NORTH CAROLINA BANKING INSTITUTE

Volume 24 | Issue 1 Article 22

3-1-2020

The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation

Lauren Davis

The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation

I. INTRODUCTION

In order to gain a competitive advantage, companies have begun to leverage the personal information of consumers.[1] Consequently, a market for consumer data has emerged, causing many companies to reform their business models to properly capture the desired data.[2] By doing so, companies are often able to profit off the information obtained without the knowledge of the consumer.[3] Thus, companies have a strong motivation to collect and use the personal data of consumers; while consumers have an equally strong desire to ensure their personal information is protected.[4] Many consumers believe they have both a right to know what personal information is being shared, as well as the ability to control the distribution of such information.[5]

The California Consumer Privacy Act ("CCPA" or "the Act") took effect on January 1, 2020, pursuant to a 2018 California ballot initiative responding to the public's desire to protect private information.[6] The legislation requires the California Attorney General to implement

---

1. *See* Adam C. Uzialko, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/RLN5-S66C] (last updated Aug. 3, 2018) ("The internet of things and artificial intelligence are two critical tools for companies in data capture and analysis, from better understanding day-to-day operations, making business decisions and learning about their customers.").

2. *Id.*

3. *Id.*

4. *See* Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, at 2 (discussing how consumers "are deeply anxious about how their personal information may be used").

5. *See* 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/#654b34ab1bc1 [https://perma.cc/3LRA-BJGU] (discussing how personal data is often buried in a "60-page privacy policy" that consumers often do not understand, and legislation is beginning to be passed to protect people from the harms that can flow from that misunderstanding).

6. John Stephens, *California Consumer Privacy Act,* ABA (July 2, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/ [https://perma.cc/E2XK-43P9]; California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018).

regulations providing more guidance by July 1, 2020.[7] Further, the CCPA grants California consumers various rights regarding their personal information held by businesses.[8] By defining a consumer as "a natural person who is a California resident," the CCPA covers any Californian defined as such under state income tax law.[9] Key provisions of the CCPA include granting consumers (1) the right to know what personal information is obtained by companies, (2) the right to delete information companies obtain, (3) the ability to opt out from the sale of their personal information, and (4) the promise that consumers will not be discriminated against for following through with any of these options.[10]

Financial institutions are subject to the CCPA because the Act applies to businesses that conduct any amount of business in California and that (1) have annual gross revenue of more than $25 million, (2) buy and sell personal information from 50,000 or more consumers, or (3) derive 50% or more of their annual revenue from selling consumers' personal information.[11] What is still unclear, however, is the question of whether these measurements are to be valued on a global basis or only from California sources; California's Attorney General has until July 2020 to address this question.[12] Since the language of the CCPA does not specify, "the prevailing consensus" leans toward the fact that the $25 million is overall revenue, as opposed to only California-based revenue.[13] Nonetheless, as financial institutions naturally acquire and process vast amounts of data as a necessary part of their operations,[14] these businesses

7. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.185(a) (West 2018) ("On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title . . . .").

8. *Id.* § 1798.110.

9. *Id.* § 1798.140(g).

10. *Id.* § 1798.110.

11. *Id.* § 1798.140(c).

12. Joseph J. Lazzarotti & Jason C. Gavejian, *California Consumer Privacy Act FAQs for Covered Businesses*, JACKSON LEWIS (Oct. 10, 2019), https://www.jacksonlewis.com/publication/california-consumer-privacy-act-faqs-covered-businesses [https://perma.cc/E6MJ-DBFX].

13. ALAN L. FRIEL & MELINDA L. MCLELLAN, BAKERHOSTETLER, THE CALIFORNIA CONSUMER PRIVACY ACT: FREQUENTLY ASKED QUESTIONS 2 (2019).

14. *See* Frederik Van Remoortel, *Financial Institutions and the General Data Protection Regulation*, FINANCIER WORLDWIDE MAG., Nov. 2016, at 26 ("Financial institutions and service providers to the financial industry process a vast amount of personal data on a daily basis.").

are forced to implement safer data privacy techniques to conform with the new CCPA standards.[15]

Regardless of the CCPA, banks, brokerage companies, and insurance companies throughout the nation have been under scrutiny and have followed certain data privacy regulations since November 11, 1999, when Congress enacted Title V of the Gramm-Leach-Bliley Act ("GLBA").[16] The GLBA contains two basic privacy provisions impacting financial institutions: Safeguard rules and Privacy rules.[17] Within these rules, the GLBA defines "personal information" more narrowly than the CCPA.[18] Consequently, following the enactment of the CCPA, GLBA-regulated financial institutions were forced to analyze the new CCPA requirements closely with respect to their operations.[19] Specifically, these institutions examined their activities involving "targeted online advertising, tracking web page visitors," and obtaining geolocation data.[20]

Following this analysis, many financial institutions found that some operating activities previously outside the scope of the GLBA regulation were now within the scope of regulation under the CCPA.[21] Though the CCPA does exempt "personal information collected…pursuant to the" GLBA, the exemption does not apply if such information falls under Section 1798.150 of the CCPA.[22] Moreover, the GLBA specifically provides that it sets the floor on privacy, allowing states to adopt stricter standards.[23] As such, in this case, the CCPA is not

15. *See* Reece Hirsh & Kristin M. Hadgis, *California's New, GDPR-Like Privacy Law Is a Game-Changer*, BLOOMBERG LAW, July 11, 2018, at 8 (explaining the need for businesses to "thoroughly review" data collected from consumers, while reorganizing personal information to comply with newly enacted notices derived from the CCPA).

16. *The Gramm-Leach-Bliley Act*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/glba/ [https://perma.cc/9XXD-6YVA].

17. *See* FED. TRADE COMM'N, *Financial Institutions and Customer Information: Complying with the Safeguards* (2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [https://perma.cc/UE5V-TJM4] (evaluating compliance with the GLBA safeguard provision); *see also* FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 5 (2002) (discussing the privacy provision within the GLBA) [hereinafter FED. TRADE COMM'N PRIVACY].

18. Stephens, *supra* note 6.

19. *Id.*

20. *Id.*

21. *See id.* (explaining how the GLBA does not give full exemption from provisions within the CCPA).

22. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.145(e) (West 2018).

23. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6824(b) (2018).

preempted by the GLBA for financial institutions; rather, the CCPA elevates California legislation above the minimum federal requirements to protect consumers.[24]

Before the CCPA, many financial institutions were already altering their methods for processing personal information in response to the European Union's ("EU") General Data Protection Regulation ("GDPR").[25] The GDPR took effect on May 25, 2018, and reaches financial institutions and other companies across the U.S. that (1) process personal data in the EU, (2) were established outside the EU but offer goods and services in the EU, or (3) monitor behavior of individuals in the EU.[26] The GDPR imposes, among many things, heightened client consent requirements and data breach reporting mandates.[27] Although the GDPR and CCPA have much in common, their provisions contain key differences, from the enforcement methods and provisions, to the process of opting out of the sale of personal information.[28] Consequently, aligning with the standards set forth within the GDPR alone is not enough to comply with the requirements of the CCPA.[29]

This Note proceeds in five parts. Part II discusses the background of the CCPA and how it is the "absolute toughest data privacy law in the United States" to date.[30] Part III analyzes the GLBA data privacy requirements and the aspects of the CCPA that reach further than the standards set forth in the GLBA.[31] Part IV examines the EU's data privacy history within the GDPR and the major parallels and differences between it and the CCPA.[32] Part V summarizes the comparisons

24. Stephens, *supra* note 6 ("GLBA entities will remain subject to the provisions and requirements of the CCPA if they engage in activities falling outside of the GLBA.").

25. Lindsay A. Seventko, Note, *GDPR: Navigating Compliance as United States Bank*, 23 N.C. BANKING INST. 201, 203 (2019).

26. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) [hereinafter GDPR].

27. *Id.*

28. *See generally* ALICE MARINI, ALEXIS KATEIFIDES & JOEL BATES, DATAGUIDANCE, COMPARING PRIVACY LAWS: GDPR V. CCPA (2018) (comparing and contrasting the GDPR to the CCPA broadly).

29. *See* Tyler Stites, *Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions,* 38 REV. BANKING & FIN. L. 132, 144 (2018) (explaining how compliance through navigating the GDPR will be "valuable," however not all-encompassing).

30. *See infra* Part II.

31. *See infra* Part III.

32. *See infra* Part IV.

throughout this Note and identifies how financial institutions are tackling the standards and adapting to change.[33]

II. BACKGROUND OF THE CCPA

The CCPA passed swiftly in 2018 and took effect at the beginning of 2020.[34] The broad purpose behind the CCPA is to give California consumers more control over their own information.[35] Due in part to several high profile data breaches, distrust in how companies and financial institutions were handling personal information increased in 2014.[36] Specifically, in 2014, JP Morgan Chase experienced a breach that exposed sensitive information to outside parties for an entire month before being detected.[37] Many of the consumers affected were previously unaware of the magnitude of personal information that JP Morgan Chase had compiled about them.[38] This breach, and others, increased consumer concerns about companies' use of their personal information,[39] and, despite pushback from major companies, California legislators responded with the enactment of the CCPA.[40] Furthermore, during the drafting phases of the CCPA, non-profits advocated for even more protective legislation, as will be prospectively spelled out in a new California ballot initiative likely to occur in November 2020.[41]

---

33. *See infra* Part V.

34. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/L92N-ERKB].

35. *See* Uzialko, *supra* note 1 (discussing business needs for capturing data and newly enacted laws, such as the CCPA).

36. *See* Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households,* N.Y. TIMES: DEALB%K (Oct. 2, 2014, 12:50 PM), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ [https://perma.cc/EJC5-JB4H] (explaining how the breach "emerge[d] at a time when consumer confidence in the digital operations of corporate American has already been shaken").

37. *Id.*

38. *See id.* (explaining the JP Morgan Chase breach as "another example of how Americans' most sensitive personal information is in danger").

39. *Id.*

40. Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime In the United States?*, 23 J. TECH. L. & POL'Y 68, 91 (2018).

41. *See* Eric P. Mandel, *Introducing the CPREA: California Privacy Rights and Enforcement Act of 2020,* DRIVEN (Oct. 4, 2019), http://www.driven-inc.com/introducing-the-cprea-california-privacy-rights-and-enforcement-act-of-2020/ [https://perma.cc/QVK8-D9PC] ("Consumer advocates who thought CCPA was a nice start but didn't go far enough will find much to like about CPREA.").

In addition to financial institutions, the CCPA applies to a broad range of companies and organizations. [42] The CCPA is thus a broad-ranging privacy bill and was the first law of its kind to be passed in the United States.[43] The statute defines businesses to include entities that conduct business in California and that (1) have gross revenue of $25 million, (2) receive personal information of 50,000 or more consumers, or (3) derive 50% or more of its annual revenue from the sale of consumers' personal information.[44]

Furthermore, the CCPA defines "personal information" just as broadly as it does businesses, covering "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."[45] There are multiple examples given as to what constitutes this personal information, such as postal addresses, online identifiers, email addresses, and "other similar identifiers."[46] In September of 2019, the CCPA was amended to address ambiguously defined terms by subtly revising the definition of "personal."[47] The amended definition clarifies that "an objective standard" is applied to what falls within the category of personal information and the "mere possibility that information can be linked to an individual is not enough" to qualify as such.[48]

Overall, the CCPA aims to grant California consumers various rights with regard to their personal information held by businesses: the right to know, the right to be forgotten, the right to opt out, the right to equal service and price, and the right to pursue a civil remedy if compliance is not followed by businesses.[49] Though the CCPA creates a partial exemption for financial institutions through a carve-out

42. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(c) (West 2018).

43. *See* Lapowsky, *supra* note 34 ("It is the first law of its kind in the United States.").

44. CAL. CIV. CODE § 1798.140(c).

45. *Id.* § 1798.140(o)(1).

46. *Id.* § 1798.140(o)(1)(A).

47. JEFFREY P. CUNARD ET AL., DEBEVOISE & PLIMPTON, NOT WITH A BANG BUT A WHIMPER: AT THE DEADLINE, MINOR AMENDMENTS TO THE CALIFORNIA CONSUMER PRIVACY ACT 4 (2019).

48. *Id.*

49. *See* CAL. LEG. ASSEMB. B. 25, 2019 Leg., Reg. Sess. (Cal. 2018) (discussing how the CCPA "grants consumers various rights with regard to their personal information held by businesses").

provision,[50] financial institutions are still impacted by the following key provisions of the CCPA.[51]

A. The Right to Know

First, the right to know requires businesses to disclose which personal information will be collected from consumers.[52] In response, consumers are allowed to request personal information that has been collected or already sold.[53] After a consumer requests information, the business must follow up by delivering the requested information to the consumer within forty-five days if it is found to be a verifiable request.[54] In order to thoroughly comply with this provision it is recommended that these businesses, which include financial institutions, create "document retention policies to preserve, retain, and store the records of CCPA requests and the business's responses to those requests for at least twenty-four months."[55]

B. The Right to be Forgotten

Another important component of the CCPA is the right to be forgotten.[56] This provision allows consumers to request that a business delete their collected personal information and to direct any third-party service providers to do the same.[57] Since financial institutions fall under the realm of businesses covered by the CCPA, they must have a reliable methodology of tracking personal information of consumers so that it can be swiftly deleted.[58] However, this right has exceptions that still allow businesses the ability to retain "necessary" information to complete

50. *See* CAL. CIV. CODE § 1798.145(e) ("This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act.").

51. Stites, *supra* note 29, at 136.

52. Stephens, *supra* note 6.

53. CAL. CIV. CODE § 1798.130(a)

54. *Id.* § 1798.130(a)(2).

55. Memorandum from Fried Frank on a Checklist to Clients and Friends 3 (Dec. 19, 2019) (on file with author).

56. Hirsh & Hadgis, *supra* note 15, at 4.

57. CAL. CIV. CODE § 1798.105.

58. Erin Bryan, Joseph Lynyak III & Tom Scanlon, *National Financial Institutions – Developing a Project Plan to Comply with the California Consumer Privacy Act*, DORSEY & WHITNEY LLP (June 28, 2019), https://www.jdsupra.com/legalnews/national-financial-institutions-21135/ [https://perma.cc/7RQH-QM6Y].

transactions, to provide goods and services to the consumer, or to perform a contract between the parties.[59]

C. The Right to Opt Out

The CCPA also requires businesses give their customers the right to opt out of the sale of personal information.[60] To meet this requirement, businesses must provide clear notice to consumers, such as a hyperlink that states "Do Not Sell My Personal Information" on their website.[61] Even more protections are given to minors; instead of an opt-out right, the CCPA requires that minors have an opportunity to clearly opt in to the sale of their information.[62] Essentially, this means that businesses cannot sell personal information of consumers between the ages of thirteen to sixteen without initial affirmative consent.[63] Thus, similar to the necessary requirements of a new methodology to delete personal information, financial institutions must also create a new system for the implementation of the opt-in and opt-out elections.[64]

D. The Right to Equal Service and Price

The rights granted within the provisions of the CCPA are further protected by the CCPA's right to equal service and price, regardless of whether a consumer chooses to take advantage of the rights granted in the CCPA.[65] This implies that a business cannot discriminate against consumers who choose to exercise their rights under the CCPA.[66] However, businesses are permitted to charge the consumers exercising their rights different rates if the difference is directly related to the "value provided to the consumer by the consumer's data."[67] Also, the CCPA spells out explicit exceptions; for example, if the difference in price or the difference in quality of a product is "reasonably related" to the value that is obtained from the personal information, then no prohibition against

59. Hirsh & Hadgis , *supra* note 15, at 4.
60. CAL. CIV. CODE § 1798.120(a).
61. Stephens, *supra* note 6.
62. CAL. CIV. CODE § 1798.120(c).
63. Hirsh & Hadgis, *supra* note 15, at 4.
64. Bryan, Lynyak & Scanlon, *supra* note 58.
65. CAL CIV. CODE § 1798.125.
66. *Id.*
67. Hirsh & Hadgis, *supra* note 15, at 5.

discrimination is present.[68] Similarly, if the business set up a method for offering "financial incentives" to consumers that requires an opt-in provision, then discrimination is also not considered to be present.[69]

E. Enforcement

Finally, the enforcement provisions of the CCPA apply to businesses that do not comply with the new regulations.[70] For example, as stated above, the CCPA expressly prohibits discrimination against consumers when they choose to exercise their rights under the CCPA.[71] When an intentional violation of the CCPA occurs and the business "fails to cure any alleged violation within 30 days after being notified of alleged noncompliance," the California Attorney General may bring a civil action in the name of the people of California for penalties up to $7500 per violation.[72] These civil penalties can accumulate because the CCPA does not specify the maximum amount that can possibly result from liability of multiple penalties for numerous violations.[73] With a focus on financial institutions, the language in the CCPA's carve out for GLBA-regulated entities explicitly states that although there are exceptions for financial institutions in compliance with the CCPA, "[t]his subdivision shall not apply to Section 1798.150."[74] Therefore, under the CCPA's private cause of action enforcement provision, financial institutions' consumers whose information has been "subject to an unauthorized access… or disclosure as a result of the business's violation of the duty" to comply with the reasonable security procedures and practices set forth in the CCPA can institute civil actions to recover the proper relief.[75]

Overall, the CCPA is "one of the most comprehensive [privacy measures] in the United States" and regulates consumer information more

68. *See* CAL. CIV. CODE § 1798.125 ("Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data."); *see also* Stephens, *supra* note 6 ("[T]his requirement does not prohibit a Covered Business from charging different prices or providing different quality goods or services if the difference is 'reasonably related' to the value of the personal information at issue.").

69. MARINI, KATEIFIDES & BATES, *supra* note 28, at 34.

70. CAL CIV. CODE § 1798.155.

71. *Id.* § 1798.125.

72. *Id.* § 1798.155(b).

73. MARINI, KATEIFIDES & BATES, *supra* note 28, at 37.

74. CAL. CIV. CODE § 1798.145(e).

75. *Id.* § 1798.150.

extensively than ever before.[76] Sections III and IV of this Note further compare provisions of the CCPA to both the GLBA and the GDPR, distinguishing standards within the CCPA that go beyond what was required in past acts.[77]

III. GLBA DATA PRIVACY REQUIREMENTS

In 1999, Congress enacted privacy standards for the financial services industry through Title V of the GLBA.[78] Title V contains privacy protections for consumer financial information, and is specifically divided into two basic data privacy provisions: the "Safeguards Rule" and the "Privacy Rule."[79] These rules create affirmative and continuing obligations to respect the privacy of consumers and to protect the security and confidentiality of the nonpublic personal information obtained.[80] Further, as briefly stated above, the GLBA sets the floor for data privacy acts in the U.S.; this is due to Section 6807 of the GLBA, considered to be a "reverse preemption" provision.[81] This provision provides that GLBA-regulated entities will not receive a full exemption from complying with state law privacy acts that may go beyond the reach of the GLBA.[82] Since portions of the CCPA requirements contradict the GLBA,[83] the GLBA regulated entities will remain subject to the requirements of the CCPA where operations fall outside the scope of the GLBA.[84] Moreover, conflicts arise between the CCPA and the GLBA because, although there is a "reverse preemption"

76. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/X3AV-PEJV].

77. *See* Hirsh & Hadgis, *supra* note 15, at 8 (discussing how businesses in preparing for the CCPA "required significant commitment of time and resources").

78. *See The Gramm-Leach-Bliley Act*, *supra* note 16 ("GLBA primarily sought to 'modernize' financial services.").

79. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801 (2018).

80. *Id.*

81. *See* 15 U.S.C. § 6807 ("[A] State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter."); *see also* Bryan, Lynyak & Scanlon, *supra* note 58 ("GLBA contains a 'reverse preemption provision' that provides that state law privacy rights trump privacy rights as contained in the GLBA.").

82. Bryan, Lynyak & Scanlon, *supra* note 58.

83. 15 U.S.C. § 6807.

84. *See* Stephens, *supra* note 6 (discussing the fact that the CCPA reaches different points of protection outside the scope of the GLBA).

provision in the GLBA, the CCPA carves out an explicit exception for the GLBA in Section 1798.145(e) of the CCPA.[85]

Therefore, this "reverse preemption" provision of the GLBA has created confusion among financial institutions in determining which of their operations were not already regulated under the GLBA, due to the broad and all-encompassing language within the CCPA.[86] This section analyzes financial institution activities that are subject to newly heightened regulations because they take place within the CCPA, but fall outside the reach of the GLBA.[87]

A. Background and History

Enacted on November 12, 1999, and fully implemented two years later, the GLBA requires financial institutions to notify customers about their information sharing practices.[88] Additionally, financial institutions are required to alert their customers and consumers of specific rights to opt out of information sharing with the institution and to enable certain protections against the sharing of personal data with third parties.[89] The interpretation of "nonpublic personal information" is vital within both the Safeguard and Privacy rules.[90] The term is broadly defined to mean "personally identifiable financial information [that is]: (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[91] Regulation P of the Code of Federal Regulations ("CFR") provides further explanation as to what qualifies as nonpublic personal information; for example, this type of information could include a customer's name or street address obtained using financial information not publicly available, such as an account number.[92]

---

85. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.145(e) (West 2018).

86. Stephens, *supra* note 6.

87. *See infra* Part III.A–D.

88. *See The Gramm-Leach-Bliley Act*, *supra* note 16 ("GLBA primarily sought to 'modernize' financial services.").

89. FED. TRADE COMM'N PRIVACY, *supra* note 17, at 9.

90. *See id.*, at 4 (explaining that nonpublic personal information is "any identifiable financial information" collected about an individual unless the information is "otherwise 'publicly available'").

91. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(4)(A) (2018).

92. Regulation P, 12 C.F.R. § 1016.3(p)(3)(ii) (2018).

Moreover, "publicly available information" is not explicitly defined within the GLBA; however, under Regulation P it means information that "you have a reasonable basis to believe is lawfully made available to the general public."[93] Specific examples of public personal information are not provided.[94] Nonetheless, the interpretation of public personal information primarily relies on information that financial institutions have a "reasonable basis" to believe is publicly available; thus, information in government records or information within a phonebook is included in that interpretation.[95] This moderately flexible standard lies at the heart of the differences in scope of the CCPA requirements compared to those within the GLBA.[96]

B. GLBA Carve Out Provision: CAL. CIV. CODE § 1798.145(e)

As referenced throughout this Note, the CCPA carves out an exemption provision for GLBA-regulated entities.[97] However, since the CCPA covers a broader set of information, "personal information," as opposed to "nonpublic personal information," the CCPA does not fully exempt financial institutions from compliance, due to the previously mentioned "reverse preemption" provision.[98] The applicability of the CCPA to financial institutions depends on how much the business "collects, obtains, uses, discloses, or otherwise handles information . . . that is not personally identifiable financial information" collected to perform financial services or give financial products to consumers.[99] Since financial institutions often collect personal information outside of the "direct product or service offering," the GLBA exemption does not fully protect financial institutions from compliance with the CCPA.[100]

---

93. *Id.* § 1016.3(r)(1).

94. FED. TRADE COMM'N PRIVACY, *supra* note 17, at 5.

95. *See id.* (outlining more examples of steps to take in order to come to a "reasonable basis" as to whether or not the information is nonpublic or not).

96. *See* Stephens, *supra* note 6 (qualifying language within the CCPA as "broad").

97. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.145(e) (West 2018).

98. Kristen Mathews & Adam Fleisher, *Financial Institutions and the CCPA: What Remains After the Law's Exceptions,* BLOOMBERG LAW, Oct. 2019, at 3.

99. *Id.*

100. *What Financial Institutions Need to Know About the California Consumer Privacy Act*, WINSTON & STRAWN LLP (2019), https://www.winston.com/en/thought-leadership/what-financial-institutions-need-to-know-about-the-california-consumer-privacy-act.html [https://perma.cc/8EZS-XAXM].

For example, it is likely that financial institutions' interactions with potential customers fall outside the scope of the GLBA but within the scope of the CCPA.[101] More specifically, if a financial institution initiates interactions with potential consumers and personal information is obtained, this falls within the realm of a CCPA protection not exempt by the GLBA carve-out provision.[102] This often comes in the form of financial institutions encouraging potential consumers to fill out surveys or sweepstakes with personal information through various avenues, such as visiting the financial institution's website.[103] Additionally, if financial institutions collect a person's unique identifiers following their visiting the institution's website, the personal information collected falls outside the scope of the GLBA's "nonpublic personal information," though, it does land within the CCPA's more encompassing protections.[104]

Since the GLBA carve-out in the CCPA further specifies that the exemption does not take away liability under Section 1798.150, granting consumers potential relief through a private cause of action, financial institutions are now subject to entirely new kinds of causes of action.[105] This is new because the GLBA does not set forth a private right of action for consumers to pursue individual or class-action claims; therefore, financial institutions after CCPA implementation may now begin receiving consumer-initiated lawsuits.[106]

C. Privacy Rules in Comparison to the CCPA

The Privacy rules implemented by the GLBA require financial institutions to provide consumers notice regarding use of their nonpublic personal information throughout the entirety of the consumer-business relationship.[107] Specifically, the rules involve both heightened compliance standards determining what falls in the realm of nonpublic

101. Mathews & Fleisher, *supra* note 98, at 4.

102. *Id.*

103. *Id.*

104. *Id.*

105. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150 (West 2018) (discussing the proper relief a consumer may be entitled to if a breach occurs with their personal information as protected under the CCPA).

106. David J. Oberly, *Analyzing the California Consumer Privacy Act's Impact on Financial Institutions*, BLANKROME (Aug. 26, 2019), https://www.blankrome.com/publications/analyzing-california-consumer-privacy-acts-impact-financial-institutions [https://perma.cc/CP96-Q5UX].

107. *See* FED. TRADE COMM'N PRIVACY, *supra* note 17, at 6 (discussing specific obligations businesses have to consumers under the privacy rule regarding "privacy notices").

personal information, as well as some exceptions for compliance.[108] As mentioned previously, nonpublic personal information is defined in the GLBA as consumer-specific financial information given by the consumer to the financial institution from transactions done on behalf of the consumer, or otherwise attained by the financial institution.[109] This category of information differs from "personal information" within the CCPA, defined as information that could be associated or linked to specific consumers or households.[110] Therefore, in assessing consumer rights under the GLBA's privacy section, Section 6802, financial institutions subject to GLBA regulation must determine whether they possess consumer "personal information" falling beyond the GLBA's nonpublic personal information.[111]

1. Collection of Geolocation Data and Targeted Online Advertising

For example, financial institutions that collect geolocation data or use targeted online advertising by tracking webpage visitors, may be subject to the CCPA and thus required to give notice to consumers and allow for them to opt out of the sharing of this personal information.[112] If a financial institution chooses not to alter its processing methodology for this data, then it is likely to pay heavy fines or face litigation authorized by the enforcement provisions of the CCPA.[113] This provision stands out because, under GLBA data regulations, financial institutions are likely protected when obtaining and using the information collected from geolocation data advertising.[114] This was due primarily to either the

108. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C.§ 6809(4) (2018).

109. *Id.*

110. CAL. CIV. CODE § 1798.140(o)(1).

111. *See* David M. Stauss, Kristen Poetzel & Malia K. Rogers, *GLBA and the California Privacy Act: Analyzing SB 1121's Change to the Financial Institution Carve-Out Provision*, BALLARD SPAHR LLP (Sept. 25, 2018), https://www.ballardspahr.com/alertspublications/legalalerts/2018-09-25-glba-and-the-california-privacy-act-analyzing-sb-1121s-change [https://perma.cc/5EYY-A3TK] (explaining how the language in the CCPA is not a "full exemption" for GLBA entities, instead entities are subject "if they engage in activities falling outside the GLBA – which they almost certainly do").

112. *Id.*

113. CAL. CIV. CODE § 1798.155.

114. *See* Stauss, Poetzel & Rogers, *supra* note 111 (discussing how GLBA regulated entities once used "targeted online advertising, tracking web page visitors, and/or collecting geolocation date" without a need to reanalyze and assess new methodologies).

safeguards financial institutions were granted under GLBA exceptions or through the more flexible protocols throughout the GLBA.[115]

However, GLBA-regulated financial institutions benefit in some respects due to the carve-out provision from the CCPA, though these exemptions differ on a case-by-case basis.[116] Nevertheless, when data collection is done in "connection with the provision of a financial service" and for this reason beyond the scope of marketing efforts, the GLBA-regulated financial institutions may be protected from CCPA enforcements against them.[117] Thus, financial institutions must completely immerse themselves in the language of the exemption and make specific distinctions about whether or not personal information is collected through marketing efforts that inevitably do not lead to providing customers with financial products or service.[118]

2. Notice Rights and the Right to Opt out

Both the CCPA and the GLBA provide specific requirements for initial notice standards for consumers, as well as opt-out rights.[119] The CCPA requires a business to "provide a clear and conspicuous" way to enable consumers to opt out of the sale of their personal information and to include descriptions of the opt-out rights when doing so.[120] Similarly, the GLBA also requires a "clear and conspicuous" notice of what the financial institution's data privacy policies and practices consist of and "an explanation of how the consumer can exercise that nondisclosure option."[121]

Furthermore, the CCPA opt-out requirements provide a list of exceptions where a business "shall not be required to comply with a

115. *See* Stephens, *supra* note 6 ("GLBA-regulated entities will still be subject to millions of dollars of potential damages if they experience a data breach.").

116. *See* John E. Clabby & Michael L. Yaeger, *Are Banks and Other Lenders Subject to the CCPA?*, CARLTON FIELDS (Aug. 29, 2019), https://www.carltonfields.com/insights/publications/2019/are-banks-and-other-lenders-subject-to-the-ccpa [https://perma.cc/A73E-W3DE] (discussing the exemptions "designed for types of data").

117. *Id.*

118. *Id.*

119. *See* FED. TRADE COMM'N PRIVACY, *supra* note 17, at 6 (discussing the notice requirements involving both "annual notice" and "opt-out notice"); *see also* Stephens, *supra* note 6 (discussing the rights to opt-out and the requirement upon companies to make the opportunity to do so clear).

120. Pardau, *supra* note 40, at 100.

121. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6802(a) & (b) (2018).

consumer's request to delete," including circumstances where there is a need to detect illegal activity, to comply with legal obligations, or to perform contracts between the business and the consumer.[122] These exceptions run parallel to the GLBA opt-out right exceptions, as they also allow for the disclosure of nonpublic personal information to protect against potential fraud, to comply with laws, or to provide processing of a "financial product or service" consented to by the consumer.[123] However, the GLBA also incorporates another exception which conflicts with the CCPA protections: under the GLBA, disclosure to nonaffiliated third parties is allowable to perform functions on behalf of the financial institution, including marketing, as long as there is a contractual agreement with that third party to keep the information obtained confidential.[124] In essence, the CCPA's new protections now override that final exception because the GLBA merely sets the floor of protection, and the GLBA carve-out provision within the CCPA does not constitute a full exemption.[125]

The CCPA supplements the standard requirements of the GLBA opt-out provisions, resulting in a need for compliance changes for a majority of financial institutions.[126] First, the statute states that a "consumer shall have the right, at any time to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[127] The CCPA also adds that a business cannot sell personal information of a consumer less than thirteen years of age without affirmative authorization, thus creating an opt-in provision for a group of consumers not covered within the GLBA.[128] The CCPA also goes beyond the scope of the GLBA by requiring that businesses act swiftly if a consumer contacts and directs the business not to sell the consumer's personal information retrospectively, unless expressly stated otherwise.[129]

---

122. *Id.*

123. *Id.* § 6802(e).

124. *Id.* § 6802(b)(2).

125. *See id.* § 6802(b) (describing the opt out right "in general" as well as the "exception").

126. *See* Pardau, *supra* note 40, at 81 (explaining the similarities of the CCPA to the GLBA).

127. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.120(a) (West 2018).

128. *Id.* § 1798.120(c).

129. *See id.* § 1798.130(a)(2) (explaining the measures of delivery of personal information to consumers using words like "promptly" and "readily").

Conversely, the main disclosure requirements within the opt-out provisions of both the GLBA and the CCPA are similar, with only a few aspects of the CCPA reaching beyond those of the GLBA.[130] The GLBA requires privacy notices regarding the following: (1) the categories of nonpublic personal information collected and disclosed, (2) the third parties to whom the business discloses the nonpublic personal information, (3) an explanation of the consumer's right to opt out of disclosure of nonpublic personal information, and (4) the businesses policies and practices in protecting the confidentiality and security of nonpublic personal information.[131] The CCPA requires similar categories within its privacy notices, including (1) lists of what information is collected about consumers, (2) which third parties are also gaining access to this information, (3) the purpose behind the collection of the personal information, and (4) the consumer's right to opt out.[132] Still, the CCPA differs in multiple respects.[133] Under the CCPA, financial institutions must also (5) provide a description of consumer rights under the act, (6) list designated methods for submitting requests for personal information collected, and (7) make a clear statement that the consumer still has the right to request the deletion of personal information later.[134]

Although there is much overlap between these laws, there are also important differences. Thus, financial institutions may decide to alter the contracts given to consumers by providing more information and adding disclosures to encompass the broad reach the CCPA has over them.[135]

D. Safeguard Rules in Comparison to the CCPA

The GLBA explicitly imposes an "affirmative and continuing" policy obligation upon financial institutions, which obligates financial institutions to safeguard the nonpublic personal information obtained

130. *See* Pardau, *supra* note 40, at 81 (discussing how the CCPA is similar to the GLBA, however more "stringent").

131. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6803(c) (2018).

132. CAL. CIV. CODE § 1798.130.

133. *See* Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6803(c) (describing "information to be included").

134. CAL. CIV. CODE § 1798.130.

135. *See* Stauss, Poetzel & Rogers, *supra* note 111 (explaining the implications of only following the GLBA under the newly enacted CCPA due to the fact the GLBA does not grant a full exemption).

from customers.[136] The GLBA further requires financial institutions to implement measures to (1) guarantee the "security and confidentiality" of consumers' information, (2) "protect against any anticipated threats" to the information, and (3) prevent "unauthorized access" to the use of the information that could "result in substantial harm or inconvenience to any customer."[137] In order for businesses to comply with the Safeguards rule, they must address risks to consumer information in each step of their operation, assessing whether it is necessary to obtain and store the personal information of their consumers.[138]

By imposing reasonable security measures without granting an exemption for the GLBA, the CCPA's main safeguard protects consumers in new respects by ensuring that businesses do not discriminate against consumers that choose to exercise their rights within the CCPA.[139] For example, if one consumer chooses to opt out of the sale of their collected personal information to a third party, while another consumer does not choose to do so, the business cannot offer the compliant consumer a different quality good unless the difference is "reasonably related" to the value of the personal information obtained.[140] Thus, the safeguard implementations from the CCPA protect consumer information in a new way that is outside the scope of the GLBA, requiring additional provisions to be added and operations to be altered throughout businesses. [141]

IV. THE GDPR

The CCPA has been referred to as "California's Mini GDPR" because of its striking similarities to the EU's data privacy law implemented in May 2018.[142] Like the CCPA, the GDPR attempts to

136. Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801(b).

137. *Id.*

138. Juliana De Groot, *What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Bliley Act in 2019*, DIGITAL GUARDIAN (July 15, 2019), https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act [https://perma.cc/7ZY9-ZCLD].

139. CAL. CIV. CODE § 1798.125.

140. Stephens, *supra* note 6.

141. *See id.* (specifically requiring more protections to consumers who desire to exercise rights under the CCPA).

142. Mike Khoury, *California's Mini-GDPR? The Newly-Enacted California Consumer Privacy Act of 2018*, PRIVACY DATA BREACH (July 10, 2018), https://www.lexology.com/library/detail.aspx?g=60487525-76ea-44e3-97a8-3b9b02987c2e/ [https://perma.cc/73JH-RDRK].

protect individuals from the misuse of their personal information.[143] Moreover, the newest California ballot initiative, the California Privacy Rights and Enforcement Act of 2020, will make the California law even more similar to the GDPR if passed.[144] Nonetheless, due to the extensive reach of the GDPR, many U.S. financial institutions were already forced to conform to the GDPR standards, thus making the more recent effects of the CCPA less of an obstacle to follow.[145] The GDPR impacts companies that (1) process personal data in the EU, (2) are established outside the EU but are offering goods and services in the EU, or (3) monitor behavior of individuals in the EU.[146] Many domestic financial institutions are subject to the GDPR and must therefore reevaluate their client consent requirements, review existing contracts, update privacy policies, and create new data breach reporting mandates to be confident with their GDPR compliance.[147]

A. Key Provisions

The main regulations coming from the GDPR are (1) the right to use, (2) the right to delete, (3) the right to portability, (4) the right to edit, and (5) the right to restrict processing.[148] These rights, specifically the right to delete and the right to portability, have caused the most stress for financial institutions, as it has not been common practice for banks to navigate these types of requests.[149] For example, these new consumer requests for the deletion of their past or present data or their requests to easily access copies of their personal data in a usable format, pose new challenges due to the opposing interests of financial institution's accounting and taxation needs.[150] To that end, in order to comply, U.S.

143. *See id.* (discussing the protections both acts give consumers and how "[t]he CCPA is similar to Europe's General Data Protection Regulation ("GDPR"), which went into effect on May 25, 2018. Much like the GDPR, the cost of noncompliance can be staggering.").

144. *See* Purvi Patel, Joseph Roth Rosnet & Robert Famigletti, *Here We Go Again: New CCPA Ballot Initiative, Fall 2020*, CPO MAG., Oct. 22, 2019, at 28 ("The CPREA would require businesses to adhere to new general data protection principles.").

145. *See* Hirsh & Hadgis, *supra* note 15, at 8 ("Organizations that have recently prepared for the GDPR compliance" have already altered their methodology in how they process and protect consumer information).

146. GDPR, *supra* note 26, at 3(1).

147. Stites, *supra* note 29, at 138 (analyzing how those subject to the GDPR must provide "appropriate notification of personal data breaches").

148. Seventko, *supra* note 25, at 220.

149. *Id.* at 221.

150. *Id.*

banks underwent data mapping, providing institutions with better capabilities to respond to such requests.[151] Specifically, the data mapping process often consists of purchasing third party programs to generate tables that detail the entire business's processing activity, frequently also followed by a detailed "visual depiction of the lifecycle" of their consumer's personal information.[152]

This data mapping has permitted financial institutions to establish the infrastructure necessary to comply with new privacy standards.[153] Furthermore, data mapping was prevalent not only in GDPR compliance, but also with adjusting compliance methods for the CCPA.[154] Since data mapping creates effective visual tools to see where consumers information is at any point in time, it allows for "facilitat[ing] more robust and accurate privacy notices."[155] It also provides tools to allow for an ease to adjusting contracts with consumers regarding their new privacy rights, and make overall adjustments to technical tools for operations and retaining staff simpler.[156]

B. Parallels Between the GDPR and the CCPA

Both the GDPR and CCPA structure themselves around the collection and protection of similar types of "personal information" from consumers.[157] Specifically, both the CCPA and the GDPR define "personal information" in a substantially similar manner; both definitions encompass personal data relating to or associated with a particular consumer.[158] The only caveat is that the CCPA is slightly broader because it also includes information that is linked at the household or

151. Stites, *supra* note 29, at 143.

152. Dan Goldstein, *Where to Begin to Operationalize CCPA Compliance,* THE PRIVACY ADVISOR (Jan. 19, 2019), https://iapp.org/news/a/where-to-begin-to-operationalize-ccpa-compliance/ [https://perma.cc/H7VW-6EF4].

153. Stites, *supra* note 29, at 143.

154. *Id.*

155. Goldstein, *supra* note 152.

156. *See* Maya Goethals & Michael Imeson, *After the DustSettles – How Financial Services Are Taking a Sustainable Approach to GDPR Compliance in a New Era for Privacy, One Year on*, DELOITTE LLP, 2019, at 10 ("GDPR has been a key priority for banks" because it required "adjustments to their technical tools and contracts" as well as "train[ing] their people.").

157. *See* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, THOMAS REUTERS, 2018, at 2 (discussing how the information protected by both acts is "substantially similar").

158. *Id.*

device level.[159] The two laws are also similar in their provision of the consumer right to transparency of information because they both require subjected institutions to inform consumers about personal data collected and the purpose behind the collection if requested to do so.[160] This right to transparency created new obligations requiring covered entities to keep records of processing operations and to create new ways to track information.[161] Additionally, the GDPR has a similar right to be forgotten to the CCPA that grants consumers the right to request the deletion of personal information collected by the business.[162] The key difference is that the CCPA protects this right broadly with only minor exceptions, [163] while the GDPR only allows deletion of data in certain circumstances.[164] Consequently, under the CCPA, it is easier for a consumer to take advantage of this right to be forgotten, imposing more of a compliance burden on financial institutions.[165]

The CCPA sets out mandatory privacy policy disclosures, necessitating businesses to "affirmatively inform" consumers of categories of information taken, sources from which it was collected, and the purpose behind taking the information.[166] Additionally, under the CCPA, the business has only the preceding twelve months after the request to disclose the required information requested. [167] Furthermore, the disclosure requirements in the GDPR also require informing consumers about the personal information collected by the business and the intended uses, however it does not specify a certain timeframe like

159. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(1) (West 2018) (describing personal information as including information that "could be reasonably linked, directly or indirectly, with a particular consumer or household"); Jehl & Friel, *supra* note 157, at 2.

160. *See* Hirsh & Hadgis, *supra* note 15, at 3 (discussing how the CCPA is "GDPR-like" with regard to disclosure requirements for businesses within the scope to follow).

161. *See* Van Remoortel, *supra* note 14, at 26 ("This involves, for example, new obligations to keep records of processing operations.").

162. *Id.*

163. CAL. CIV. CODE § 1798.105.

164. GDPR, *supra* note 26, at 17.

165. *See* Jehl & Friel, *supra* note 157, at 5 (discussing that the right to be forgotten under the GDPR "only applies if the request meets one of six specific conditions while the CCPA right is broad.").

166. Chris Cwalina, Jeewon Kim Serrato, Steve Roose & Tristan Coughlin, *California Consumer Privacy Act: Disclosure Requirements*, NORTON ROSE FULBRIGHT (Sept. 11, 2018), https://www.dataprotectionreport.com/2018/09/california-consumer-privacy-act-disclosure-requirements/ [https://perma.cc/L9DV-D7SM].

167. CAL. CIV. CODE § 1798.100(d).

the CCPA requires.[168] These additional layers of consumer protection under both laws come at a cost for financial institutions because their data processing operations have to be practically altered at every step.[169] Without these necessary procedural changes, financial institutions would not be able to make personal information readily available upon consumer request and thus would not be able to comply.[170]

The financial institutions with a presence in the EU had an advantage in preparedness with respect to compliance with the CCPA due to the significant overlap between the CCPA and the GDPR.[171] However, due to the following key differences between the CCPA and the GDPR, mere compliance with the GDPR did not mean that the financial institutions would not have to alter their operations and procedures.[172]

C. Differences Between the GDPR and the CCPA

The most readily apparent difference between the GDPR and the CCPA is the reach of their regulation to financial institutions.[173] Not only are these laws governed by different entities, but the differences extend beyond that, as the EU's "territorial" reach is generally broader in nature.[174] The GDPR's protection is for consumers who are citizens or residents of the EU, even including consumers in the EU only temporarily,[175] while the CCPA only covers "a natural person who is a

168. Jehl & Friel, *supra* note 157, at 6.

169. *See* Goethals & Imeson, *supra* note 156, at 12 ("We needed to up-skill our frontline staff on how to handle all the request, complaints and questions that we knew would come in.").

170. *See id.* (discussing coping with data privacy law and the changes to the training and skill necessary to comply).

171. *See* Stites, *supra* note 29, at 143 (discussing the value in already have navigated the GDPR when it comes to CCPA compliance techniques).

172. *See id.* (explaining how the CCPA is still "distinct from the GDPR").

173. *See* MARINI, KATEIFIDES & BATES, *supra* note 28, at 9 (outlining how the territorial scope of the GDPR only requires that the business "offer goods, services or monitor the behavior of persons in the EU," while the CCPA requires the business to not only conduct business in California but also comply to additional requirements before falling under the threshold).

174. *See id.*, *supra* note 28, at 9 (discussing the differences in the territorial scope of the CCPA and GDPR).

175. *See* GDPR, *supra* note 26, at 3(2) ("This Regulation applies to the processing of data of data subjects who are in the Union by a controller or a processor not established in the Union"); *see also* Seventko, *supra* note 25, at 208 ("[A] data subject in the Union could be a citizen of the EU, a resident of the EU, or merely a person temporarily in the EU.").

California resident."[176] In other words, both laws only protect their respective natural consumers.[177] Furthermore, not only do these laws protect different individuals, but their authority over various companies also differs, primarily depending on the companies' location and consumer reach.[178] Many U.S. financial institutions are subject to both the CCPA and the GDPR due to their size and because of their reach throughout a multitude of countries.[179] However, there are still financial institutions subject to the CCPA that are not within the scope of the GDPR due to a lack of presence in the EU.[180]

Other CCPA provisions that are distinct from the GDPR are the opt-out right for personal information sales to third parties and the minor's opt-in rights within the CCPA.[181] Reiterated from Part III, the CCPA's opt-out and opt-in provisions create a strict set of standards for companies.[182] In contrast, the GDPR does not provide a specific right to opt out of personal information sales; instead, for example, under Article 7 of the GDPR, the consumer may "withdraw his or her consent at any time;" however, this "shall not affect lawfulness of processing based on consent before its withdrawal."[183] Thus, unlike the CCPA, the GDPR requires more effort on the part of the consumer to withdraw consent, as opposed to being alerted that he or she has an option to do so.[184] The two laws are substantially different in this regard because the CCPA's standards are less flexible and require "clear and conspicuous" treatment in allowing consumers to opt-out.[185] Therefore, while financial institutions under the GDPR have to modify operations for allowing the withdrawal of consent, under the CCPA the financial institutions must have new methodology for marketing financial products and services to consumers.[186]

---

176. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(g) (West 2018).

177. MARINI, KATEIFIDES & BATES, *supra* note 28, at 7.

178. *Id.* at 9.

179. *Id.* at 8.

180. *See id.* (explaining that in order to be under the GDPR some sort of business "presence" must be established).

181. CAL. CIV. CODE §§ 1798.105, 1798.120.

182. Stephens, *supra* note 6.

183. GDPR, *supra* note 26, at 7.

184. Jehl & Friel, *supra* note 157, at 4.

185. *Id.*

186. *See id.* (explaining the "opt-out" process is "substantially different" in comparison).

The final key differences between the CCPA and GDPR that affect the way financial institutions operate surrounds the enforcement methods behind the acts and the non-discrimination method exceptions.[187] While the CCPA explicitly sets guidelines, as discussed in Part II of this Note, the GDPR addresses avoidance of discriminatory processing implicitly, by expressing that personal information should be "processed… fairly," and that processing may only be done with "freely given" consent.[188] This should not mean that data under the CCPA is less likely to be used for discriminatory purposes because, although the CCPA has explicit language setting boundaries for business operation, it also sets up explicit exceptions.[189]

When discrimination is present, or when another provision in either the CCPA or GDPR is not met, "monetary penalties" may follow due to the enforcement provisions present in both laws.[190] As stated previously, the expenses that follow from a violation of the CCPA will be enforced by the California Attorney General, however, companies that have allegedly breached the CCPA are given a thirty-day grace period to "cure violations, if possible."[191] Comparatively, the GDPR can also result in "significant economic liability" when breached.[192] However, the GDPR penalties vary because the bar is set at "as much as four percent of the company's prior year global revenue," thus setting a maximum though very large limit to the penalty that is not present within the CCPA.[193] The final key difference between these enforcement methods is that the GDPR has a provision requiring a breach notification to occur

187. *Id.* at 6.

188. *See* GDPR, *supra* note 26, at 5–7 (discussing the "principles relating to processing of personal data" and the "lawfulness of processing"); *see also* MARINI, KATEIFIDES & BATES, *supra* note 28, at 34 ("The GDPR does not explicitly include this right and therefore no scope is defined.").

189. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.125 (West 2018) (describing different ways a business can be assumed to have discriminated, as well as exceptions to the general non-discrimination rule) ; *see also* Stephens, *supra* note 6 (explaining how there are scenarios where discrimination is allowable).

190. MARINI, KATEIFIDES & BATES, *supra* note 28, at 37.

191. *See* CAL. CIV. CODE § 1798.155 ("A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance."); *see also* Jehl & Friel, *supra* note 157, at 6 ("CCPA grants companies a 30-day period to cure violations, if possible.").

192. Jehl & Friel, *supra* note 157, at 6.

193. *Id.* at 7; see also Fines and Penalties, GDPR EU, https://www.gdpreu.org/compliance/fines-and-penalties/ [https://perma.cc/VZX5-EL6G] ("4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringement.").

within seventy-two hours after the business becomes aware of the breach, while the CCPA does not specify such a timeline.[194] Instead, the CCPA's breach notification timeline is governed by a separate California statute, which sets that "disclosure shall be made in the most expedient time possible and without unreasonable delay."[195]

After the GDPR and the CCPA went into effect, they both required "broad-scale changes" in order to avoid these harsh penalties, through improved business compliance procedures, revisions to daily operations practices, and new security measures.[196]

V. CONCLUSION

Financial institutions already in compliance with the GDPR likely experienced an easier adjustment to the CCPA due to the vast overlap between the key provisions in each, such as the requirements for transparency, the right to be forgotten, and the right to data portability.[197] On the other hand, a majority of U.S. financial institutions already complied with the GLBA and therefore may have been under the mistaken belief they were already in compliance with the CCPA.[198] Thus, the CCPA and its new bundle of regulations and compliance standards may have come as a surprise to many financial institutions.[199]

What should not come as a surprise, however, is the arrival of new privacy acts that are attempting to replicate the framework given within the CCPA. [200] For example, New York, Maryland, and Hawaii have followed suit by attempting to add more consumer privacy protective measures. [201] Overall, privacy acts of this nature require strict compliance to avoid penalties.[202] For that reason, in 2019, in attempting

194. Stephens, *supra* note 6.

195. CAL. CIV. CODE § 1798.29.

196. Stephens, *supra* note 6.

197. Hirsh & Hadgis, *supra* note 15, at 8.

198. *See* Stephens, *supra* note 6 (explaining how the GLBA does not give full exemption from provisions within the CCPA).

199. *See* Hirsh & Hadgis, *supra* note 15, at 8 (discussing how before implementation there were "many questions" remaining on how to fully comply with the CCPA).

200. *See* Natasha Kohne et al., *New Nevada Privacy Law Takes Effect In October – Comparison Of Nevada Law To CCPA*, MONDAQ LTD, Sept. 18, 2019, at 1 (describing how the Nevada law is "similar to the California Consumer Privacy Act" but narrower in scope).

201. *See* Elizabeth Feld, Note, *United State Data Privacy Law: The Domino Effect After the GDPR*, 24 N.C. BANKING INST. Part III (2020) (discussing states that have "Followed GDPR Data Privacy Trends").

202. Jeri Longtin-Kloss, *Dorsey & Whitney Launches California Consumer Privacy Act Compliance Screening and Assessment Tools,* BUS. WIRE (Sept. 17, 2019),

to alter their polices to comply with the CCPA, many businesses chose to use third party compliance screening tools to assess how many procedural modifications were going to be necessary. [203] For example, in September 2019, Dorsey & Whitney LLP launched a free CCPA screening tool for businesses to help in compliance with the CCPA.[204] This tool helped companies "determine whether the CCPA appl[ied] to their operations" by separating the CCPA into four threshold issues.[205] Based on the companies' responses to the questions, the screening tool provided a determination on whether the Act applied.[206] Regardless whether these screening tools were utilized or not, financial institutions at a minimum had to go through a data mapping process, as well as come up with plans to demonstrate that their "data security measures are reasonable based upon industry standards" in order to avoid expensive statutory damages.[207] The financial institutions also had to be prepared to address "complex operational problem[s]" by making specific workflows for each type of consumer request that exists under the CCPA regulations.[208]

The CCPA is a significant addition to U.S. privacy law that requires major compliance changes for covered entities.[209] The question then becomes whether a uniform federal statute would be a better approach to consumer protection, as opposed to forcing varying compliance measures created by state legislation.[210] Although the GLBA and the GDPR have similar provisions to the CCPA, simply complying with their privacy requirements is not sufficient under the CCPA because the CCPA is currently the "absolute toughest data privacy law in the United States."[211]

---

https://www.businesswire.com/news/home/20190917006052/en/ [https://perma.cc/EYP7-9VTE].

203. *Id.*

204. *Id.*

205. *Id.*

206. *Id.*

207. Bryan, Lynyak & Scanlon, *supra* note 58.

208. Goldstein, *supra* note 152.

209. Stephens, *supra* note 6.

210. *See* Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. Part I (2020) (stressing the importance of a potential federal data privacy policy).

211. Stephens, *supra* note 6; *see* Elizabeth Feld, Note, *United State Data Privacy Law: The Domino Effect After the GDPR*, 24 N.C. BANKING INST. Part III (2020) (comparing the "strikingly" similar aspects of the CCPA and the GDPR).

LAUREN DAVIS*

* I would like to thank my friends and family for their support throughout law school and in the process of developing this Note. I am incredibly grateful to Professor Lissa L. Broome, Morgan O. Schick, Brianne Marino Glass, Blake Leger, Erin A. Catlett, and the staff members of the North Carolina Banking Institute Journal for their thoughtful edits and comments which guided me to the final stages of the publication process.