Science and Technology Law Review

Volume 23 | Number 2 Article 7

2020

The California Consumer Privacy Act's Potential Incompatibility with the United States' Legal and Economic Landscape

Alexandra Henry
Southern Methodist University, Dedman School of Law, ashenry@smu.edu

The California Consumer Privacy Act's Potential Incompatibility with the United States' Legal and Economic Landscape

*Alexandra Henry**

I. INTRODUCTION

Data privacy and security concerns are a persistent trend that continues to worry American consumers.[1] The United States currently has no comprehensive federal law that regulates how businesses use personal data, but individual states are starting to create their own laws to solve the issue of consumers' concerns about their personal data.[2] The California Consumer Privacy Act (CCPA) is a new state consumer data privacy law that addresses its consumers' concerns about their personal information, while offering the most stringent data privacy protection for its residents in the United States.[3] The most important and ground-breaking part of this law is that consumers will have control of the way their personal information is used, and they can even request to have their information deleted, which is a right also seen in the European Union's General Data Protection Regulation (GDPR).[4]

The CCPA's main objective is to give consumers control over their personal information by increasing their data privacy rights.[5] However, it is important to consider whether these rights under the CCPA are realistically

---

* Alexandra Henry is a 2021 candidate for Juris Doctorate from SMU-Dedman School of Law. She received a Bachelor of Business Administration from Southern Methodist University in 2017.

1. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

2. Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley–And Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

3. Daphne Leprince-Ringuet, *What is the CCPA? Everything You Need to Know About the California Consumer Privacy Act Right Now*, ZDNET (Dec. 20, 2019, 2:43 PM), https://www.zdnet.com/article/california-consumer-privacy-act-everything-you-need-to-know-about-the-ccpa/.

4. Letter from the Info. Tech. and Innovation Found. to Att'y Gen. Xavier Becerra (Mar. 8, 2019), http://www2.itif.org/2019-comments-ccpa.pdf; *Right to Erasure*, INFO. COMM'RS OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (last visited Mar. 3, 2021).

5. *California Consumer Privacy Act Fact Sheet*, CAL. DEP'T JUST., OFF. ATT'Y GEN., https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last visited Mar. 3, 2021).

achievable to comport with America's current "patchwork of data privacy laws."[6] It is also important to consider how the CCPA would be compatible with the way that America's current economy operates. Some companies may not be able to realistically adhere to the CCPA's requirements due to smaller businesses being unable to afford the high costs associated with compliance with the law.[7] The CCPA will also have a significant economic impact on the United States, as businesses located outside of California will also have to follow the requirements of this new law if they fall under the CCPA.[8] Moreover, the CCPA may face constitutional issues under the Dormant Commerce Clause, the First Amendment, the Void for Vagueness doctrine, and the Supremacy Clause. The CCPA will challenge all types of businesses, especially major technology companies and smaller businesses, before it can truly be effective in protecting consumers' data privacy in California and throughout the United States.

II. BACKGROUND OF THE CALIFORNIA CONSUMER PRIVACY ACT

The CCPA was passed in California due to growing concerns about consumers' protection of personal information. The CCPA was passed in 2018 and went into effect on January 1, 2020.[9] Enforcement of this new law began on July 1, 2020.[10] California consumers will receive new rights under this law, including (1) the right to know what information companies are using or collecting about them; (2) the right to ask businesses to delete their personal information; (3) the right to "opt-out of the sale of personal information"; and (4) the right to not be discriminated by businesses on the basis of service or price when they exercise a privacy right.[11] There are also specific rules within the law regarding the right to opt-out of the sale of personal information that apply to minors.[12] Consumers younger than the age of sixteen are required to provide opt-in consent for the sale of personal information, and

6. Courtney Reigel, *2020 Update: Data Privacy Laws in the United States*, GAVIN L. OFF. (Jan. 28, 2020), https://www.gavinlawoffices.com/2020/01/2020-update-data-privacy-laws-in-the-united-states/.

7. Aly McDevitt, *CCPA Compliance Costs Projected to Reach $55B*, COMPLIANCE WK. (Jan. 10, 2020), https://www.complianceweek.com/data-privacy/ccpa-compliance-costs-projected-to-reach-55b/27847.article.

8. *Id.*

9. *California Consumer Privacy Act Fact Sheet*, *supra* note 5.

10. *Private and Public CCPA Enforcement Will Launch on January 1, 2020, Despite California AG Delay*, COOLEY (Dec. 20, 2019), https://cdp.cooley.com/private-and-public-ccpa-enforcement-will-launch-on-january-1-2020-despite-california-ag-delay/.

11. *California Consumer Privacy Act Fact Sheet*, *supra* note 5.

12. *Id.*

consumers under the age of thirteen must have a parent or guardian provide the opt-in consent for the sale of personal information.[13]

The CCPA also applies to certain businesses located both in California and outside of California.[14] The CCPA will apply to any for-profit business that "has gross annual revenues in excess of $25 million; buys, receives or sells the personal information of 50,000 or more consumers, households, or devices," or "derives 50 percent or more of annual revenues from selling consumers' personal information."[15] The CCPA also introduces new obligations that businesses must follow if they fall under the three thresholds.[16] Businesses will be required to provide notice to consumers "before data collection" occurs.[17] Businesses will also have to respond to consumer requests who want to "know, delete, and opt-out" of personal data collection within a specific timeframe.[18] Businesses will be required to verify the identity of consumers making requests about their personal information to ensure that the correct person is being informed about the use or deletion of their personal information.[19]

The CCPA only protects Californian consumers' personal information, but the broad definition of personal information has been a major issue in the rulemaking process.[20] Personal information is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household."[21] Categories of information that constitute personal information under the CCPA, include: (1) personal identifiers; (2) commercial information; (3) Internet or network activity information; (4) geolocation data; (5) biometric information; (6) professional or employment-related information; (7) education information; and (8) audio, electronic, visual, thermal, olfactory, or similar information.[22] Personally identifiable information includes information such as a "real name, alias, postal address, unique personal identifier, IP address, email address, account name, social security

13. *Id.*

14. Armistead Whitney, *Cybersecurity Response to the California Consumer Privacy Act*, SEC. MAG. (Mar. 5, 2020), https://www.securitymagazine.com/articles/91847-cybersecurity-response-to-the-california-consumer-privacy-act.

15. *California Consumer Privacy Act Fact Sheet*, *supra* note 5.

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. Sara H. Jodka, *California's Data Privacy Law: What It Is and How to Comply (A Step-By-Step Guide)*, DICKINSON WRIGHT (July 12, 2018), https://www.dickinson-wright.com/news-alerts/californias-data-privacy-law.

22. *Id.*

number, driver's license number, passport number, or other similar identifiers."[23] Commercial information includes "records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies."[24] Internet and electronic network activity information includes "browsing history, search history, and information regarding a California resident's interaction with an internet web site, application, or advertisement."[25] The broad way that personal information is defined in the statute is important for the constitutional "void for vagueness" doctrine that is later discussed in this Comment.

Multiple revisions of the CCPA have already occurred after the CCPA went into effect on January 1, 2020. On February 7, 2020, the California Attorney General issued additional revisions to the CCPA.[26] The recent revisions to the CCPA attempt to provide clarity to vague definitions and provisions in previous versions of the CCPA.[27] One of the revisions explains that data must "relate to a particular consumer" in order to constitute personal information under the CCPA.[28] The revisions also impose additional obligations on businesses that collect consumers' information through mobile applications, requiring businesses to provide notice to consumers when it does so.[29] The revisions to the CCPA also state how service providers can use consumer information "they obtain from businesses in the course of providing their services" by listing acceptable uses of that information.[30] Service providers can use consumer information when they "combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity."[31]

On March 13, 2020, the California Attorney General proposed additional revisions to the CCPA, including information about the disclosure of sensitive data in responding to consumers requests to know what information

23. *Id.*

24. *Id.*

25. *Id.*

26. Kirk J. Nahra & Ali A. Jessani, *California Attorney General Publishes Revisions to Proposed Regulations*, WILMER HALE (Feb. 11, 2020), https://www.wilmerhale.com/en/insights/client-alerts/20200211-california-attorney-general-publishes-revisions-to-proposed-ccpa-regulations.

27. *Id.*

28. *Id.*

29. CAL. CODE REGS. tit. 11, § 999.305(a)(4) (2020).

30. Nahra & Jessani, *supra* note 26.

31. CAL. CODE REGS. tit. 11, § 999.314(c) (proposed Feb. 7, 2020).

is being collected about them.[32] The proposed revision stated that "where a business collects sensitive data and withholds that data in responding to a request to know what information the business is holding about a consumer, that business must now provide a description of the information with sufficient particularity."[33] The revised version of the CCPA explains this idea by saying that if a company that has personal information about a consumer, such as a fingerprint, the company would only have to say that it collects "unique biometric data including a fingerprint scan," and it would not have to disclose the actual image of the fingerprint.[34] The CCPA will likely continue to go through this notice and comment procedure multiple times before it becomes enforceable in July 2020.[35] While the California Attorney General has proposed multiple revisions of the CCPA in an attempt to clarify vague definitions and modify certain provisions, businesses may still be unclear if they violate the law and consumers may be unsure if they receive protections until the law has completed the rule-making process.[36]

III. THE CCPA COMPARED TO OTHER STATE CONSUMER PROTECTION LAWS IN THE UNITED STATES

While the Federal Trade Commission (FTC) protects consumers' data privacy rights at the federal level, the FTC does not have the authority to monitor companies' compliance of these rights, so regulation of these data privacy rights remains with the individual states.[37] While the states all have similar purposes with their data privacy laws, some inconsistencies are present in the various state data privacy laws.[38] The CCPA is the most recent data privacy regulation to capture the attention of other states, and it could potentially become the consumer privacy standard in the United States, with

32. Susan Kohn Ross & Timothy M. Carter, *CCPA: More Regulatory Changes Proposed*, NAT'L L. REV. (Mar. 13, 2020), https://www.natlawreview.com/article/ccpa-more-regulatory-changes-proposed.

33. *Id.*

34. *Id.*

35. *About the Regular Rulemaking Process*, CAL. OFF. ADMIN. L., https://oal.ca.gov/rulemaking_participation/ (last visited Mar. 3, 2021).

36. *California Attorney General Finalizes CCPA Regulations*, COVINGTON (June 22, 2020), https://www.cov.com/en/news-and-insights/insights/2020/06/california-attorney-general-finalizes-ccpa-regulations.

37. Ryan Brooks, *U.S. Data Privacy Laws: State-Level Approaches to Privacy Protection*, NETWRIX (Aug. 27, 2019), https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/.

38. *Id.*

other states, including New York, Massachusetts, and Nevada, already creating similar consumer data privacy laws.[39]

The New York Consumer Privacy Act (NYPA) is still pending in the state senate, but is very similar to the CCPA, as it gives individual control over their personal information, with the ability to "request that the business correct or delete the data, and opt out of having their data shared with or sold to third parties" in addition to what personal data the business has about the consumer.[40] The NYPA has a similar extraterritorial effect and reach that the CCPA has, with the NYPA applying to "legal entities that conduct business in New York" or that "intentionally target" residents of New York with their products or services."[41] However, the NYPA differs from the CCPA because it does not contain a revenue threshold for businesses to comply with it.[42] The main difference between the NYPA and the CCPA is that the NYPA requires companies to "put their own customer's privacy rights before their own profits," imposing fiduciary duties on companies to comply with the NYPA.[43]

The current Massachusetts data privacy law, also known as the "Standards for the Protection of Personal Information of Residents of the Commonwealth," has been in effect since 2010.[44] The data privacy act requires that "that every person or business owning or licensing personal information regarding a resident of Massachusetts is required to develop, implement and maintain a comprehensive information security program."[45]

The Nevada Privacy Law took effect on October 1, 2019.[46] Nevada's data privacy law differs from the CCPA because it "applies to online businesses that purposefully direct their activities at Nevada residents," whereas the CCPA applies to any "online and offline business that touches a Califor-

39. *U.S. Cybersecurity and Data Privacy Outlook and Review-2020*, GIBSON DUNN (Jan. 17, 2020), https://www.gibsondunn.com/wp-content/uploads/2020/01/us-cybersecurity-and-data-privacy-outlook-and-review-2020.pdf.

40. Brooks, *supra* note 37.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. Mark Keppler, *The Massachusetts Data Protection Act: Tightening Up Individual State Data Privacy Laws*, I.S. PARTNERS (May 21, 2019), https://www.ispartnersllc.com/blog/what-is-massac.husetts-data-protection-act/.

46. *Following California's Lead, Nevada Privacy Law Gives Consumers Right to Opt Out*, COOLEY (June 18, 2019), https://www.cooley.com/news/insight/2019/2019-06-18-nevada-privacy-law-gives-consumers-right-to-opt-out.

nia resident's data."[47] The Nevada Privacy Law does not afford consumers the rights of access, deletion, portability, or non-discrimination while the CCPA provides all of these rights to its consumers.[48] Another major difference between these two data privacy laws is that the Nevada Privacy Law does not give consumers a private right of action, while the CCPA gives its consumers a limited private right of action for certain types of data breaches.[49] In addition to Nevada, Massachusetts, and New York, other states have started to either update their current consumer data protection laws or create new consumer data protection laws.[50]

IV. SUPPORT FOR A FEDERAL PRIVACY LAW MAY INHIBIT THE CCPA'S EFFECTIVENESS

While state data privacy laws help protect consumers' information in each individual state, legal executives also support the creation of a federal data privacy law.[51] Executives and attorneys at large technology companies such as Google, Amazon, and AT&T have "voiced support for a federal privacy law."[52] Various bills about consumer data privacy have been introduced in 2019, demonstrating the federal legislature's intentions to eventually create a comprehensive federal data privacy law.[53] The Social Media Privacy Protection and Consumer Rights Act "would require online platforms, such as public websites, web applications, mobile applications, social networks, ad networks, mobile operating systems" to obtain opt-in consent from consumers.[54] The "Digital Accountability and Transparency to Advance Privacy Act" would have a similar purpose to the CCPA, requiring companies "to

47. Allison Schiff, *California Isn't The Only State Getting Busy With New Privacy Laws*, ADEXCHANGER (Sept. 11, 2019), https://www.adexchanger.com/privacy/california-isnt-the-only-state-getting-busy-with-new-privacy-laws/.

48. *The Nevada Privacy Law (SB-220) vs. The California Consumer Privacy Act (CCPA)*, ONETRUST (Sept. 17, 2019), https://www.onetrust.com/the-nevada-privacy-law-sb-220-vs-the-california-consumer-privacy-act-ccpa/.

49. *Id.*

50. Schiff, *supra* note 47. Maine has a new consumer data privacy law targeting Internet Service Providers that will go into effect in July 2020. Pennsylvania's pending data privacy law is similar to the CCPA, with a lower threshold of $10 million in revenue for a company to violate it. *Id.*

51. Katie Branson, *Senate Commerce Committee Holds Hearing on Consumer Data Privacy*, EDUCAUSE (Oct. 22, 2018), https://er.educause.edu/blogs/2018/10/senate-commerce-committee-holds-hearing-on-consumer-data-privacy.

52. *Id.*

53. Katie Branson, *Federal Consumer Data Privacy Legislation in the 116th Congress*, EDUCAUSE (May 13, 2019), https://er.educause.edu/blogs/2019/5/federal-consumer-data-privacy-legislation-in-the-116th-congress.

54. *Id.*

notify and describe to consumers how data is collected, processed, stored, and disclosed" in addition to requiring companies to provide consumers "personal information collected upon request" and obtaining opt-in consent from consumers.[55] The Information Transparency and Personal Data Control Act would require "any entity collecting, storing, processing, selling, or sharing sensitive data . . . to receive opt-in consent from the consumer in order to collect and use such data."[56] Under this Act, companies would also have to "provide consumers with the identity and contact information of entities collecting, processing, selling, and sharing sensitive personal information, third parties involved, and the purpose, storage period, and specific information shared."[57] Although the above bills have not been reviewed in formal committees, they indicate the lawmakers' concerns and that "lawmakers are laying down markers to illustrate their priorities in the larger federal privacy legislation debate."[58]

In addition to the introduction of these various data privacy laws in 2019, the U.S. Government General Accountability Office (GAO) has suggested that Congress should create more federal protection for consumers' data privacy in America.[59] The GAO is an "independent, non-partisan agency" that is an "advisor to Congress and federal agencies" by providing "objective [and] reliable information" to help the federal government operate more efficiently.[60] The GAO recently issued a report where they "explored areas where lawmakers might consider reform" in the consumer data privacy industry.[61] In this report, the GAO analyzed FTC and Federal Communications Commission (FCC) internet privacy enforcement actions and interviewed executives and members from the data privacy industry and consumer advocacy groups to understand how these government agencies have "overseen consumers' Internet privacy."[62] The GAO also interviewed Internet-industry stakeholders, who stated that "an overarching Internet privacy statute could enhance consumer protection by clearly articulating to

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY (2019), https://www.gao.gov/assets/700/696437.pdf [hereinafter GAO-19-52].

60. Katie Branson, *GAO Recommends That Congress Consider Comprehensive Consumer Privacy Legislation*, EDUCAUSE (Mar. 12, 2019), https://er.educause.edu/blogs/2019/3/gao-recommends-that-congress-consider-comprehensive-consumer-privacy-legislation.

61. *Id.*

62. GAO-19-52, *supra* note 59.

consumers, industry [sic], and agencies what behaviors are prohibited."[63] A former FCC commissioner also stated that a federal privacy statute could "enhance Internet privacy oversight by creating uniform standards for all players in the Internet ecosystem that is focused on the consumer rather than the regulatory legacy of the companies involved."[64] Even Apple's CEO Tim Cook has supported the creation of a federal data privacy bill.[65] While the CCPA is one of the few state statutes to expand on data privacy protection for consumers, the GAO report shows that Internet industry stakeholders and agency leaders support the creation of a federal data privacy statute, which may end up replacing the CCPA.[66]

V. THE CCPA COMPARED TO THE GDPR

The CCPA and the EU's GDPR contain similar provisions and rights, with the CCPA giving consumers the right to have their data be deleted and the GDPR providing its citizens the right to be forgotten, also known as the "right to erasure."[67] Under the "right to erasure," consumers can request verbally or in writing to have their personal data be deleted, and companies would have one month to respond to these consumer requests.[68] The "right to erasure" is not absolute, and only applies to consumers in certain circumstances.[69] Consumers only have the right to request their data be deleted if:

> the data is no longer necessary; the processing was solely based on consent; the processing was based on the controller's legitimate interest, but that interest is outweighed by the data subject's rights; the data is being processed unlawfully; erasure is already required by law; [or] that data was collected from a child as part of offering an information society service.[70]

63. *Id.*

64. *Id.* at 31.

65. Zoe Schiffer, *'The Time is Now to Have a Federal Privacy Bill,' Says Tim Cook*, THE VERGE (Nov. 22, 2019, 3:10 PM), https://www.theverge.com/2019/11/22/20978140/tim-cook-apple-federal-privacy-bill-facebook-breakup-big-tech.

66. Branson, *supra* note 60.

67. *California Consumer Privacy Act (CCPA) Fact Sheet*, *supra* note 5; *Right to Erasure*, *supra* note 4.

68. *Right to Erasure*, *supra* note 4.

69. *Id.*

70. David Zetoony et al., *CCPA Privacy FAQs: Do the CCPA and the GDPR Have the Same Exceptions to the Right to be Forgotten?*, JD SUPRA (Aug. 16, 2019), https://www.jdsupra.com/legalnews/ccpa-privacy-faqs-do-the-ccpa-and-the-54983/.

While the "right to erasure" has certain limitations, under the CCPA, consumers can request to have their data be deleted, "regardless of the purpose for which the data was originally collected."[71] Other differences between the CCPA and the GDPR's right to be forgotten include the extent of the right to delete information.[72] Under the CCPA, businesses may have to delete information if it is taken directly from the consumer.[73] If a business obtained information about a consumer from a third party, or is able to "develop the information from its own experiences with the consumer," then the information may not have to be deleted "pursuant to a deletion request" under the CCPA.[74] However, the GDPR has stricter requirements for its right to be forgotten. Under the GDPR, a business would have to comply with a consumer's request to have their data deleted, even if that information is obtained through a third party or is developed using its "information from its own experiences with the consumer."[75]

Businesses that function as data center managers may have more complicated issues with a consumer's right to have their data be deleted under the CCPA and a consumer's right to be forgotten under the GDPR.[76] Data center manager companies are businesses that provide "data center services, data storage, and backups" of consumer information for other companies.[77] A data center manager company called Iron Mountain is based in Boston, Massachusetts, and would not normally be subject to another state's data privacy law because most of its business is "only indirectly relevant" by providing the infrastructure for the data and it lacks access to the actual data itself.[78] However, because it has employees located in California and it provides its services to individuals, Iron Mountain is subject to the CCPA.[79] These data center manager companies may also be required to delete information for individual customers or records, which typically is done through applications that access the data.[80] However, under the CCPA, consumer requests to have their data deleted "may come outside of traditional channels, require deletion across multiple systems, and at a scale too large to handle through existing

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

76. Maria Korolov, *CCPA and GDPR: The Data Center Pitfalls of the 'Right to Be Forgotten,'* IT PRO TODAY (Feb. 5, 2020), https://www.itprotoday.com/data-privacy/ccpa-and-gdpr-data-center-pitfalls-right-be-forgotten.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

processes."[81] The CCPA and GDPR also differ in many ways. The GDPR applies to any "business, organization, or institution that collects, processes, or operates on the data of people located in the European Union."[82] The CCPA only applies to for-profit businesses that deal with Californian consumers and have "gross annual revenues in excess of $25 million; buys, receives or sells the personal information of 50,000 or more consumers, households, or devices" or "derives 50 percent or more of annual revenues from selling consumers' personal information."[83] But both data privacy laws have extraterritorial effects, as businesses located outside of the EU are subject to the GDPR and businesses located outside of California can be subject to the CCPA.[84]

The GDPR and the CCPA also differ in their scope of who they protect.[85] The GDPR protects a larger group of people because it protects anyone's personal data in the EU while the CCPA only protects Californian consumers' data.[86] While both the GDPR and the CCPA provide civil penalties against businesses who violate the data privacy laws, the GDPR imposes higher fines on companies compared to the CCPA.[87] Civil penalties under the GDPR can go up _20,000,000, or four percent of annual global revenue for the company, whichever is higher.[88] Under the CCPA, a maximum amount of a civil penalty is $2,500.00 per violation, or $7,500.00 for each intentional violation.[89] Businesses are subject to civil penalties under the CCPA if they "fail to 'cure' any alleged violation within 30 days of receiving a noncompliance notice."[90] The GDPR also covers the processing of all personal data, while the CCPA only protects consumer data.[91] The CCPA excludes certain categories of information, such as medical information and financial information because they are covered by other data privacy laws such as the

81. *Id.*

82. Casey Crane, *CCPA v. GDPR: What You Need to Know About These Data Privacy Laws*, HASHED OUT (Nov. 6, 2019), https://www.thesslstore.com/blog/ccpa-vs-gdpr-what-you-need-to-know-about-these-data-privacy-laws.

83. *California Consumer Privacy Act Fact Sheet*, *supra* note 5.

84. Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, PRACTICAL L., https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf (last visited Mar. 3, 2021).

85. DataGuidance & Future of Privacy Forum, *Comparing Privacy Laws: GDPR v. CCPA*, FUTURE OF PRIVACY FORUM 7, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (last visited Mar. 3, 2021).

86. Crane, *supra* note 82.

87. *Id.*

88. Jehl & Friel, *supra* note 84.

89. Crane, *supra* note 82.

90. *Id.*

91. DataGuidance & Future of Privacy Forum, *supra* note 85, at 11.

Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act.[92]

VI. POTENTIAL VERIFICATION ISSUES FOR CONSUMER REQUESTS FOR INFORMATION

An issue that the CCPA will face that the GDPR has also confronted is requiring consumers to give companies more personal information to delete their information that they have as a part of the identity-verification process.[93] Companies in the EU have faced problems with hackers taking advantage of the GDPR provision that allows consumers to receive the data that companies held about its consumers.[94] Hackers would impersonate the consumers to steal the consumer's personal information from the company.[95] After the GDPR went into effect, a hacker was able to gain access to a technology executive's Spotify account and filed a data request through the website.[96] Through this data retrieval process that was intended to help consumers feel safer about retrieving their personal data, the hacker was able to retrieve the technology executive's personal information, including their home address and credit card information.[97] Californian legislators saw this problem with hackers that the GDPR faced and have implemented a more thorough identity-verification process in the CCPA to ensure that the correct consumer was getting their own information, not hackers.[98] Legislators created Article 3 of the text of the proposed regulations of the CCPA, which is devoted to issues with "business practices for handling consumer requests."[99] Article 3 lays out the requirements that businesses must follow for verifying consumers' identities when they request to know or request to delete their personal information.[100] The CCPA states that a business's compliance with the CCPA includes complying with consumer "request[s] to know categories of personal information."[101] Companies would be required to "verify the identity of the consumer making the request to a reasonable degree of certainty . . . [which] may include matching at least two data points provided by

92. *Id.* at 11–12.

93. Kashmir Hill, *Want Your Personal Data? Hand Over More Please*, N.Y. TIMES (Jan. 15, 2020), https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html.

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. CAL. CODE REGS. tit. 11 §§ 999.312–18 (2020).

100. *Id.*

101. *Id.* § 999.325.

the consumer with data points maintained by the business" under Section 999.312 of the CCPA.[102]

Through this verification process, companies are still requiring consumers to give more personal information to retrieve their personal information, which goes against the CCPA's purpose of securing consumers' personal data.[103] Companies are requiring photographs, such as selfies and government IDs, to verify the user's identity before sending the consumer their personal information.[104] This necessary but cumbersome verification process may turn into a never-ending cycle of providing information just to recover your own personal information.[105] Berbix and Wirewheel are companies considered to be third-party "privacy software platform[s]" that businesses use to comply with the CCPA.[106] These "privacy software platform[s]" require consumers to provide additional personal identification information, such as the front and back of a driver's license and a selfie to ensure the consumer's identity for the information request.[107] However, these "privacy software platforms" are exempt from the CCPA because they qualify as service providers under the CCPA.[108] These "privacy software platforms" perform their identity-verification services for businesses by using a third-party software company to process and verify consumers' personal data, a process that seems to spread consumers' personal information even farther out of their reach before they can retrieve their personal information.[109]

Although "privacy software platforms" like Wirewheel claim that the third-party service providers they use, such as Idology, keep consumer's personal data and images encrypted, the Subject Rights Request Notice on Wirewheel's website explicitly states that the consumer personal data is encrypted "as long as they are kept within the platform."[110] Therefore, if a consumer's selfie or driver's license information is somehow not kept within the platform, consumers are not actually maintaining control of their personal information.[111] Companies would be handling even more personal informa-

102. *Id.*

103. Hill, *supra* note 93.

104. *Id.*

105. *Id.*

106. Alistairr Barr, *Come On a Trip Into the New Privacy Circle of Hell*, BLOOMBERG (Jan. 9, 2020, 5:45 AM), https://www.bloomberg.com/news/newsletters/2020-01-09/come-on-a-trip-into-the-new-privacy-circle-of-hell; Hill, *supra* note 93.

107. Barr, *supra* note 106.

108. *Id.*

109. *Subject Rights Request Notice*, WIREWHEEL, https://wirewheel.io/subject-rights-request-notice/ (last updated Dec. 31, 2019).

110. *Id.*

111. Barr, *supra* note 106.

tion, such as consumer's photographs or drivers licenses, in order to verify less sensitive information, which is counterintuitive to the core concept of protecting consumer data privacy.[112] While companies seem to have a plan to comply with the identity-verification requirements from the CCPA through using "privacy software platforms," the extensive chain of technology and third-party software companies involved in the identity-verification process make it possible for mistakes to be made, especially with the these processes being relatively new as a part of complying with the CCPA.[113]

VII. CONSTITUTIONAL IMPLICATIONS OF THE CCPA

Several legal scholars have noticed "constitutional vulnerabilities" in the CCPA.[114] Legal scholars have considered whether the CCPA's "cross-border implications violate the [D]ormant [C]ommerce [C]lause" and whether the CCPA's definition of "personal information" is constitutionally void due to its vagueness.[115] Issues may also arise under the First Amendment due to CCPA imposing content-based restrictions on speech in data.[116]

A. The CCPA May Be Invalid Under the Dormant Commerce Clause

The CCPA would likely face scrutiny under the Dormant Commerce Clause due to the burdens that the CCPA imposes on businesses through interstate commerce.[117] The CCPA does not directly discriminate against out-of-state businesses, but it does indirectly impose burdens of compliance on certain out-of-state businesses if they meet certain threshold standards stated in the CCPA.[118] The CCPA containing regulations that make it more difficult for out-of-state companies to do business with residents of California may

112. *Id.*

113. *Id.*

114. Aluya Zeltzer Hutnik et al., *Potential Constitutional Challenges to the CCPA*, AD L. ACCESS (Dec. 12, 2019), https://www.adlawaccess.com/2019/12/articles/potential-constitutional-challenges-to-the-ccpa/.

115. *Id.*

116. Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law Is Unworkable, Burdensome, and Possibly Unconstitutional*, TECH. & MKTG. 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.

117. *Id.*

118. Jennifer Huddleston, *Should Congress Be Concerned About California's Data Privacy Law?*, THE HILL (Dec. 3, 2019, 4:30 PM), https://thehill.com/opinion/technology/472834-should-congress-be-concerned-about-californias-data-privacy-law.

violate the Dormant Commerce Clause.[119] The Dormant Commerce Clause is inferred from Article I of the Constitution, which holds that "state and local laws may not unduly burden commerce between the states, and thereby preventing states from regulating beyond their borders."[120] The Dormant Commerce Clause could invalidate the CCPA if legislators conclude that it is a discriminatory law and they conduct an analysis under the *Pike v. Bruce Church* balancing test.[121]

The first method of determining if a law is following the Dormant Commerce Clause is determining whether the law discriminates against out-of-state businesses.[122] Under the doctrine of extraterritoriality, legislators could argue that the CCPA is "seeking to regulate activity that takes place entirely outside the borders of California."[123] In the data privacy context, an example of this question would be "does a consumer privacy law treat data obtained or processed by in-state companies differently than that from out-of-state companies?"[124] If a consumer privacy law were to treat in-state businesses differently from out-of-state businesses, it would be a violation of the Dormant Commerce Clause.[125] Because the CCPA imposes the same compliance requirements for both businesses operating in California and businesses in other states, the CCPA is not facially discriminatory against interstate commerce.[126]

However, even if a law does not explicitly demonstrate preference to in-state companies, "it may still have a discriminatory impact on out-of-state parties," such as out-of-state small businesses.[127] The extraterritorial nature of the transmission and use of data via the Internet creates problems for the CCPA under the Dormant Commerce Clause.[128] Because data is commonly

119. Andrew O'Sullivan, *Are California's New Data Privacy Controls Even Legal?*, REASON (Dec. 17, 2019, 8:35 AM), https://reason.com/2019/12/17/are-californias-new-data-privacy-controls-even-legal/.

120. Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, REGUL. TRANSPARENCY PROJECT 6 (Dec. 2, 2019), https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf.

121. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

122. Huddleston & Adams, *supra* note 120, at 3.

123. Cynthia J. Cole & Neil Coulson, *Patchwork of US Data Privacy Laws: A Complicated and Preemptive Local Landscape*, BAKER BOTTS 3 (Sept. 18, 2018), https://www.bakerbotts.com/insights/publications/2018/09/patchwork-of-us-data-privacy-laws.

124. Huddleston & Adams, *supra* note 120, at 7.

125. *Id.*

126. Huddleston, *supra* note 118.

127. Huddleston & Adams, *supra* note 120, at 7.

128. *Id.*

transmitted by businesses and between states through the Internet, the CCPA will likely affect businesses outside of California.[129] It will be difficult for businesses outside of California to accurately determine how many of its online consumers are California residents, and how many of those consumers visit their websites in one year, so businesses will still have to comply with the CCPA even if they only have a small number of California consumers.[130] However, geolocation technology may help businesses track their consumers more effectively, allowing businesses outside of California to overcome the CCPA's extraterritorial influence on out-of-state businesses.[131] By using geolocation technology when collecting consumers' data, businesses can pinpoint the location of each consumer when they visit a website or complete a transaction with a business via a website.[132] The precision provided by geolocation technology may help businesses located outside of California avoid compliance requirements with the CCPA, but it may be costly for certain companies, such as smaller businesses, to be able to use that technology.[133]

The second way a law could be invalid under the Dormant Commerce Clause is to consider whether the "in-state benefits of the law outweigh the burden on the out-of-state parties" in interstate commerce.[134] In *Pike v. Bruce Church*, the Supreme Court created this balancing test by holding that a law that "regulates even-handedly to effectuate a legitimate local public interest, and if its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[135] The legitimate interest that the CCPA is intending to serve is the protection of Californian consumers' rights to data privacy.[136] The issue that arises under the CCPA and the *Pike* test is whether Californian citizens' right to data privacy is more important than the burden of compliance imposed on all other states that engage in online commerce with consumers.[137]

The CCPA will likely require businesses that engage in online commerce to comply with the law due to a company's ability to precisely track the location of every online consumer through using geolocation technol-

129. Cole & Coulson, *supra* note 123.

130. *Id.* at 4.

131. *Id.*

132. *Id.*

133. *Id.*

134. Huddleston & Adams, *supra* note 120, at 7.

135. Cole & Coulson, *supra* note 123, at 4; Pike v. Bruce Church, Inc., 397 U.S. 137, 143 (1970).

136. Cole & Coulson, *supra* note 123, at 4.

137. *Id.*

ogy.[138] Legal scholars argue that this burden of compliance imposed by the CCPA does not provide a significant amount of data protection for its consumers, claiming that the only new significant protection that the CCPA provides is the right for consumers to demand the deletion of their personal data.[139] It is likely that the CCPA could be invalidated under the *Pike* test in the future, due to the high burden of the cost of compliance that the CCPA imposes on out-of-state businesses and the minor legitimate interests that serve Californian consumers.[140]

B. Void for Vagueness

Failing to properly define the term "personal information" in the CCPA may be an issue under the void for vagueness doctrine.[141] Legal experts and data privacy consultants are particularly concerned about vague definitions of important terms and "mechanism descriptions regarding how firms should collect and share data," making it difficult to comply with the CCPA.[142] A statute is "void for vagueness if it fails to give a person of ordinary intelligence fair notice that his or her contemplated conduct is forbidden by statute."[143] Under the CCPA, "personal information" is defined as 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."[144] The definition of "personal information" is vague and unclear, along with other terms in the CCPA such as "business," "third party," "sale," and "aggregate consumer information."[145] These terms could be subject to the "void for vagueness" doctrine because they impose "materially different obligations, restrictions, and liability exposure if a company misinterprets these vague terms."[146] An amendment to the CCPA, Amendment AB 874, has clarified the definition of personal information by stating that "personal information does not include de-identified or aggregated consumer information."[147]

138. *Id.*

139. *Id.*

140. *Id.* at 5.

141. Hutnik et al., *supra* note 114.

142. Sam Sabin, *Companies Know California Privacy Law Goes Into Effect by Jan. 1, but Little Else*, Morning Consult (Aug. 21, 2019, 11:31 AM), https://morningconsult.com/2019/08/21/companies-know-california-privacy-law-goes-into-effect-by-jan-1-but-little-else/.

143. Hutnik et al., *supra* note 114.

144. *Id.*

145. *Id.*

146. *Id.*

147. Whitney, *supra* note 14.

The California Attorney General's office recently issued changes called "Modified Regulations" to the CCPA on February 7, 2020.[148] The "Modified Regulations" have revised terms such as "categories of sources," "categories of third parties," and "household[s]," which are included in the definition of personal information in Section 999.301.[149] Section 999.301 of the Modified Regulations has narrowed the definition of a "household" under the definition of personal information, redefining a "household" as a "person or group of people who (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."[150] Section 999.301 of the Modified Regulations has also added new terms in the CCPA regulation including "employment benefits," "employment-related information," "signed," and "value of consumer's data."[151]

The Modified Regulations also includes Section 999.302, which provides guidance for interpreting the definitions included in the legislation, particularly the definition of "personal information."[152] Section 999.302 helps explain the restrictions imposed on the broad definition of "personal information."[153] Section 999.302 states that whether certain information constitutes "personal information" depends on "whether the business maintains information in a manner that 'identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.'"[154] Section 999.302 also provides an example of when a website is not collecting personal information under the CCPA, which is helpful for businesses like website analytic providers to know if they fall under the CCPA.[155]

Although these "Modified Regulations" provide some clarity on what constitutes personal information by providing guidance for interpreting the definition and providing additional information, the definition of personal information may still be ambiguous to businesses and to the average consumer, who is the primary target of this law.[156]

148. Kate Black & Gretchen A. Ramos, *OAG Imposes Significant Changes to CCPA Regulations*, NAT'L L. REV. (Feb. 11, 2020), https://www.natlawreview.com/article/oag-proposes-significant-changes-to-ccpa-regulations.

149. *Id.*

150. CAL. CODE REGS. tit. 11, § 999.301 (2020).

151. Nahra & Jessani, *supra* note 26.

152. CAL. CODE REGS. tit. 11, § 999.302 (proposed Feb. 7, 2020).

153. *Id.*

154. *Id.*

155. Nahra & Jessani, *supra* note 26.

156. *Id.*

C. The CCPA Raises Issues with the First Amendment

Data protection laws such as the CCPA might place content-based restrictions on free expression by "treating data differently depending on how it is used."[157] Because the CCPA can restrict the flow of certain information through data, it is important to consider the First Amendment and make sure that the CCPA is not an unconstitutional restriction on speech.[158] Various standards of review apply to different types of speech under the First Amendment.[159] The strict scrutiny standard typically applies to political or ideological speech while commercial speech receives intermediate scrutiny, a lower standard of review.[160] Content-based restrictions on speech typically receive strict scrutiny review.[161] A content-based law "discriminates against speech based on the substance of what it communicates" while a content-neutral law "applies to expression without regard to its substance."[162] Content-neutral laws can be constitutional if they overcome intermediate scrutiny.[163] The government can place restrictions on speech "relating to its time, manner, and place so long as it is narrowly tailored [and] content neutral."[164] Laws that are content-based restrictions are "presumptively unconstitutional" because they "limit speech based on its subject matter."[165] The Supreme Court's holding in *Sorrell v. IMS Health* indicates that there may be additional constitutional issues with the CCPA because sales restrictions in the CCPA may constitute content-based restrictions.[166] In *Sorrell*, the Supreme Court held that a Vermont statute violated the First Amendment "by restricting the sale or disclosure of records of a doctor's prescription habits for mar-

157. Jennifer Huddleston, *State Data Privacy Laws May Well Be Unconstitutional*, THE BRIDGE (Dec. 9, 2019), https://www.mercatus.org/bridge/commentary/state-data-privacy-laws-may-well-be-unconstitutional.

158. *Id.*

159. *Will the CCPA and Other State Privacy Laws Face Constitutional Attack?*, METAVERSE L. (Sept. 5, 2019), https://www.metaverselaw.com/privacylaws/.

160. *Id.*

161. David L. Hudson, Jr., *Content Based*, FIRST AMENDMENT ENCYCLOPEDIA, https://www.mtsu.edu/first-amendment/article/935/content-based (last visited Mar. 3, 2021).

162. *Id.*

163. *Id.*

164. Huddleston & Adams, *supra* note 120, at 9.

165. Hudson, *supra* note 161.

166. Mike Masnick, *Yes, Privacy Is Important, But California's New Privacy Bill Is an Unmitigated Disaster in the Making*, TECHDIRT (July 9, 2018, 10: 44 AM), https://www.techdirt.com/articles/20180708/00485140195/yes-privacy-is-important-californias-new-privacy-bill-is-unmitigated-disaster-making.shtml; *see* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2663 (2011).

keting purposes."[167] The Supreme Court held that the Vermont law was a "content-based restriction of commercial speech" because the law "prohibited the disclosure [of information] for marketing, but not for other purposes" and "prevented use of the information by pharmaceutical marketers, but permitted the transmission and use of the very same information by other kinds of speakers to counter pharmaceutical advertising."[168] The issue the CCPA might face is that its "distinction between [a] 'sale' and mere analytics or processing" of data could be perceived as a "similar content-based restriction."[169] The CCPA requires businesses "to notify consumers of the sale of their personal information to third parties," but the CCPA also exempts "'third parties' from coverage if they agree in a contract to process the personal information only for purposes specified by the company."[170]

Sorrell established that the "collection, dissemination, and use of personal data [. . .] is entitled to First Amendment Protection."[171] Just because the collection of personal data "comes from a commercial motivation does not strip it of its status of speech," so consumers' personal information that is collected and used under the CCPA receives First Amendment protection.[172]

D. Preemption Issues with Existing Federal Laws

Although there is not a comprehensive data privacy law for the entire country, there are several data privacy laws that cover certain industries, such as the financial and health industries, protecting categories of information.[173] The health industry has the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which "requires the protection and confidential handling of protected health information," and the financial services industry has the Gramm-Leach-Bliley Act to protect consumer information, which requires financial institutions to "ensure the security and confidentiality of cus-

167. Kosseff, *supra* note 116 (construing *Sorrell*, 131 S. Ct at 2653 (2011)).

168. Christopher Mohr, *Data Is Speech: The Constitution Has a Role in Informational Privacy II*, SOFTWARE & INFO. INDUS. ASS'N (Oct. 11, 2018), https://www.siia.net/blog/index/Post/76979/Data-is-Speech-The-Constitution-Has-a-Role-in-Informational-Privacy-II; *see id.*

169. Huddleston & Adams, *supra* note 120, at 10.

170. Kosseff, *supra* note 116.

171. Mohr, *supra* note 168.

172. *Id.*

173. *See generally Health Insurance Portability and Accountability Act*, DEP'T HEALTH CARE SERVS., https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx (last visited Mar. 3, 2021) (stating that an objective of HIPAA is to protect healthcare information); *see generally Privacy Issues Under Gramm-Leach-Bliley*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/consumers/consumer/alerts/glba.html (last visited Mar. 3, 2021) (summarizing privacy requirements for financial institutions in the Gramm-Leach-Bliley Act).

tomer information [. . .] and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer."[174] The CCPA has recognized the issue of potential conflicts with these laws, and has exempted its coverage from protection for information that is already covered by HIPAA and the Gramm-Leach-Bliley Act.[175] However, the Gramm-Leach Bliley Act only protects information in the context of "consumer financial products," so information about consumers that is obtained in the commercial financial context is not covered by the Gramm-Leach Bliley Act and is therefore subject to the CCPA.[176]

Internet industry executives and legislators have "called for a federal solution to fully preempt the CCPA."[177] Although there is not currently a general federal law that would preempt the CCPA, it appears that may happen with the support from industry executives and agencies like the GAO supporting the creation of a federal data privacy law.[178] For Congress to be able to preempt a state law, it would need to "enact a law that conflicts with the state law, expressly displaces the state law, or occupies the field of regulation 'so comprehensively' that there is no room for supplementary state legislation."[179] Although preemption is not currently an issue for the CCPA under the Supremacy Clause, it might become an issue that California legislators will have to consider when Congress creates a federal data privacy law that would conflict with the CCPA in the future.[180]

VIII. THE ECONOMIC IMPACT OF THE CCPA

The CCPA will have a major economic impact nationwide due to the way that businesses operate online. While the law will likely have the greatest impact on the technology sector due to prominent technology companies being headquartered in California, other nationwide businesses, including construction, retail, and healthcare industries, will also be affected by the

174. *Health Insurance Portability and Accountability Act*, *supra* note 173; *Privacy Issues Under Gramm-Leach-Bliley*, *supra* note 173.

175. Wilson C. Freeman, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, CONG. RSCH. SERV. 2 (Nov. 1, 2018), https://fas.org/sgp/crs/misc/LSB10213.pdf.

176. Anna Fridman, *What Financial Institutions Need to Know About the CCPA*, LAW.COM (Oct. 4, 2019, 11:55 AM), https://www.law.com/therecorder/2019/10/04/what-financial-institutions-need-to-know-about-the-ccpa/.

177. Freeman, *supra* note 175, at 4.

178. *See* GAO-19-52 (small caps needed despite use of capital letters and numbers), *supra* note 59, at 37.

179. Freeman, *supra* note 175, at 4.

180. *See id.*

CCPA.[181] The CCPA's extraterritorial effect on companies in the United States may create unintended consequences for smaller businesses and industries that may be unable to keep up with the cost of compliance and additional burdens imposed on them.[182]

A. The Extraterritorial Effect of the CCPA on Out-of-State Businesses

Because the CCPA may apply to any business outside of California if it "collects or sells California consumers['] personal information while conducting business in California and meet[s] one of the other quantitative thresholds," most companies outside of California could fall under the CCPA.[183] The CCPA applies to companies that do business in California, so the way that "doing business in California" is interpreted will determine if a company is subject to the CCPA.[184] The act of "doing business in California" includes "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit" according to the California Franchise Tax Board.[185] Companies located outside of California can also do business in California "whether or not the transaction is considered exclusively engaged in interstate commerce."[186] Companies located outside of California can be included in the scope of the CCPA by "collecting, selling or disclosing personal information of California residents," but it may be difficult for smaller companies to know if they fall under the CCPA if they are not aware how many of their online customers are from California.[187] It will be difficult for companies to know if their customers are California residents without asking for their personal information, which goes against the core principle of giving consumers more control of their personal data and minimizing the transmission of consumer data.[188] Because many companies use consumers' data without know-

181. *See* David Roland-Holst et al., *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, CAL. DEP'T JUST., OFF. ATT'Y GEN. 22, 29 (Aug. 2019), https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf (stating that CCPA will affect non-California businesses that provide goods and services to California customers and estimating compliance costs by sector).

182. *See id.*

183. DataGuidance & Future of Privacy Forum, *supra* note 85, at 8.

184. *Id.* at 8–9.

185. *Id.* at 9.

186. CAL. CODE REGS. tit. 18, § 23101 (defining "Doing Business").

187. DataGuidance & Future of Privacy Forum, *supra* note 85, at 9.

188. *See* Alison Divis, *How the CCPA Benefits Consumers and Business Owners*, PAC. DATA INTEGRATORS, https://www.pacificdataintegrators.com/insights/ccpa-benefits (last visited Mar. 3, 2021).

ing where they are from, they will likely "choose to comply with all state privacy laws regardless of the location of its customers" to cover its bases in case of inadvertently violating another state's data privacy law.[189] The extra-territorial nature of the type of activity covered by the CCPA creates problems for businesses located outside of California because they may be bearing additional costs of complying with this data privacy law when they may not be required to do so.[190] More clarity on what constitutes "doing business" in California in the context of the CCPA would help businesses outside of California determine if they fall under the CCPA.[191]

B. The High Cost of Compliance May Burden Smaller Businesses

The CCPA may negatively impact small businesses throughout America by taking away potential opportunities for growth from these companies by having such high compliance costs.[192] The estimated cost of compliance is $55 billion for 2020, with the cost to maintain a CCPA-compliant system to be approximately $16.5 billion throughout the next decade.[193] The size of a company will also affect its ability to comply with the CCPA.[194] It will be more difficult for smaller businesses to comply with the CCPA due to the high cost of compliance due to smaller businesses lacking the ability to pay the costs of compliance.[195] Larger corporations, like Google and Facebook, should easily be able to afford paying large amounts of money to comply with the CCPA, especially since they already comply with the GDPR and will not have to make as many adjustments in the data privacy sector of their

189. *Will the CCPA and Other State Privacy Laws Face Constitutional Attack?*, *supra* note 159.

190. *See id.*

191. *See* CAL. CODE REGS. tit. 18, § 23101 (defining "Doing Business"); *see also* DataGuidance & Future of Privacy Forum, *supra* note 85, at 8 (explaining the ambiguity of the "doing business" standard).

192. *See* Kosseff, *supra* note 116.

193. Huddleston & Adams, *supra* note 120, at 4; *see also* Roland-Holst et al., *supra* note 181, at 11 ("The total cost of initial compliance with the CCPA . . . is approximately $55 billion.").

194. *See* Huddleston & Adams, *supra* note 120, at 5; *see generally* Lisa Burden, *California Consumer Privacy Act (CCPA): What Small Businesses Need to Know*, ZENEFITS (Dec. 30, 2019), https://www.zenefits.com/workest/california-consumer-privacy-act-ccpa-what-small-businesses-need-to-know/ (explaining what businesses are subject to the CCPA).

195. *See* Huddleston & Adams, *supra* note 120, at 5; *see also* Roland-Holst et al., *supra* note 181, at 31 ("Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.").

business compared to smaller companies.[196] Smaller companies that are not equipped to handle the high compliance costs may also receive less attention from potential investors, which would restrict a company's ability to earn larger profits and build its capital for future growth.[197]

People might also be hesitant to become entrepreneurs and form small businesses due to fear of not being able to comply with the CCPA due to the extensive financial costs associated with the CCPA.[198] The CCPA may implicitly create barriers to entry for small businesses wanting to compete in larger industries, such as the technology industry.[199] Large technology corporations, like Facebook and Google, can afford to create "compliance infrastructure to address regulatory challenges" while smaller companies may struggle to keep up with these challenges.[200] Small businesses make up the majority of the U.S. economy, with approximately two-thirds of new jobs in America being created by small businesses.[201]

Smaller businesses will bear additional expenses along with the initial cost of complying with the CCPA. These expenses would include "secondary economic losses" in other areas of a business, such as advertising and marketing.[202] Advertising companies are particularly affected by the CCPA since the function of their business focuses on the use of online customer data to determine their target audience as a core part of their business.[203] The CCPA's definition of "personal information" is broad and now includes types of personal information that "specifically impact[s] advertising," including consumers' geolocation data, IP addresses, commercial information (which includes "records of products or services purchased"), and internet information (which can be an "interaction . . . with an advertisement").[204]

196. Antonio Garcia Martinez, *Why California's Privacy Law Won't Hurt Facebook or Google*, WIRED (Aug. 31, 2018, 8:00 AM), https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/.

197. Huddleston & Adams, *supra* note 120, at 5.

198. *See Will the CCPA and Other State Privacy Laws Face Constitutional Attack?*, *supra* note 159; *see generally id.* ("Newer and smaller players may struggle with increased barriers to entry from such requirements.").

199. *See* Huddleston & Adams, *supra* note 120, at 5.

200. *Id.*

201. Jason Dorè, *Small Businesses Generate 44 Percent of U.S. Economic Activity*, U.S. SMALL BUS. ADMIN. (Jan. 30, 2019), https://advocacy.sba.gov/2019/01/30/small-businesses-generate-44-percent-of-u-s-economic-activity/.

202. *See* Huddleston & Adams, *supra* note 120, at 5.

203. *See id.*

204. Michelle Tyde & John Brigagliano, *The Impact of the CCPA on Advertising,: What You Need to Know*, KILPATRICK TOWNSEND 2, https://www.kilpatricktownsend.com/-/media/2019/Advertising-Law-Guides-CCPA_10Takeaways_05-19_v3.ashx (last visited Mar. 3, 2021).

The expansive definition of "personal information" under the CCPA will substantially impact the digital marketing and advertising industry because the CCPA now protects information that was not previously "within the scope of personal information under U.S. state and federal laws."[205] Smaller advertising and digital marketing companies that cannot afford to comply with the CCPA through creating "system modifications" may have to cut off their Californian division of consumers entirely, which would have a negative effect on the smaller businesses in the advertising industry.[206]

C. Technology Companies Taking Advantage of the CCPA's Service Provider Exception

Some companies may be exempt from the CCPA due to the nature of their business as service providers.[207] Salesforce's Audience Studio has created a "suite of new tools for customers to manage CCPA compliance," which focuses on management of the consumer's rights to "delete my data," "give me a copy of my data," and "do not sell my personal information."[208] Because Salesforce is a service provider, it has certain obligations under the CCPA to offer these tools for its customers.[209] The CCPA defines a "service provider" as for-profit companies that have "a contractual relationship with a business to process consumer personal information for specific purposes . . . [and] the contract prohibits the service provider from processing or using the data in ways not outlined within the contract."[210] Businesses that are "service providers" are not considered to be a seller of:

> personal information under the law if the sharing of personal information is necessary to perform a business purpose, the business has provided notice that the information is being used or shared, and the service provider does not further collect, sell or use the

205. *Id.*

206. Ivan Guzenko, *How CCPA Will Impact the Word's Digital Economy*, FORBES (Oct. 31, 2019, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2019/10/31/how-ccpa-will-impact-the-worlds-digital-economy/#f38e62c69225.

207. *CCPA Service Provider Exception: Obligations, Vendor Contract Agreements and More*, CLARIP, https://www.clarip.com/data-privacy/service-providers-cali-privacy-act/ (last visited Mar. 3, 2021).

208. *California Consumer Privacy Act (CCPA)*, SALESFORCE, https://help.salesforce.com/articleView?id=mc_rn_december_2019_dmp_ccpa.htm&type=5 (last visited Mar. 3, 2021).

209. *See* Lisa Rapp, *CCPA Explained: What Are Businesses, Service Providers, and Third Parties?*, RAMPUP (Oct. 25, 2019), https://rampedup.us/ccpa-explained-businesses-service-providers-third-parties/.

210. *Id.*

> personal information of the consumer except as necessary to perform the business purpose.[211]

The core "business purpose" of a company will determine if that company is a service provider, which is what several major technology companies in the business of selling consumers' personal information want to redefine themselves as in order to avoid having to comply with the CCPA.[212] For the processing of personal data to be "considered a business purpose, the use of the personal information by a service provider must be reasonably necessary and proportionate to achieve the operational purpose for which the information was collected, processed, or a compatible purpose."[213]

Facebook and other advertising technology companies are attempting to redefine themselves as service providers under the CCPA so they will be exempt from complying with the law.[214] Large technology companies, such as Google and Facebook, have been negotiating with Californian legislators to allow segments of their company to qualify as service providers so they will not have to stop selling their consumers' personal information, which is one of the primary ways that these companies make profits.[215] Service providers are exempt from the CCPA because they "process data on behalf of businesses [. . .] and they don't sell consumer information."[216] The core function of certain technology companies, specifically Google and Facebook, is the exploitation and monetization of personal data.[217] Google and Facebook are a "duopoly that today controls more than half of the worldwide market in online advertising."[218] Social media companies, like Facebook, rely on consumer data such as "user demographics [and] location" to help businesses create targeted advertising as a part of their business model.[219] With Facebook's $17.7 billion third-quarter revenue from 2019 consisting of

211. *CCPA Service Provider Exception: Obligations, Vendor Contract Agreements and More*, *supra* note 207.

212. *See id.*

213. *Id.*

214. Barr, *supra* note 106.

215. *Tech Companies Seek to Avoid California Privacy Requests*, BLOOMBERG (Dec. 31, 2019, 10:03 AM), https://www.bloomberg.com/news/audio/2019-12-31/tech-companies-seek-to-avoid-california-privacy-requests-radio?cmpid=BBD010820_TECH&utm_medium=email&utm_source=newsletter&utm_term=200108&utm_campaign=tech.

216. *Id.*

217. *See* Confessore, *supra* note 2.

218. *Id.*

219. Queenie Wong, *CCPA: What California's New Privacy Law Means for Facebook, Twitter Users*, CNET (Jan. 3, 2020, 9:20 AM), https://www.cnet.com/news/ccpa-what-californias-new-privacy-law-means-for-facebook-twitter-users/.

mostly profits from advertising, Facebook likely does not want to give up access to its consumer's personal data.[220]

Facebook's platform for using consumer data for advertising and targeting consumers is called Pixel.[221] Facebook promotes Pixel as a "business-to-business ad service" that uses a "single invisible pixel" on a user's webpage "to deliver cookies to the end user's browser."[222] When the cookies are on the consumer's browser, they track the consumer's online behavior "beyond Facebook, basing a personal profile" based on the websites that the consumer visits.[223] Through Pixel, Facebook obtains valuable data about the consumer, such as "location, age, gender, and interests."[224] Facebook reportedly claims that it does not sell data that web trackers, such as Pixel collect, but that it "simply provides a service to businesses and websites that install Pixel on their sites."[225] Facebook believes their Pixel service is exempt from the CCPA as a service provider because businesses that use Pixel can "install Pixel free of charge, and pay only for Facebook to deliver targeted ads based on the information" they collect about consumers.[226] The main idea that Facebook claims makes Pixel exempt from the CCPA is because they are not "directly selling the personal data they collect" to businesses; thus, they are acting as service providers rather than as a typical business.[227] However, several legal experts disagree with Facebook's approach to the service provider exception, claiming that "Facebook also seems to use the data for its own purposes, separate from providing ad services, and can't rely on the service provider exception for those uses."[228] Another legal expert claimed that that "the transfer of personal data as part of the web tracking services would be regarded in the same way a sale would under the CCPA [. . .] so long as the company is deriving some sort of 'monetary or other valuable consideration' from it," which Facebook does derive a significant monetary benefit through its high advertising revenue.[229] Facebook's argument that it should be exempt

220. *See id.*

221. *See* Sara Morrison, *Facebook is Gearing Up for a Battle with California's New Data Privacy Law*, VOX (Dec. 17, 2019, 5:00 PM), https://www.vox.com/recode/2019/12/17/21024366/facebook-ccpa-pixel-web-tracker.

222. Scott Ikeda, *Facebook Refuses to Change Web Tracking Practices, Believes That CCPA Does Not Apply to Them*, CPO MAG. (Jan. 6, 2020), https://www.cpomagazine.com/data-protection/facebook-refuses-to-change-web-tracking-practices-believes-that-ccpa-does-not-apply-to-them/.

223. *Id.*

224. Morrison, *supra* note 221.

225. *Id.*

226. Ikeda, *supra* note 222.

227. *Id.*

228. Morrison, *supra* note 221.

229. Ikeda, *supra* note 222.

from the CCPA because it is a service provider will be one of the first major challenges that the CCPA will face.[230]

Large technology companies like Google and Facebook are not as worried about the CCPA because they have already adapted its businesses to comply with the GDPR, which is more stringent than the CCPA.[231] Smaller third-party companies that transfer data between consumers and companies will have larger financial and compliance burdens to bear with the CCPA than larger companies like Facebook or Google, because they have direct "first-party" relationships with its consumers.[232]

D. The CCPA May Help Companies Strengthen Consumer Relationships for Businesses

Some businesses would benefit from the CCPA, as consumers will want to engage with companies that protect their data, thereby earning loyalty and trust from consumers.[233] The CCPA will also force businesses to be more transparent with consumers in the way they use their data. Businesses will initiate "positive dialog" with its consumers when they inform them "that you want to use their data to better meet their needs."[234] The CCPA would also help companies optimize their business processes, which would increase the efficiency in the way they operate.[235] Businesses have to audit all of the data they have in order to comply with the CCPA, and by doing this, they will have a better understanding of the type of data they have and be able to

230. *See generally* Annie Gaus, *Facebook and Regulators Likely to Clash Over New Data Privacy Rules in California*, THE STREET (Jan. 16, 2020, 2:54 PM), https://www.thestreet.com/investing/facebook-regulators-clash-california-privacy-rules.

231. Nicole Lindsey, *Google, Other Tech Companies Trying to Dilute CCPA with AdTech Exemption*, CPO MAG. (Sept. 16, 2019), https://www.cpomagazine.com/data-protection/google-other-tech-companies-trying-to-dilute-ccpa-with-adtech-exemption/.

232. *See id.*

233. *See* Brenda Stoltz, *A New California Privacy Law Could Affect Every U.S. Business–Will You Be Ready?*, ALL BUS., https://www.allbusiness.com/the-ccpa-is-bound-to-impact-your-business-are-you-prepared-122654-1.html (last visited Mar. 3, 2021).

234. Brenda Stoltz, *Is Your Business Prepared for the California Consumer Privacy Act? Industry Experts Offer Advice*, FORBES (Sept. 20, 2019, 11:24 AM), https://www.forbes.com/sites/allbusiness/2019/12/20/california-consumer-privacy-act-business-preparation/#226fca545931.

235. *See* Ilia Sotnikov, *Why New Privacy Regulations Are a Business Enabler, Not an Enemy*, NETWRIX (Oct. 24, 2019), https://blog.netwrix.com/2019/10/24/why-new-privacy-regulations-are-a-business-enabler-not-an-enemy/.

improve internal data management strategies, increase efficiencies and save money.[236]

The CCPA gives consumers more control over their personal data by holding companies accountable for how they use or misuse consumers' data.[237] Consumers will likely feel more comfortable knowing that businesses will be more careful with their data because they could sue the businesses through the new private right of action under the CCPA.[238] Consumers will also feel more secure by having more control of their personal information, knowing that they have the right to opt-out of having their data being sold or that they have the right to know what information about them is being sold by businesses.[239] With all of these new rights and causes of action against businesses under the CCPA, consumers will feel more confident in interacting and sharing personal information with companies.[240] Consumers value companies that value their data privacy, and the CCPA will help facilitate and strengthen the relationships between consumers and businesses.[241]

IX. CONCLUSION

The CCPA has a strong influence on the United States' economic and legal landscape, with other states already creating similar laws and federal bills being considered. While the CCPA will benefit consumers by giving them control over their personal data, companies requiring them to give up more information just to get their information back may be an issue that businesses will have to deal with in the identity-verification process. The emergence of state legislation being created in response to the CCPA shows that the trend of consumer control of their personal data will continue throughout the country, which is a positive change in the Internet and data privacy landscape. However, lawmakers and technology executives' support for the creation of a federal data privacy law may create hindrances for the CCPA and other state data privacy laws to be effective. The CCPA has already created a wave of consumer data privacy laws at the state level and is likely to influence the creation of a federal consumer data privacy law in the future.

Although the CCPA is not explicitly discriminatory against interstate commerce, it does place an undue burden of compliance on other states, especially on smaller businesses that might not be able to afford to comply with

236. *Id.*

237. *See* Christina Hyun Jin Kroll, *CCPA: Consumers and the Right to Sue*, NAT'L L. REV. (June 2, 2019), https://www.natlawreview.com/article/ccpa-consumers-and-right-to-sue.

238. *Id.*

239. *See* Divis, *supra* note 188.

240. *See id.*

241. *See id.*

the CCPA. The CCPA also has a sweeping extraterritorial effect through its burden of compliance, likely affecting the way the majority of company's outside of California operate their businesses. While the CCPA is a step in the right direction for consumers' data privacy rights, especially giving consumers the right to control their personal information, the reality of smaller businesses throughout the country being able to comply with the CCPA will take time.