Clients&FriendsMemo

The Digital Revolution Takes on New Meaning: Among Calls for Heightened U.S. Data Privacy Measures, California is King

March 1, 2019

California's ambitious new data privacy law, the California Consumer Privacy Act of 2018 ("CCPA"),[1] will go into effect on January 1, 2020 and promises to bring a new era of digital regulation to America's shores. Financial institutions that just navigated their way through implementing the European Union's General Data Protection Regulation ("GDPR"),[2] which became effective in May 2018,[3] may be uneasy about the prospect of complying with yet another new data privacy compliance regime. They will find some comfort in the fact that many of the systems and processes designed for GDPR compliance will serve their needs under the CCPA as well. However, between now and the go-live date of the CCPA, U.S. federal and state laws and regulations are likely to continue to evolve and expand, and financial institutions will need to prepare for CCPA implementation while staying abreast of other fast-moving developments. In this article we provide some key takeaways for how firms can be as prepared as possible for the continuing evolution of U.S. data privacy law.

I. The New California Data Privacy Law Will Apply Broadly to Financial Institutions with Customers in California

Financial institutions with customers who are California residents almost certainly fit within the types of businesses to which the CCPA will apply. A "**business**" subject to the CCPA includes for-profit sole proprietorships, partnerships, limited liability companies, corporations, associations, or any other legal entities that collect consumers' personal information and that satisfy one or more of the following criteria:

---

1 *SB-1121 California Consumer Privacy Act of 2018* (Sept. 24, 2018), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121.

2 European Commission, General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

3 *See* Joseph Moreno et al., *The EU's New Data Protection Regulation – Are Your Cybersecurity and Data Protection Measures up to Scratch?*, Cadwalader, Wickersham & Taft LLP (Mar. 6, 2017), https://www.cadwalader.com/resources/clients-friends-memos/the-eus-new-data-protection-regulation--are-your-cybersecurity-and-data-protection-measures-up-to-scratch#.

(a) has annual gross revenues in excess of $25 million;

(b) alone or in combination annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or

(c) derives 50% or more of its annual revenue from selling consumers' personal information.[4]

The CCPA also applies to legal entities that control or are controlled by a CCPA-covered business, and where the two legal entities share common branding (such as a shared name, servicemark, or trademark).[5]

For U.S. businesses seeking to remain outside the purview of the CCPA, the available carve-out is extremely narrow. Businesses that collect or sell the personal information of a California resident are exempt from the CCPA only if "every aspect of that commercial conduct takes place wholly outside of California." This requires that (a) the personal information must have been collected when the consumer was outside of California, (b) no part of the sale of the consumer's personal information occurred in California, and (c) no personal information collected while the consumer was in California was sold. In practice, this means that any firm with a website or other digital presence visited by California residents will likely be ensnared by the CCPA even if they lack employees or a physical presence in the state.[6]

Businesses that fail to comply with the CCPA are subject to the possibility of a state enforcement action and consumer lawsuits (available only after providing notice to the business and the business fails to cure the violation within 30 days).[7] However, unlike the GDPR which can impose fines calculated as a factor of global revenue, the CCPA assesses penalties of up to $2,500 per violation and up to $7,500 per intentional violation.[8]

II. California's Expansive Concept of "Personal Information" Is Similar to the GDPR

When determining what consumer data will constitute personal information under the CCPA, firms can look to certain similarities with the GDPR.

---

4 Cal. Civ. Code § 1798.140(c)(1).

5 § 1798.140(c)(2).

6 § 1798.145(a)(6).

7 § 1798.150(b).

8 § 1798.155(b).

Under the CCPA, "**personal information**" means "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." This includes, but is not limited to, names, addresses, identification number (such as social security, driver's license, or passport), email address, and Internet Protocol (IP) address. It also includes biometric information, internet activity information (such as web browser or search history, or information regarding a consumer's interaction with a website), geolocation data, and employment-related or education information.[9] This definition is largely consistent with how the GDPR broadly defines "personal data" for residents of the EU.[10]

The CCPA does not apply to data that has been "deidentified," which means personal information that cannot reasonably identify, relate to, describe, or be linked to a particular consumer.[11] This is akin to the GDPR's exclusion for "anonymized" data which cannot be used to identify a data subject. In addition, the CCPA does not apply to "aggregate consumer information," which is information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household or device.[12]

One difference between the two regimes, however, is that the CCPA's definition of personal information excludes "publicly available" information, which is information that is lawfully made available from federal, state, or local government records.[13] The GDPR does not have a similar exception and instead provides the same protections to personal data regardless of its source.

III. California Consumers Will Enjoy a New Bill of Rights Protecting their Personal Information

Another similarity between the CCPA and the GDPR is the recognition of several fundamental rights that consumers will soon enjoy relating to the collection, use, and sale of their personal information. Under the CCPA, these can effectively be described as:

(1) Right of Disclosure. A business that collects a consumer's personal information will be required, at or before the point of collection, to inform consumers as to the

[9] § 1798.140(o)(1).

[10] Article 4 of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[11] § 1798.140(h).

[12] § 1798.140(a).

[13] § 1798.140(o)(2). Under the CCPA, personal information loses its "publically available" designation if that data is "used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained." *Id.*

categories of personal information to be collected and the purposes for which the categories of personal information will be used.[14] A consumer, *i.e.*, a "natural person who is a California resident," will also have the right to request such a business disclose to that consumer the categories and specific pieces of personal information the business has collected.[15] Such a request must be complied with promptly, by mail or electronically, and free of charge to the consumer; however, businesses will not be required to provide such information per consumer request more than twice in a 12-month period.[16] Together with this right, consumers will also have the ability to request the business or commercial purpose for collecting or selling personal information, and the categories of third parties with whom the business shares personal information.[17] Finally, consumers will have the right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose what personal information was collected and the categories of third parties to whom it was sold.[18]

(2) Right of Deletion. A consumer will have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.[19] If a business has received such a request, it will be required not only to delete the consumer's personal information from its records, but also to direct any service providers to do the same.[20] This obligation to delete personal information at consumer request is subject to several exceptions, including for the completion of a financial transaction, to detect security incidents or debug errors, and to comply with legal obligations.[21]

(3) Right to "Opt Out." A consumer will have the right to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information going forward.[22] Once a business has received such an instruction from a consumer, it may not resume selling that consumer's personal

[14] § 1798.100(b).

[15] § 1798.100(a).

[16] § 1798.100(d).

[17] § 1798.110(a).

[18] § 1798.115(a).

[19] § 1798.105(a).

[20] § 1798.105(c).

[21] § 1798.105(d).

[22] § 1798.120(a).

information unless express authorized to do so.[23] This right of a consumer to "opt out" must be clearly communicated to consumers on a business' website under a banner titled "Do Not Sell My Personal Information," with an accompanying link that enables a customer to opt out of the sale of the consumer's personal information.[24]

(4) Right to Non-Discrimination. Businesses will be prohibited from discriminating against consumers who exercise their various rights under the CCPA by denying them goods or services, charging different prices, or providing a different level or quality of goods or services.[25]

IV. Financial Institutions Should Not Expect a Complete Carve-Out Under Federal Law

The CCPA will not apply to personal information that is collected, processed, sold, or disclosed under certain federal laws.[26] One such law is the Gramm-Leach-Bliley Act ("GLBA"),[27] which covers financial institutions that offer consumers financial products, like banks, and contains its own consumer privacy-related protections.[28] However, this is not a complete exception because the CCPA defines personal information far more broadly than the financial transaction-related data contemplated by the GLBA, and includes such data as browser history and IP address. As a result, firms will need to contemplate what personal information they collect in addition to what is captured under the GLBA and be prepared to protect it accordingly under the CCPA.

V. Conclusion

California may be the next big word on U.S. data privacy legislation, but it is unlikely to be the last. In recent years, Congress and other states have faced increased pressure to explore new cybersecurity and data privacy legislation due to a multitude of factors including a growing awareness of how businesses collect and use personal information as seen with Cambridge Analytica's use of Facebook data, and public frustration with companies' perceived lackluster responses to major customer data breaches.[29] A recent report from the U.S. Government

---

[23] § 1798.120(c).

[24] § 1798.135(a)(1).

[25] § 1798.125(a)(1).

[26] § 1798.145(e).

[27] 15 U.S.C. §§ 6801-6809, 6821-6827.

[28] Federal Financial Institutions Examination Council, *Gramm-Leach-Bliley Summary of Provisions*, https://www.ffiec.gov/exam/InfoBase/documents/02-con-g-l-b_summary_of_provisions-010416.pdf.

[29] *See* Joseph Moreno, *States Respond to Equifax Cyber Breach with Enforcement Actions and Calls for Enhanced Regulatory Powers*, Cadwalader, Wickersham & Taft LLP (Oct. 13, 2017), https://www.cadwalader.com/resources/clients-friends-memos/states-respond-to-equifax-cyber-breach-with-enforcement-actions-and-calls-for-enhanced-regulatory-powers.

Accountability Office further highlights America's growing appetite for GDPR-like legislation, calling it an "appropriate time for Congress to consider comprehensive Internet privacy legislation."[30] And while the last Congress failed to enact any new national data privacy legislation into law, both the House and Senate have held hearings recently to receive testimony on guiding principles for a potential federal data privacy law, with a key question being whether any such law should preempt state laws like the CCPA.[31] So while a full-blown U.S. equivalent of the GDPR may not yet be in the cards, the current mood among the public and among lawmakers points in the direction of more rather than less intensive data privacy rules to come.

* * *

If you have any questions, please feel free to contact any of the following Cadwalader attorneys.

Joseph V. Moreno	+1 202 862 2262	joseph.moreno@cwt.com
Sophie K. Cuthbertson	+1 202 862 2341	sophie.cuthbertson@cwt.com
James A. Treanor	+1 202 862 2330	james.treanor@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com
Stephen Weiss	+1 202 862 2347	stephen.weiss@cwt.com

[30] United States Government Accountability Office, *Internet Privacy Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility* (Jan. 2019), https://www.gao.gov/assets/700/696437.pdf.

[31] U.S. House Committee on Energy & Commerce Subcommittee on Consumer Protection & Commerce, *Hearing on "Protecting Consumer Privacy in the Era of Big Data"* (Feb. 26, 2019), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-protecting-consumer-privacy-in-the-era-of-big-data; U.S. Senate Committee on Commerce, Science, and Transportation, Policy Principles for a Federal Data Privacy Framework in the United States (Feb. 27, 2019), https://www.commerce.senate.gov/public/index.cfm/hearings?ID=CBA2CD07-4CC7-4474-8B6E-513FED77073D; Alfred Ng, *At Hearing on Federal Data-Privacy Law, Debate Flares Over State Rules*, CNET (Feb. 26, 2019), https://www.cnet.com/news/at-hearing-on-federal-data-privacy-law-debate-flares-over-state-rules/; Daniel R. Stoller, *New FTC Powers Weighed in Senate Data Privacy Hearing (1)*, Bloomberg Law (Feb. 27, 2019), https://news.bloomberglaw.com/privacy-and-data-security/new-ftc-powers-weighed-in-senate-data-privacy-hearing-1.