or identifiable individual."[35] Thus, personal data includes not only names, addresses, social security numbers and email addresses, but also location data, behavioral data, financial information, IP addresses, health

25. Rustad & Koenig, *supra* note 14, at 375.

26. *See id.* at 373.

27. *Id.*

28. *How Did We Get Here?*, EU GDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here [https://perma.cc/MK7Y-NDTC].

29. *See Regulations, Directives, and Other Acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en [https://perma.cc/T2AZ-AEU3].

30. *How Did We Get Here?*, *supra* note 28.

31. *The European Union Legislative Process*, EU GDPR.ORG, https://eugdpr.org/the-process [https://perma.cc/DE4D-ERC2].

32. *GDPR FAQS*, EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs [https://perma.cc/7GGT-3DZV].

33. *GDPR Key Changes*, EU GDPR.ORG, https://eugdpr.org/the-regulation [https://perma.cc/H9KB-PSB4].

34. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1, 32 (EU) [hereinafter GDPR].

35. *The Quick and Easy Guide for GDPR – Part 3 – GDPR in a Nutshell*, COURSEDOT, https://blog.coursedot.com/index.php/2018/03/19/the-quick-and-easy-guide-for-gdpr-part-3-gdpr-in-a-nutshell [https://perma.cc/5GCV-VPXE] [hereinafter *GDPR in a Nutshell*].

information, ethnic information, and any other data that relates to an identified or identifiable consumer.[36]

Key provisions of the GDPR include extraterritorial application to non-European companies who handle the data of European consumers, a duty to notify consumers within seventy-two hours if their data has been breached, the requirement that companies obtain consent prior to collecting consumers' personal data, and the duty to erase personal data upon request.[37] The GDPR is significantly more expansive than the Data Protection Directive that it replaced.[38] For example, its definition of personal data is much broader, it affects a wider range of companies, and it applies to companies outside of the EU.[39] The law is mandatory for all EU member states and it applies to any companies that sell, collect or store EU citizens' data or offer any goods or services in any of the thirty-one nations in the European Economic Area ("EEA").[40] The GDPR also provides consumers with additional rights, including: (1) the right to demand that a company delete their data (right to be forgotten); (2) the right to prohibit certain uses of their data (right to object); (3) the right to rectify inaccurate personal data (right to rectification); (4) the right to request that their personal data be transferred to another company (right to data portability); (5) the right to know what data is being collected, and the purposes for which it is being collected, among other things (right of access); and (6) the right to be informed within seventy-two hours in the event of a data breach (right to be notified).[41] The GDPR also mandates that companies acquire consumers' explicit consent to collect and process their data, meaning individuals must opt in to having their data collected, and silence does not constitute consent.[42] Further, the regulation

36. *Id.*; *see also* GDPR, *supra* note 34, at 33 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person . . . ."). "[A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location, data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person . . . ." GDPR, *supra* note 34, at 33.

37. Rustad & Koenig, *supra* note 14, at 376–77.

38. *See id.*

39. *Id.*

40. *The Quick and Easy Guide for GDPR – Part 2 – The Need for Regulation*, COURSEDOT (Mar. 15, 2018), https://blog.coursedot.com/index.php/2018/03/15/the-quick-and-easy-guide-for-gdrp-part-2-the-need-for-regulation [https://perma.cc/ZQ62-N7YG]. By contrast, the Data Protection Directive of 1995 only applied to non-EU companies that had a presence in Europe. *See* Rustad & Koenig, *supra* note 14, at 376–77.

41. GDPR, *supra* note 34, at 43–46, 52; Rustad & Koenig, *supra* note 14, at 376–77.

42. GDPR, *supra* note 34, at 6; *GDPR in a Nutshell*, *supra* note 35; Ibrahim Hasan, *New EU Data Protection Regulation*, LAW SOC'Y GAZETTE (Feb. 8, 2016), https://www.lawgazette.co.uk/legal-updates/new-eu-data-protection-regulation/5053436.article [https://perma.cc/2F9M-4WVQ].

requires that data controllers have a legitimate reason for processing consumers' personal data.[43] To enforce the GDPR, each member state is required to appoint independent public authorities to monitor the application of the law.[44] Additionally, most organizations handling personal data will be required to appoint a data protection officer to ensure that the company is complying with the regulation.[45] Infringements of the GDPR are subject to hefty fines, another indication that the regulation is more stringent than the Data Protection Directive of 1995.[46] For infringements of some provisions of the GDPR, companies can be subject to administrative fines of up to ten million euros or 2 percent of the total global annual turnover of the prior fiscal year, depending on which figure is higher.[47] Infringements of other provisions of the regulation will be subject to fines of up to twenty million euros or 4 percent of the total global annual turnover of the prior fiscal year.[48]

The passage of the GDPR has been met with mixed reviews. While the regulation was intended to protect consumers and advance EU citizens' fundamental right to privacy, some large technology companies have argued that the regulation impedes innovation due to its stringent compliance requirements.[49] According to Amazon Vice President and Associate General Counsel, Andrew DeVore, meeting the GDPR's requirements "required [Amazon] to divert significant resources to administrative and record-keeping tasks and away from invention on behalf of customers."[50] In the time since the GDPR was approved by the EU Parliament, other countries, including the United States, have been grappling with how to address data privacy issues within their own borders.

B. THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

In the United States, there is not yet any federal equivalent to the GDPR. Federal data protection laws enacted in the United States thus far have targeted specific industries.[51] The advantage to this approach is that the laws

43. Hasan, *supra* note 42; *see also* GDPR, *supra* note 34, at 36.

44. GDPR, *supra* note 34, at 65.

45. Hasan, *supra* note 42; *see also* GDPR, *supra* note 34, at 55.

46. *See* Hasan, *supra* note 42.

47. GDPR, *supra* note 34, at 82.

48. *Id.* at 83.

49. Ben Kochman, *Tech Giants Want Uniform Privacy Law, But No GDPR*, LAW360 (Sept. 26, 2018, 7:40 PM), https://www.law360.com/cybersecurity-privacy/articles/1086064/tech-giants-want-uniform-privacy-law-but-no-gdpr?nl_pk=5f5af549-4d24-4b9f-972b-b52dbd4ccd42&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy [https://perma.cc/F6V5-HY5].

50. *Id.*

51. Rustad & Koenig, *supra* note 14, at 381. Some of these industries include securities (Financial Industry Regulatory Authority ("FINRA")), heath care (Health Insurance Portability and Accountability

are narrowly tailored to the particular industry, but it also means that there are gaps in data protection in the United States.[52] As a result of these gaps, states have begun enacting their own data privacy statutes. California has been a consistent leader in the United States on the data privacy front, as it enacted the first laws requiring consumers to be notified of data security breaches and website privacy policies.[53] In 2018, it also enacted the CCPA, which has been described as one of the toughest data privacy laws in the country.[54] The California State Legislature moved rapidly to pass the bill.[55] On May 3, 2018, supporters of the CCPA announced that they had obtained the necessary signatures to include the act on the November 2018 ballot.[56] The ballot initiative was led and largely funded by Alastair Mactaggart, a real estate tycoon.[57] Mactaggart's version of the law was very restrictive and included numerous provisions that were described as being harmful to the business community. However, he agreed to withdraw the initiative if the legislature passed, and the governor signed, a similar version of the law by June 28, 2018.[58] The legislators were eager to pass their own law as it would be easier for them to make changes to it, whereas a ballot initiative would be more difficult to amend.[59] The legislature acted quickly and had minimal opportunities to deliberate, but was able to enact the law on June 28, 2018, right before the deadline.[60] Similar to the GDPR, the CCPA gives consumers greater control over their personal data.[61] In addition, like the GDPR, the CCPA was passed with a two-year grace period and does not go into effect until January 2020, meaning legislators have had opportunities to amend the

Act of 1996 ("HIPAA")), consumer financial services (Gramm-Leach-Bliley Act ("GLBA")), and children's online privacy (Children's Online Privacy Protection Act ("COPPA")). *Id.*

52. *Id.*

53. *See* Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, IAPP (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018 [https://perma.cc/78LJ-67NH].

54. Colin Lecher, *California Just Passed One of the Toughest Data Privacy Laws in the Country*, THE VERGE (June 28, 2018, 3:46 PM), https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote [https://perma.cc/XN9Y-ZZKH].

55. Kelly, *supra* note 11.

56. Purvi Patel & Alexandra Laks, *California May Pass Its Own GDPR*, LAW360 (May 17, 2018, 12:18 PM), https://www.law360.com/articles/1043957/california-may-pass-its-own-gdpr [https://perma.cc/X67G-FB4A].

57. Lecher, *supra* note 54.

58. ERIC GOLDMAN, INTERNET LAW 357–64 (2019); Davis-Denny et al., *supra* note 23.

59. Lecher, *supra* note 54.

60. *See* Davis-Denny et al., *supra* note 23.

61. *See* Allison Grande, *Calif. Enacts Internet Privacy Law, Erasing Ballot Effort*, LAW360 (June 28, 2018, 11:01 PM), https://www.law360.com/articles/1058573/calif-enacts-internet-privacy-law-erasing-ballot-effort [https://perma.cc/WSZ3-WB5G].

law before it takes effect.[62] The law has already been amended twice since its passing in June 2018. On August 31, 2018, the California Legislature passed Senate Bill 1121, which included some substantive revisions to certain provisions of the law, and former governor Jerry Brown signed the amendments in September 2018.[63] Attempts to amend the law prior to the end of the legislative term have continued through 2019,[64] and on October 11, 2019, Governor Newsom signed seven additional bills amending the CCPA into law.[65]

In the law's current state, the CCPA applies to businesses that collect and sell California consumers' personal information or disclose that information for a "business purpose."[66] Businesses include any for-profit legal entity "that collects consumers' personal information, or on the behalf of which such information is collected, and that . . . determines the purposes and means of the processing of consumers' personal information, that does business in the State of California . . . ."[67] The law has extraterritorial application as it is not limited to companies physically located in California, but instead applies to any that do business with California residents.[68] Additionally, the business must satisfy at least one of the following thresholds: it has an annual gross revenue of greater than $25 million; it buys, receives, sells, or shares for "commercial purposes" the personal information of at least fifty thousand consumers, households, or devices; or it derives 50 percent or more of its annual revenues from sales of consumers' personal

62. *Id.*

63. SULLIVAN & CROMWELL LLP, UPDATE—IMPORTANT AMENDMENTS TO THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (2018), https://www.sullcrom.com/files/upload/SC-Publication-Update-Important-Amendments-to-the-California-Consumer-Privacy-Act-of-2018.pdf [https://perma.cc/3XM5-TZU3]; David Caplan, *Governor Jerry Brown Signs Amendment to the California Consumer Privacy Act*, JD SUPRA (Sept. 27, 2018), https://www.jdsupra.com/legalnews/governor-jerry-brown-signs-amendment-to-20020 [https://perma.cc/LCC3-2XZD].

64. *See* Michelle Bae & Jeremy Greenberg, *CCPA Amendment Update June 2019 – Twelve Bills Survive Assembly and Move to the* Senate, FUTURE PRIVACY F. (June 4, 2019), https://fpf.org/2019/06/04/ccpa-amendment-update-june-2019-twelve-bills-survive-assembly-and-move-to-the-senate [https://perma.cc/AA3M-G3WN]. In California, bills can be introduced in either the State Assembly or the Senate, but amendments introduced in the State Assembly must be passed by a majority vote before moving to the Senate for a vote. *Id.* After passing the Senate, bills are then sent to the governor to be approved or vetoed. *Id.* The California Attorney General's Office can then clarify or modify the law by promulgating regulations under its rulemaking authority. *Id.*

65. Gretchen A. Ramos, *Governor Newsom Signs CCPA Amendments*, NAT'L L. REV. (Oct. 15, 2019), https://www.natlawreview.com/article/governor-newsom-signs-ccpa-amendments [https://perma.cc/5F62-R3JX].

66. Sara H. Jodka, *California's Data Privacy Law: What It Is and How to Comply (A Step-By-Step Guide)*, NAT'L L. REV. (July 17, 2018), https://www.natlawreview.com/article/california-s-data-privacy-law-what-it-and-how-to-comply-step-step-guide [https://perma.cc/DSP4-7VU2].

67. CAL. CIV. CODE § 1798.140(c)(1) (West 2019).

68. Jodka, *supra* note 66.

data.[69] In addition to applying to a wide range of businesses, the CCPA applies to a broad amount of information. Under the CCPA, "personal information" is any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[70] Among other things, personal data includes: (1) identifiers such as a real name, alias, mailing address, unique personal identifier, IP address, email address, social security number, driver's license number, passport number; (2) commercial information, including personal property records and products or services purchased; (3) biometric information; (4) internet activity, including search history and other information related to a consumer's interaction with a website, application, or advertisement; (5) geolocation data; (6) audio, electronic, visual, thermal, and olfactory information; (7) professional or employment-related information; and (8) education information.[71] Personal information does *not* include publicly available information.[72] The definition of "consumer" is also quite broad, as it includes any "natural person who is a California resident."[73] It is worth noting that the law does not prevent a business from collecting or selling a consumer's personal information

> if every aspect of that commercial conduct takes place wholly outside of California. . . . [C]ommercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.[74]

The CCPA affords consumers with a number of rights, including the right to know whether their personal information is being collected, which pieces of personal information a business has collected, and for what purpose the business is doing so.[75] They also have the right to opt out from the sale of their information, and they are protected from any discrimination from a business for exercising the right to opt out.[76] To comply with opt-out requirements, a business must include a "clear and conspicuous" link on its

69. CAL. CIV. CODE § 1798.140(c)(1)(A)–(C).

70. *Id.* § 1798.140(o)(1). Assembly Bill 874 amended the definition of "personal information" by qualifying the phrase "capable of being associated with" by adding the word "reasonably." Assemb. 874, 2019–2020 Reg. Sess. (Cal. 2019) (enacted).

71. *Id.* § 1798.140(o)(1)(A)–(J).

72. *Id.* § 1798.140(o)(2).

73. *Id.* § 1798.140(g).

74. *Id.* § 1798.145(a)(6).

75. *Id.* §§ 1798.100, 1798.110, 1798.115.

76. *Id.* §§ 1798.120, 1798.125(a).

webpage that says, "Do Not Sell My Personal Information."[77] While businesses may not discriminate against customers for opting out, they are permitted to offer financial incentives to consumers who do not opt out.[78] However, consumers under the age of sixteen (or the consumer's parent or guardian) must affirmatively consent to having their information sold.[79] Additionally, consumers have the right to request that the business delete their personal information, also known as the right to be forgotten.[80]

With respect to the enforcement of CCPA, a business will have thirty days after being notified of noncompliance to cure any alleged violation.[81] Businesses that violate the CCPA will be subject to an injunction and a civil penalty of no more than $2,500 for each violation or $7,500 for each intentional violation via a civil lawsuit brought by the California Attorney General.[82] The law also provides for a private right of action if a consumer's nonencrypted or nonredacted personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure" due to the business's violation of the duty to implement reasonable security practices to protect consumers' information.[83] Violators of this provision may be obligated to pay damages ranging from $100 to $750.[84]

Clearly, the requirements imposed by the CCPA are substantial, and therefore businesses will need to make significant changes to ensure they are complying with the law. Companies will need to update their privacy policies to incorporate the new rights that consumers will enjoy from the CCPA.[85] Companies will also need to maintain a database tracking their data collection activity and any requests by consumers regarding their personal data.[86] This will likely require hiring new employees and setting up departments to handle the requests for information about data being collected, manage the opt-out process, and monitor requests to be forgotten.[87] Businesses are also required to provide at least two methods for consumers to request information afforded by the CCPA, including, at minimum, a toll-free telephone number and a website address (if the business

77. *Id.* § 1798.135(a).
78. *Id.* § 1798.125(b).
79. *Id.* § 1798.120(c)–(d).
80. *Id.* § 1798.105(a).
81. *Id.* § 1798.155(a).
82. *Id.* § 1798.155(b).
83. *Id.* § 1798.150(a)(1).
84. *Id.* § 1798.150(a)(1)(A).
85. Jodka, *supra* note 66.
86. *Id.*
87. *See* Davis-Denny et al., *supra* note 23.

has a website).[88] Further, because companies will be penalized for failing to protect consumers' data through reasonable security practices, companies will need to evaluate their existing data protection measures and make any necessary changes to ensure compliance with that standard.[89] Also, due to the CCPA's requirement that consumers under the age of sixteen affirmatively consent to having their data sold, companies must find a way to determine the ages of the consumers whose data they are collecting so they know whether affirmative consent is required.[90] Companies have until January 2020 to implement their compliance processes.

The passage of the CCPA has not been without controversy, as reactions to the law have been mixed. Many have been critical of the law's rapid journey through the legislature, as the seven-day period in which the California State Legislature introduced and enacted the CCPA allowed for only minimal input from those who the law will affect.[91] Additionally, the law has been criticized as being poorly drafted due to typos, drafting errors, and "terrible policy ideas."[92] Mactaggart, who spearheaded the campaign to enact the CCPA, has countered arguments that the "sky would essentially fall" if the CCPA were left intact and that the law is anti-business.[93] Further, Mactaggart disputed claims that the law was rushed, arguing that the language in the CCPA "reflects thousands of hours of careful drafting."[94] However, it is mutually agreed by both supporters and opponents of the law that the current version of the CCPA is unsatisfactory.[95] Some privacy advocates consider the law to only modestly protect consumers' rights and believe it should be expanded, whereas opponents of the law, including a trade organization called the Internet Association, argue that the law is a "major threat" to those doing business in California.[96]

88. Consumer privacy: consumer request for disclosure methods, Assemb. 1564, 2019–2020 Reg. Sess. (Cal. 2019) (enacted). Assembly Bill 1564 amended this provision to clarify that businesses that exclusively operate online and have a direct relationship with consumers are only required to provide consumers with an email address through which they can submit requests for information. *Id.*

89. *See* Jodka, *supra* note 66.

90. Determann, *supra* note 53.

91. GOLDMAN, *supra* note 58, at 357.

92. *Id.*

93. Allison Grande, *Federal Privacy Law Shouldn't Lower the Bar, Senators Told*, LAW360 (Oct. 10, 2018, 10:36 PM), https://www.law360.com/articles/1090519/federal-privacy-law-shouldn-t-lower-the-bar-senators-told [https://perma.cc/8JB7-U4TM].

94. *Id.*

95. Kate Christensen, *The California Consumer Privacy Act of 2018: Are Your Interests at Stake?*, GOLDEN GATE U. L. REV. BLOG (Oct. 1, 2018), https://ggulawreview.wordpress.com/2018/10/01/the-california-consumer-privacy-act-of-2018-are-your-interests-at-stake [https://perma.cc/6E5N-6JFR].

96. *Id.*

C. THE CCPA VS. THE GDPR: A COMPARATIVE ANALYSIS

Given that the GDPR went into effect in May 2018 and the CCPA was enacted just one month later, it is unsurprising that the two laws are often compared with one another. At the time the law was passed, the CCPA differed drastically from every other privacy law in the United States, and its closest equivalent was the GDPR.[97] Although the laws do contain many similarities, the differences between the two laws should also be recognized. Conducting a comparative analysis of the two laws is useful for evaluating the differences between European and American data privacy laws, and the ways in which the CCPA should further conform with, or differ from, the GDPR after the California law takes effect.

1. Comparing the CCPA and the GDPR

At first blush, the CCPA and the GDPR appear to be substantially similar. For one, both laws implemented a two-year ramp-up period before taking effect, allowing companies to adopt compliance procedures and avoid being penalized in the interim.[98] Additionally, the two laws protect similar types of information. While the definition of personal information in the CCPA is much broader than is generally used in data privacy statutes elsewhere in the United States, the CCPA's protections are more similar to those of the GDPR, which also defines "personal information" broadly.[99] Both laws cover "nearly all data related to a particular individual," including data that can be linked to, or that can be used to identify, an individual.[100] The California law applies even more broadly than the GDPR as it covers not only individual data, but information pertaining to households and devices as well.[101] The rights and duties afforded by both laws are also similar. The laws grant residents the right to notice regarding the data being collected and the way it will be used, as well as the right to know what data companies have collected about them, the purposes for which the information was collected, and the types of third-parties to whom the

97. Grant Davis-Denny et al., *What Corporate Attys Should Know About Calif. Privacy Act*, LAW360 (Sept. 25, 2018, 1:47 PM), https://www.law360.com/articles/1085787/what-corporate-attys-should-know-about-calif-privacy-act [https://perma.cc/TFN7-NN47]. Now, however, several other states have begun putting forward their own data privacy laws. *See infra* Part III.

98. *See* Grande, *supra* note 93.

99. Michael R. Overly, *Is California's Consumer Privacy Act of 2018 Going to Be GDPR Version 2?*, NAT'L L. REV. (Sept. 6, 2018), https://www.natlawreview.com/article/california-s-consumer-privacy-act-2018-going-to-be-gdpr-version-2 [https://perma.cc/2WBZ-TUM8].

100. Grant Davis-Denny, *California's Consumer Privacy Act vs. GDPR*, LAW360 (Aug. 1, 2018, 1:42 PM), https://www.law360.com/articles/1066413/california-s-consumer-privacy-act-vs-gdpr [https://perma.cc/G3Q2-UDKB].

101. Determann, *supra* note 53.

information has been disclosed.[102] Further, the laws grant residents the right to request that a business delete information it has collected about them, as well as the right to receive their data in a portable format in order to move the data to another company.[103] The two laws are also alike in their extraterritorial application, as both apply to companies outside their borders if the companies collect the personal data of consumers located within their borders.[104]

The laws also carry significant potential liabilities, both permitting fines to be imposed on companies that do not comply, although the severity of the fines do differ.[105] In order to avoid these penalties, the two laws also require companies to overhaul their existing practices to achieve compliance.[106] Finally, both laws contain ambiguities, are complex, and will change the world of data privacy not only in California and the EU, but globally.[107]

2. Differences Between the CCPA and the GDPR

Despite the areas of overlap between the CCPA and the GDPR, the two laws also differ in important ways. The GDPR's requirements have been interpreted as being more stringent than the CCPA's.[108] For example, the GDPR applies to all companies that that sell, collect or store EU residents' data or offer any goods or services in any of the nations in the EEA,[109] but the CCPA applies minimum thresholds that companies must meet in order to be subject to the law.[110] As a result of these thresholds, smaller companies that would be subject to the GDPR could be exempt from the CCPA. Additionally, the CCPA requires companies to provide consumers above the age of sixteen with the option to opt out of having their data collected and sold, whereas the GDPR mandates that companies obtain affirmative consent to collect and process personal data.[111] While it is likely that many

102. *See id.*

103. *See id.*

104. Kristen J. Matthews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER: PRIVACY L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018 [https://perma.cc/GP4R-7BH5].

105. Davis-Denny, *supra* note 100.

106. *See* Matthews & Bowman, *supra* note 104.

107. *See* Davis-Denny, *supra* note 100.

108. Kelly, *supra* note 11.

109. *See supra* Part I.

110. *See id.* (explaining that, to be subject to the CCPA, a company must meet one of the following requirements: (1) it maintains a gross revenue of greater than $25 million; (2) it buys, receives, sells, or shares for "commercial purposes" the personal information of at least fifty-thousand consumers, households, or devices; or (3) it derives 50 percent or more of its annual revenues from sales of consumers' personal data).

111. Jodka, *supra* note 66.

consumers presented with the opt-in mechanism will mindlessly opt in without considering or caring about the consequences of having their personal data collected, the law at least tries to place greater control into the hands of consumers by requiring them to act, as opposed to the more passive opt-out requirement imposed by the CCPA. This also suggests that under the CCPA, the default rule is that data processing and sale is acceptable, and consumers must take affirmative steps to enjoy the rights afforded them by the law, whereas under the GDPR, the default presumption is that data should not be collected and sold without consent, and consumers do not have to take affirmative steps to enjoy those rights, indicating that the GDPR is more consumer-friendly than the CCPA.[112]

Another reason the California law is more lenient than the GDPR is that, under the CCPA, publicly available information does not fall under the category of personal information.[113] Publicly available information includes any information that is legally available in federal, state, or local government records.[114] This provision suggests that there is a significant amount of publicly available data that can permissibly be collected and sold under the CCPA, but not under the GDPR, which does not include an exception for publicly available information.

The GDPR permits EU residents to force businesses to correct inaccurate data, and businesses must restrict data processing when a consumer has objected to data accuracy or the lawfulness of the business's purpose for data processing.[115] Further, the GDPR also typically forbids the processing of certain types of "sensitive" data, including race, political opinions, and religious beliefs, whereas the CCPA does not mention this limitation.[116] The GDPR also imposes substantial record-keeping restrictions on businesses that have no analogue in the CCPA. For example, businesses with 250 or more employees must document all processing activity, its purposes, and to whom the information was disclosed.[117] Under the GDPR, certain businesses are also required to hire data protection officers to handle compliance tasks, whereas the CCPA does not mandate the appointment of such an employee.[118]

However, one area in which the CCPA seems to be harsher than the

112. *See* Joseph Damon et al., *supra* note 11.
113. Davis-Denny, *supra* note 100.
114. CAL. CIV. CODE § 1798.140(o)(2) (West 2019).
115. Davis-Denny, *supra* note 100.
116. *Id.*
117. *Id.*
118. *Id.*

GDPR is through its potential penalties. Although initially, the CCPA required a finding of intent to break the law, indicating it would be easier to impose fines for violations of the GDPR than the CCPA, the California State Legislature amended the CCPA's civil penalty provisions in September 2018 to include a maximum fine for *unintentional* violations of the law.[119] Potential penalties under the CCPA could be significantly higher than the maximum penalty under the GDPR, as the CCPA imposes fines per individual violation and user violated, regardless of whether the violation was intentional.[120]

Another way in which the California law may be stricter than the GDPR is through its antidiscrimination provision. The CCPA bars companies from discriminating against customers who exercise their privacy rights under the law by denying them goods or services, charging different prices, or providing a different quality of goods or services, whereas the GDPR allows companies to offer consumers a choice between paying for services and free services contingent on express consent to data monetization.[121] However, the CCPA does seem to include a loophole by allowing companies to offer financial incentives to California residents for the collection and sale of their data if they obtain prior opt-in consent, which may bring the law more in line with the GDPR.[122]

Ultimately, conducting a comparative analysis of the two laws indicates that while they appear to be similar, there are significant differences between the laws, and the GDPR is generally stricter than the CCPA. However, the CCPA is also stringent, more so than most of the existing privacy laws in the United States.[123] The differences in the two laws and their extraterritorial reach suggests that companies must closely evaluate their practices to determine whether they are complying with both laws, as compliance with

119. S. 1121, 2017–2018 Reg. Sess. (Cal. 2018) (enacted) (amending the CCPA to include a maximum penalty of $2,500 for each violation or $7,500 for each intentional violation).

120. Peter Loshin, *Is the New California Privacy Law a Domestic GDPR?*, SEARCHSECURITY (July 17, 2018), https://searchsecurity.techtarget.com/blog/Security-Bytes/Is-the-new-California-privacy-law-a-domestic-GDPR [https://perma.cc/XUT3-QNAM]. Using the 2017 Equifax data breach as an example, about twelve million Californians were impacted by the breach, meaning that under the CCPA, if the breach was caused unintentionally, the maximum fine could amount to $30 billion, and if caused intentionally, the maximum fine could amount to $90 billion. On the other hand, under GDPR, the maximum fine of 4 percent of annual global turnover would be only about $135 million.

121. CAL. CIV. CODE § 1798.125(a) (West 2019); Determann, *supra* note 53.

122. CAL. CIV. CODE § 1798.125(b); *see also* Determann, *supra* note 53.

123. Joshua A. Jessen et al., California *Consumer Privacy Act of 2018*, GIBSON DUNN (July 12, 2018), https://www.gibsondunn.com/california-consumer-privacy-act-of-2018 [https://perma.cc/VY3A-7UAH]. However, in the months since the passing of the CCPA, several other states have been working to enact similar laws to the CCPA within their own borders.

the GDPR does not equate to automatic compliance with the CCPA.

II. THE POTENTIAL SHORTCOMINGS OF THE CCPA

A. POTENTIAL PITFALLS OF THE CCPA

The CCPA has been closely analyzed since 2018 and will continue to be scrutinized once it takes effect in 2020. As discussed, the California State Legislature has already passed two sets of amendments, which were signed into law in September 2018 and October 2019, respectively.[124] Lawmakers should also consider the following issues noted in this Part.

1. The Constitutionality of the CCPA

In its current state, the constitutionality of the CCPA remains unclear, and there are several aspects of the law that have the potential to be challenged.

i. First Amendment

First, there is a question as to whether the current version of the CCPA violates the First Amendment of the United States Constitution.[125] Commercial speech that is regulated based on its content must directly advance a substantial governmental interest and must be drawn to achieve that interest.[126] In 2011, in *Sorrell v. IMS Health Inc.*, the Supreme Court held that a Vermont law violated the First Amendment because it permitted prescriber-identifying information to be purchased and used for certain types of speech, but prohibited pharmaceutical companies from using such information in their marketing practices.[127] The Court found that this amounted to a content-based restriction because the information could be used for other purposes, such as healthcare research and educational communications.[128] The legislators had intended to limit "detailing," a marketing practice in which pharmaceutical representatives promote the "details" of the products to doctors in person.[129] Pharmaceutical companies would lease reports containing prescriber-identifying information from data miners, who purchased the information from pharmacies, to determine which doctors would be likely to prescribe their drugs to patients.[130] The Court

124. *See* Caplan, *supra* note 63; Ramos, *supra* note 65.
125. *See, e.g.*, GOLDMAN, *supra* note 58, at 7.
126. Sorrell v. IMS Health Inc., 564 U.S. 552, 572 (2011).
127. *Id.* at 557.
128. *Id.* at 559–60, 564.
129. *Id.* at 557–58.
130. *Id.* at 558.

agreed that "[t]he capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy," but held that Vermont could not engage in content-based discrimination to promote its own side of the debate.[131] Based on the outcome of *Sorrell*, it is possible that a court may conclude that the CCPA also imposes a content-based restriction on speech. The CCPA mandates that companies notify consumers of the sale of their personal information to third parties and provide consumers with the opportunity to opt out of the sale.[132] The law exempts third parties from coverage if they agree to process the personal information only for the purposes indicated by the company and do not sell the information themselves.[133] Although the law is broader than the Vermont statute in *Sorrell*, which specifically targeted marketing practices, the CCPA does include these third-party exemptions, which could lead a court to find that the law imposes an unconstitutional content-based restriction on speech.[134] The CCPA also discusses that part of the impetus for the law was the Cambridge Analytica's Facebook data scandal.[135] This could lead a court to conclude that like in *Sorrell*, in which the law targeted the pharmaceutical companies' marketing practices, the CCPA is targeting a particular type of data-collection practice that amounts to a content-based restriction on speech.[136] As a result, it is possible that the law may be challenged on First Amendment grounds if the legislature does not address the issue in any future amendments.

The First Amendment is also implicated because CCPA's provides consumers the right to request that a business delete any personal information that the business has collected from the consumer.[137] This right is sometimes referred to as "the right to be forgotten."[138] The right to be forgotten has typically not been recognized in the United States due to its

131. *Id.* at 579–80; Peter Pizzi, *Possible Defects in California's New Privacy Law*, LAW360 (July 30, 2018, 2:31 PM), https://www.law360.com/articles/1067951?scroll=1 [https://perma.cc/CG84-87MV].

132. CAL. CIV. CODE §§ 1798.115(a), 1798.120(a) (West 2019); Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional*, TECH. & MARKETING L. BLOG (July 9, 2018), https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm [https://perma.cc/FC5J-DCQX].

133. Kosseff, *supra* note 132.

134. *Id.*

135. CAL. CIV. CODE § 2(g).

136. Kosseff, *supra* note 132.

137. CAL. CIV. CODE § 1798.105(a).

138. Grant Davis-Denny & Nefi Acosta, *What to Remember About Calif.'s Right to be Forgotten*, LAW360 (Nov. 6, 2018, 1:43 PM), https://www.law360.com/articles/1098471/what-to-remember-about-calif-s-right-to-be-forgotten [https://perma.cc/NHZ6-2TS8].

contradiction of First Amendment principles.[139] For example, forcing a website owner to remove material from the internet would generally be considered compelled speech that is not permitted under the First Amendment.[140] The legislature likely anticipated such First Amendment challenges, as they included a provision that says businesses do not need to comply with consumers' requests for deletion of their personal information if it would be necessary to maintain the information in order to exercise free speech or another right provided for by law.[141] However, this provision does not provide any further clarity as to what kind of speech would be protected and can be preserved, and what kind of speech would be unprotected and must be deleted at the request of a consumer.[142] This uncertainty could lead companies to be overly cautious and delete more information than is necessary to avoid any civil penalty resulting from the law, even if that means unknowingly deleting protected speech.[143] The legislature should consider amending the provision to include clarifying information as to what would qualify as protected speech. Otherwise, it would be unsurprising if litigation arises from this ambiguity once the law takes effect.

ii. Dormant Commerce Clause

In addition to First Amendment concerns, the CCPA may also pose issues related to the Commerce Clause of the United States Constitution, which grants Congress the power "to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[144] The idea of the Dormant Commerce Clause arose from Chief Justice Marshall's opinion in *Gibbons v. Ogden*,[145] and courts have since inferred that the Dormant Commerce Clause prohibits state laws from discriminating against or excessively burdening interstate commerce.[146] Under *Pike v. Bruce Church*, a state law that only incidentally affects interstate commerce will violate the Dormant Commerce Clause only if "the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[147] Despite this high standard, it is possible that the CCPA conflicts with the Dormant Commerce Clause. As other states begin to follow California's lead

139. David L. Hudson Jr., *Right to Be Forgotten*, FIRST AMEND. ENCYCLOPEDIA, https://mtsu.edu/first-amendment/article/1562/right-to-be-forgotten [https://perma.cc/85EN-EEXY].

140. *Id.*

141. CAL. CIV. CODE § 1798.105(d)(4).

142. Davis-Denny & Acosta, *supra* note 138.

143. *Id.*

144. U.S. CONST. art. I, § 8, cl. 3.

145. Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1 (1824).

146. Pizzi, *supra* note 131.

147. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970); *see also* Kosseff, *supra* note 132.

and enact similar data-privacy statutes (and at least several have begun the process of doing so[148]), it is likely that these laws will not be identical to the CCPA. This would mean that there would be slightly different laws on the books, which would demand disparate levels of compliance from companies that collect and process data from consumers in each state. Different states potentially imposing different data collection practices may arguably excessively burden interstate commerce because compliance with these laws would require substantial operational changes and companies would need to expend large sums of money to meet the laws' requirements.[149] Even if no other states had adopted data protection laws, if a business primarily collects data from consumers outside of California but does enough business in the state to require that it comply with the CCPA, it would likely need to make extensive changes to its current practices to ensure compliance with the CCPA.[150] Given that California is home to over forty million people and boasts the fifth largest economy in the world, many businesses will fall into this category.[151] The burden of requiring an overhaul of current data processing and storage procedures in order for a company to comply with the law of a state to which it has only a tenuous connection may arguably unduly burden participation in interstate commerce.[152] Therefore, it is possible that Dormant Commerce Clause challenges will arise with respect to the CCPA, and such challenges will likely be difficult to overcome.

2. Other Challenged Provisions of the CCPA

In addition to any aspects of the law that may violate the Constitution, there are other problematic aspects of the law that should be addressed. Some of these challenges include ambiguities in various provisions of the statute, the broad scope of the law, and the costs that companies will bear in order to comply with the law.

One reason the law has received backlash is that the Act was hurriedly drafted given the brief window of time that the California State Legislature had to pass the law to avoid it being presented on the November 2018

148. *See, e.g.*, Sabrina Hudson, *Nevada's Online Privacy Law Takes Effect, Offers More Control of Info*, L.V. REV.-J. (Sept. 30, 2019, 7:49 PM), https://www.reviewjournal.com/business/nevadas-online-privacy-law-takes-effect-offers-more-control-of-info-1860566 [https://perma.cc/JE6K-QLNQ].

149. Kosseff, *supra* note 132; Pizzi, *supra* note 131.

150. *See* Pizzi, *supra* note 131.

151. Jason Priebe & John Tomaszewski, *The California Consumer Privacy Act of 2018: What Businesses Need to Know Now*, JD SUPRA (Feb. 13, 2019), https://www.jdsupra.com/legalnews/the-california-consumer-privacy-act-of-32632 [https://perma.cc/93YB-BJ47].

152. Pizzi, *supra* note 131.

ballot.[153] In many instances, it is not thoroughly clear what the drafters intended to convey.[154] One such area of ambiguity, relates to the right to be forgotten. Although the drafters included a provision noting that a company will not be required to comply with a request to delete a consumer's personal information if the information is necessary for the business to maintain the information for any number of reasons, including the exercise of free speech, it is not yet clear exactly how much flexibility businesses will have when responding to requests to be forgotten, which might either lead businesses to be overly cautious and delete more than they need to, or result in litigation.[155] Additionally, the law does not allow businesses to discriminate against a consumer for exercising his or her rights under the law, meaning they cannot charge lower rates to customers who allow the business to collect and share their information.[156] However, the law also permits companies to offer financial incentives to consumers who do allow them to collect personal information, which implies that companies *are* allowed to charge disparate rates to those who take advantage of their rights under the law.[157] Lawmakers should address these and other ambiguous provisions by either adding clarifying language or providing specific examples that would more clearly represent what they intended to convey.

Additionally, although the GDPR is generally thought to be stricter than the CCPA, the CCPA has been challenged as being overbroad in some areas that exceed the GDPR's breadth. For example, the definition of "personal information" is wider under the CCPA than the GDPR.[158] As discussed previously in Part I of this Note, the original definition of personal information under the law was information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[159] Critics of the law argued that the definition was "so sweeping as to be meaningless" and proposed that the definition should not include information that "relates to or could be associated with a consumer" but just information that is linked or could reasonably be linked to a specific individual.[160] In 2019, Governor

153. Davis-Denny et al., *supra* note 23.

154. *Id.*

155. CAL. CIV. CODE § 1798.105(d)(1)–(9) (West 2019).

156. *Id.* § 1798.125 (a)(1).

157. *Id.* § 1798.125(b); Pizzi, *supra* note 131.

158. Jim Halpert & Andrew A. Kingman, *California Privacy Law Poised to Alter US Privacy Landscape*, DLA PIPER (June 28, 2018), https://www.dlapiper.com/en/us/insights/publications/2018/06/california-privacy-law-poised-to-alter-us-privacy-landscape [https://perma.cc/CTT2-LL4L].

159. CAL. CIV. CODE § 1798.140(o)(1).

160. Allison Grande, *Business Groups Take Up Fight to Amend Calif. Privacy Law*, LAW 360 (Aug. 10, 2018), https://www.law360.com/articles/1072336/business-groups-take-up-fight-to-amend-calif-

Newsom signed an amendment into law that narrowed the definition of "personal information" in accordance with critics' requests by including a "reasonableness qualifier, meaning that the law will now only apply to personal information that is *reasonably* capable of being associated with a California consumer or household."[161] Although this was a win for critics of the law's breadth, the definition of "personal information" is still very broad and could be subject to further challenges.[162] One can also anticipate disputes regarding the scope of the reasonableness qualifier,[163] which could require additional clarifying language by the legislature.[164]

One other area of controversy is the costs that accompany compliance with the law. According to the California Attorney General's regulatory impact assessment report, initial costs for CCPA compliance are projected to reach $55 billion.[165] The CCPA is likely to affect more than five-hundred thousand companies in the United States that collect and sell California residents' personal information.[166] In order to comply with the law, many companies will be required to overhaul their current practices and will need to devote significant resources to reengineering consumer interfaces.[167] Despite the CCPA limiting the number of companies that must comply with the law by implementing certain thresholds, as discussed in Part I of this Note, many small businesses will still be required to comply with the law, and these businesses have fewer resources to devote to compliance than large companies do.[168] Additionally, as other states enact similar laws, companies will devote even more money to comply with a patchwork system of laws

privacy-law [https://perma.cc/Y3YJ-TSUJ].

161. Chase Wright, *California Governor Signs CCPA Amendments Ahead of 2020 Effective Date*, JD SUPRA (Oct. 16, 2019), https://www.jdsupra.com/legalnews/california-governor-signs-ccpa-31226 [https://perma.cc/NRM9-7WFR].

162. Alexander Bilus et al., *CCPA Amendments and Draft Regulations Provide Some Clarity, Some Uncertainty, and Numerous Compliance Obligations*, JD SUPRA (Oct. 18, 2019), https://www.jdsupra.com/legalnews/ccpa-amendments-and-draft-regulations-51077 [https://perma.cc/SSD3-UFE3].

163. Wright, *supra* note 161.

164. *See* Monder "Mike" Khoury, *Uncertainty Remains in Key Provisions and Rules of California Consumer Privacy* Act, DAVIS WRIGHT TREMAINE LLP (June 27, 2019), https://www.dwt.com/blogs/privacy--security-law-blog/2019/06/uncertainty-remains-in-key-provisions-and-rules-of [https://perma.cc/9RT7-ZDK7]; *AB-874 California Consumer Privacy Act of* 2018, CAL. LEGIS. INFO., http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200AB874 [https://perma.cc/ZPG2-QHP5].

165. Jennifer M. Oliver, *CCPA Changes Sent to Governor's Desk as January Effective Date Draws Closer and Compliance Costs Loom Large*, NAT'L L. REV. (Oct. 10, 2019), https://www.natlawreview.com/article/ccpa-changes-sent-to-governor-s-desk-january-effective-date-draws-closer-and [https://perma.cc/TTX5-X935].

166. Grande, *supra* note 24.

167. Grande, *supra* note 61.

168. Kosseff, *supra* note 132.

with differing requirements.[169] While it is inevitable that companies will need to spend a large amount of money to comply with the CCPA, the legislature should consider a way to ease the burden on smaller companies that are subject to the law's jurisdiction but do not have the ample resources that technology giants like Google have to devote to data protection efforts.[170]

III. FEDERAL PREEMPTION AND THE FUTURE OF DATA PRIVACY LEGISLATION IN THE UNITED STATES

A. NEXT STEPS: TOWARD A NATIONAL STANDARD?

As discussed, the CCPA's passage has been controversial and many reactions have not been positive. However, in the wake of the GDPR's success and of mounting data breach scandals, the law is garnering more support.[171] In November 2018, Marriott announced that the personal information of up to five-hundred million of its guests had been compromised, one of the largest data breaches in history.[172] Under the CCPA, the company would receive fines if it had improperly handled the customers' data, and customers would have the right to inquire about what data the company had collected and was storing.[173] Companies often choose to implement inadequate data security and shoulder the burden of a data breach, but the exorbitant fines imposed by the law would incentivize companies like Marriott to invest in better data security practices.[174]

Further, it is clear that the emphasis on data privacy is being embraced around the globe.[175] Jurisdictions around the world are enacting legislation to conform to the EU's GDPR, due both to the law's extraterritorial application and the other countries' recognition of the importance of data privacy.[176] In addition to the EU Member States, the EFTA countries—

169. *Id.*

170. *Id.*

171. *See* John M. Simpson, *Massive Marriott Data Breach Shows Need for California Consumer Privacy Act*, CONSUMER WATCHDOG (Nov. 30, 2018, 11:18 AM), https://www.consumerwatchdog.org/privacy-technology/massive-marriott-data-breach-shows-need-california-consumer-privacy-act [https://perma.cc/MB33-ZSN4].

172. Sam Dean, *Marriott Data Breach Exposes Up to 500 Million Guests' Personal Information*, L.A. TIMES (Nov. 30, 2018, 5:35 PM), https://www.latimes.com/business/la-fi-marriott-data-20181130-story.html [https://perma.cc/4PXW-85BL].

173. Simpson, supra note 171.

174. *Id.*

175. *See* Rustad & Koenig, *supra* note 14, at 432.

176. *See id.* at 431–52.

Iceland, Lichtenstein, and Norway—have all agreed to adopt the GDPR.[177] Also, many Asian countries have been adapting to the GDPR.[178] For example, the EU announced a safe harbor agreement with Japan, indicating that the EU approved of Japan's data protection laws.[179] India has been working to bring itself closer to compliance with the GDPR's level of data protection.[180] A small number of Middle Eastern Companies have proposed GDPR-like data privacy laws, with Israel offering its citizens the most advanced protection in the region.[181] Australia and New Zealand have advanced data privacy laws and Australia is updating its laws to comply with the GDPR.[182] In South America, Argentina and Uruguay are the countries that are closest to compliance with the GDPR.[183] Moreover, other countries have adopted their own independent data security laws, some of which predate the GDPR, like South Africa's Protection of Personal Information Act of 2013, which includes a number of similarities to the GDPR.[184] The GDPR is developing into "the transnational gold standard of data protection" and it is time for the United States to decide whether it too will adopt this standard.[185] California's adoption of the CCPA has led several other states to introduce their own data privacy laws, and the federal government is currently grappling with whether and how to step in with a federal law addressing the United States' stance on GDPR-like data privacy.[186]

The passage of the CCPA has sparked debate among privacy advocates and large technology companies about whether the United States should adopt a national standard.[187] Since it has been anticipated that other states would follow California's lead and pass laws similar to the CCPA, large technology companies are concerned about having to comply with a patchwork system of laws, which will likely be more expensive and burdensome than compliance with one state's standard.[188] As a result, several technology companies have said they would embrace a federal

177. *Id*. at 441–42.
178. *Id*. at 434–35.
179. *See id*. at 435.
180. *See id*. at 436.
181. *Id*. at 442–43.
182. *Id*. at 444–45.
183. *Id*. at 445.
184. *Id*. at 432–33.
185. *Id*. at 453.
186. *Id*. at 405.
187. Lindsey O'Donnell, *Privacy Regulation Could Be a Test for States' Rights*, THREATPOST (Oct. 16, 2018, 10:45 AM), https://threatpost.com/privacy-regulation-could-be-a-test-for-states-rights/138303 [https://perma.cc/8EBK-CYRP].
188. *Id*.

privacy law, and representatives from Amazon, Google, Twitter, AT&T, and Charter have said they would help develop a uniform privacy law.[189] One caveat is that most of these companies would oppose a law as strict as the GDPR, and privacy advocates argue that these companies may merely want to preempt laws like the CCPA and set a diluted standard that is far more lenient than California's.[190] Privacy advocates are opposed to this approach and have said that they will resist attempts to enact a watered-down federal law that preempts any state laws.[191] One surprising ally of the privacy advocates given his position at the helm of a massive tech company, is Apple's CEO, Tim Cook, who has commended the EU's successful implementation of the GDPR and has said that Apple would support a comprehensive federal privacy law similar to the GDPR.[192] In support of that goal, Apple has developed a privacy portal which gives its users the ability to see what data Apple is collecting from them and to request that the company delete it.[193]

How likely is it that the federal government will indeed step in? Thus far, the United States has resisted comprehensive data privacy laws, instead opting for a smattering of sector-specific laws.[194] Due to gridlock in Washington, the likelihood of Congress passing an all-encompassing national standard has been unclear.[195] The Obama administration attempted to introduce a Consumer Privacy Bill of Rights, but it was met with strong opposition and eventually lost momentum.[196] The Trump Administration has thus far declined to proceed with a national cyber policy and has resisted pressure from the EU to enact GDPR-like policies.[197] Additionally, under Trump's administration, the Federal Trade Commission ("FTC") does not recognize the right to be forgotten, opposing one of the central tenets of the GDPR and the CCPA.[198] Given the current Administration's stance on these issues, it seems unlikely that the federal government will implement a

189. Kochman, *supra* note 49.

190. *Id.*

191. *Id.*

192. Chris Baraniuk, *Tim Cook Blasts 'Weaponisation' of Personal Data and Praises GDPR*, BBC (Oct. 24, 2018), https://www.bbc.com/news/technology-45963935 [https://perma.cc/8TP5-4ZMW].

193. Jerry Bowles, *'GDPR-US' Is Needed, Says Apple's Tim Cook as He Blasts "Data Industrial Complex"*, DIGINOMICA (Oct. 24, 2018), https://diginomica.com/2018/10/25/gdpr-us-is-needed-says-apples-tim-cook-as-he-blasts-data-industrial-complex [https://perma.cc/SJ2D-3BL3].

194. Lily Li, *American Privacy Laws in a Global Context: Predictions for 2018*, ORANGE COUNTY LAW., May 2018, at 31, 31.

195. *Id.* at 32.

196. *Id.*

197. Rustad & Koenig, *supra* note 14, at 453.

198. *Id.*

national standard during Trump's term, and if it does, it is likely to be much more lenient than the GDPR and the CCPA.

Despite Congress's unsuccessful efforts to address data privacy in the past, the enactment of the GDPR and the CCPA has caused a resurgence of interest in the issue. First, in December 2018, two senators released draft data privacy bills intended to stimulate discussion on the topic.[199] In February 2019, both the House and the Senate held committee hearings to jumpstart the legislative process for federal privacy legislation.[200] On February 26, 2019, the House Energy and Commerce Committee's Subcommittee on Consumer Protection and Commerce held a hearing entitled "Protecting Consumer Privacy in the Era of Big Data."[201] During the hearing, both witnesses and subcommittee members expressed support for some kind of federal privacy legislation due to the desire to protect consumers and create uniform standards with which companies can comply.[202] Witnesses and subcommittee members raised several of the common concerns about GDPR and CCPA-like laws raised earlier in this Note, including the compliance issues that arise when each state enacts its own unique version of the law, warnings regarding possible violations of the Dormant Commerce Clause, and concerns related to the compliance costs that small businesses may be less equipped to absorb than large companies.[203] On the topic of costs, Roslyn Layton, one of the witnesses from the American Enterprise Institute, claimed that since the GDPR came into law, Google, Facebook, and Amazon have increased their market share in the EU, whereas smaller businesses have suffered.[204] Dave Grimaldi, another witness from the Interactive Advertising Bureau, noted that in addition to harming smaller businesses, consumers have also been harmed by losing access to certain resources such as the Chicago Tribune and other publishers who have decided to no longer offer their services to consumers in Europe rather than adjust their practices to

199. Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, BROOKINGS: TECHTANK (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation [https://perma.cc/F4DT-Y7U5].

200. Jonathan G. Cedarbaum et al., *Congressional Committees Hold Hearings on Federal Privacy Legislation*, WILMERHALE (Mar. 1, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20190301-congressional-committees-hold-hearings-on-federal-privacy-legislation [https://perma.cc/JL7G-RA5K].

201. *Id.*

202. *Id.*

203. *Id.*

204. Allison Grande, *EU Privacy Law Not Good Model for US, House Panel Told*, LAW360 (Feb. 26, 2019, 10:31 PM), https://www.law360.com/articles/1132937/eu-privacy-law-not-good-model-for-us-house-panel-told [https://perma.cc/2RZE-KP6K].

comply with the law.[205]

The Senate Committee on Commerce, Science, and Transportation held a hearing on February 27, 2019, entitled "Policy Principles for a Federal Data Privacy Framework in the United States." Participants in this hearing also diverged on the proper approach to data privacy legislation.[206] The Senate hearing saw less discussion of the impact on smaller businesses than the House hearing did, but one senator did suggest that the GDPR had discouraged investment in start-up companies, and a number of the participants mentioned creating some sort of exception for smaller businesses in any federal law that is passed.[207] Additionally, almost all the panelists in the question-and-answer portion of the hearing represented that they favored federal preemption of state laws.[208] Many of these hearing participants and others support preemption because without it, passing a federal data privacy law would just be giving companies yet another law with which to comply.[209] Some argue that any federal standard should not preempt state laws but serve as a minimum level of compliance, allowing states to pass their own stronger laws, like the CCPA.[210] This appears to be the most realistic way of enacting a national standard in the short term because of drastically differing viewpoints and the division of party lines on this issue. However, this means that a patchwork system of laws imposing different requirements for compliance would be inevitable and would do nothing to address this major concern that critics have raised regarding state data privacy laws. It would seemingly be much simpler to adopt a national standard that parallels the GDPR since many companies in the United States must comply with GDPR anyway, however, due to strong opposition from major tech companies and the current Administration's disinterest in prioritizing this issue, it is doubtful that such a standard will be adopted in the near future. In the months following the February hearings, negotiations have halted.[211] Lawmakers allegedly reached a stalemate over whether citizens should have a private right of action against companies for data

205. *Id.*

206. Cedarbaum et al., *supra* note 200.

207. *Id.*

208. *Id.*

209. Allison Grande, *What to Watch as Congress Mulls Federal Privacy Legislation*, LAW360 (Feb. 25, 2019, 9:44 PM), https://www.law360.com/articles/1132337/what-to-watch-as-congress-mulls-federal-privacy-legislation [https://perma.cc/A8W8-GDVR].

210. Grande, *supra* note 93.

211. Kiran Stacey, *Senate Talks on US Data Privacy Law Grind to a Halt*, FIN. TIMES (June 11, 2019), https://www.ft.com/content/ecbc11d0-8bad-11e9-a24d-b42f641eca37 [https://perma.cc/7DC9-TZLJ].

breaches.[212] It remains to be seen whether these discussions in Congress will lead to federal data privacy legislation, but given what seems to be a trend toward GDPR principles in the United States, and considering the extra complications involved with a patchwork system of laws, the United States ultimately should adopt a federal standard that offers consumers similar protections as the GDPR and the CCPA. This would eliminate the issue of complying with a patchwork system as well as potential Dormant Commerce Clause challenges of state laws.

States, on the other hand, will likely have an easier time passing data privacy laws than the federal government, due to states' populations being more united and their legislative processes being less complex than the federal government's.[213] According to one commentator on the issue, "It's not a question of if states are going to enact their own privacy rules; it's a question of which state and when."[214] As of early 2019, Hawaii, Maryland, Massachusetts, New Mexico, and Rhode Island had proposed privacy bills modeled on the CCPA, and Illinois, New Jersey, New York, Oregon, Virginia, and Washington had introduced other data privacy bills not modeled on the CCPA.[215] By the middle of 2019, bills addressing various aspects of data privacy had been introduced in at least twenty-five states, including Nevada, whose data privacy law came into effect on October 1, 2019, prior to the CCPA.[216] However, not all states have been as successful as California and Nevada in passing their proposed laws. Washington and Texas had introduced bills similar to the CCPA in 2019, but neither were passed.[217] Further, the New York Legislature failed to pass the New York Privacy Act, which was considered to be more expansive than the CCPA due in part to its greater impact on smaller businesses.[218] Despite these setbacks,

212. *Id.*

213. O'Donnell, *supra* note 187.

214. Grande, *supra* note 209 (quoting Morrison & Foerster LLP partner Nathan Taylor).

215. Cedarbaum et al., *supra* note 200.

216. Hudson, *supra* note 148; 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/B7YU-5A44]; Davis Strauss et al., *What to Know About Updates to Nevada's Online Privacy Law*, LAW360 (May 30, 2019, 3:41 PM), https://www.law360.com/articles/1164320/what-to-know-about-updates-to-nevada-s-online-privacy-law [https://perma.cc/B2DT-59K9].

217. Jeewon Kim Serrato & Susan Ross, *Nevada, New York and Other States Follow California's CCPA*, NORTON ROSE FULBRIGHT: DATA PROTECTION REP. (Oct. 14, 2019), https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa [https://perma.cc/EN4R-CBAM].

218. Tim Sandle, *New York Lawmakers Reject Data Privacy Act in Surprise Turn*, DIGITAL J. (July 22, 2019), http://www.digitaljournal.com/tech-and-science/technology/new-york-lawmakers-reject-data-privacy-act-in-surprise-turn/article/554461 [https://perma.cc/32RR-6GF8].

the conversation surrounding data privacy in these states is unlikely to subside.

State legislators will likely continue working to protect their residents' data privacy regardless of whether or not Congress decides to take a national stance.[219] Thus, the patchwork system of laws seems inevitable, and, in a world without federal preemption, will require companies to keep track of the laws in each state and likely develop different methods of compliance for each state.[220] The question is, how feasible would it actually be to comply with a patchwork system? Ever since California first introduced breach notification laws in 2003, companies have had to confront a patchwork system of laws, as the breach notification requirements spread to every other state in the United States, but the patchwork system of data privacy laws could be more difficult for companies to comply with as they would "broadly apply to nearly every aspect of their day-to-day business operations."[221] Whether the patchwork system is feasible may also depend on how similar or dissimilar each state's laws are from one another. If the states follow the pattern of the data breach notification laws and each enact their own data privacy laws, there will likely be enough discrepancies among the laws that compliance with all of them will be complex. One route companies could possibly take to ease the burden of compliance would be to comply with the most stringent law in order to be compliant with all the laws. However, to know whether this is practicable will require reviewing each of the laws once they are passed. Ultimately, the fate of data privacy as either a patchwork system or a national standard remains to be seen, but the passage of the GDPR and the CCPA has ensured that the discussions surrounding data privacy in the U.S. will not die down any time soon.

CONCLUSION

Ultimately, the issue of what kind of standard the United States will adopt cannot yet be answered. Until now, attempts to pass a federal data privacy law have not succeeded.[222] But with the passage of the GDPR and the CCPA, many companies that typically have been opposed to such efforts have come out in support of a unified standard in lieu of having to comply with different privacy laws in multiple states.[223] It remains to be seen whether Congress will be able to come together and formulate a national data

219. *See* Grande, *supra* note 209.
220. *See id.*
221. *Id.*
222. *See id.*
223. *Id.*

privacy standard, as well as whether such a standard would serve as a base level from which states can build or as a watered-down law that would preempt the CCPA and other similar state laws. Until Congress decides to take action, states already have begun and will continue to follow California's lead by enacting laws similar to the CCPA.

On a related note, the CCPA is an imperfect statute, so the California State Legislature should work to make the law as clear as possible and address its major issues, including potential constitutionality challenges. Ultimately, the United States should be following the EU and many other countries' leads toward a standard similar to the GDPR; the CCPA is a positive step in this direction. Despite the fact that the law is still in flux, businesses will need to begin implementing new procedures to ensure compliance with the law when it does take effect, so they should familiarize themselves with the current version of the law, monitor the passage of any amendments, and adjust their current practices to comply with the most updated version of the law.