Client Advisory

CARTER LEDYARD & MILBURN LLP
Partners for Your Business®

Cybersecurity Practice Group

January 2, 2019

The California Consumer Privacy Act; Is U.S. Federal Data Privacy Legislation Next?

Data privacy was front and center in 2018. As discussed in our April 2018 and December 2018 Advisories, the European Union's (EU) General Data Protection Regulation (GDPR) became effective on May 25, 2018, and companies throughout the world have been faced with challenges in complying with the regime's data protection and privacy framework. The emphasis on data privacy and protection has also led to key developments in the United States. In June 2018, the State of California passed an expansive and landmark consumer privacy law, the California Consumer Privacy Act of 2018 ("CCPA" or "the Act"), which was amended in September and becomes operative on January 1, 2020.[1] Although not as broad as the GDPR, the CCPA similarly gives California residents basic rights relating to their personal information, has an extraterritorial reach (in that it applies to businesses outside the state), and provides for monetary penalties and enforcement actions. That said, there are significant differences between the GDPR and the CCPA, and compliance with one may not necessarily equate to compliance with the other.

In addition, 2018 saw increased momentum towards federal legislation in the United States that would provide a uniform set of federal consumer data privacy rules. This Advisory summarizes the CCPA's major provisions and discusses developments toward federal data privacy legislation in the United States.

I. The California Consumer Privacy Act

California Governor Jerry Brown signed the CCPA into law on June 28, 2018, and the law was amended on September 23, 2018. In an effort to bolster the right of privacy ensured by the California Constitution, the CCPA provides an array of rights to consumers regarding the sale and safe storage of their personal data by businesses whose commercial conduct reaches into the state. Moreover, the CCPA creates a private right of action and provides a civil-enforcement mechanism under the regulatory authority of the California Attorney General. It does not, however, include a specific requirement that data breaches be reported, which is a fundamental aspect of the GDPR. While there

[1] CAL. CIV. CODE § 1798.100 *et seq.*

may be further amendments to the Act prior to January 1, 2020, the following is a summary of some of the current provisions.

To Whom Does the CCPA Apply?

The CCPA is concerned with protecting consumer personal information. The CCPA broadly defines a consumer as "a natural person who is a California resident" as defined in state regulations pertaining to personal income tax. Thus, similar to the GDPR, which protects the personal data of all data subjects in the EU, the CCPA protects the personal information of all California residents.

Also, like the GDPR, it applies to businesses wherever located, even those outside the State of California. It applies to any covered business—wherever located—which collects information by any means (email, computer, etc.) from a California resident while the individual is in California. Thus, given the size of California's population (the most populous U.S. state) and the size of its economy (the 5th largest in the world), the CCPA will have a significant global reach.

That said, unlike the GDPR (which applies to all entities that process applicable personal data), the CCPA is concerned only with for-profit entities that meet at least one of three criteria: (i) have annual gross revenues in excess of $25,000,000; (ii) buy, receive, sell, or share the personal information of 50,000 or more individuals, devices, or households; or (iii) derive at least half its annual revenues from selling consumers' personal information. § 1798.140(c). The CCPA also applies to entities controlled by a covered business or that share common branding with the business. Importantly, such criteria effectively exempts small for-profit companies, non-profits (such as charities and foundations), and companies that either do not deal in consumer person information or do so on a small scale.

Furthermore, in spite of the CCPA's purported global reach, there is a geographic exception that may be important in determining whether a business's activities necessitate compliance with the CCPA. The CCPA is not applicable to the sale of consumer personal information where "every aspect of that commercial conduct takes place wholly outside of California." § 1798.145(a)(6). Under the CCPA, "commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold." *Id*. In this regard, the geographic scope is narrower than the GDPR.

Scope of Personal Information Covered

The primary focus of the CCPA is the sale and safe-keeping of consumer personal information. Like the GDPR, the CCPA defines personal information broadly—as any "information that identifies,

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." § 1798.140(o). This includes real names, IP addresses, email addresses, postal addresses, biometric information, browsing history, geolocation information, and employment information. The CCPA also sweeps in any information relating to a consumer's interactions with websites or online advertisements. Personal information also includes any inferences that can be drawn from information identified under the CCPA, if those inferences can be used to create a profile of, among other things, a consumer's preferences, habits, behaviors, attitudes, or intelligence. Personal information, however, does not include information that is publicly available.

Consumer Rights and Business Obligations

A covered business must affirmatively disclose, at or before the time information is collected, the types of personal information collected and the purposes for which that information will be used, and may not use it for additional purposes without notice. § 1798.100. A consumer has a right to notice of this information. In addition, a covered business must disclose the type of personal information collected about the consumer in the preceding 12 months and the categories of personal information sold or disclosed for a business purpose in the preceding 12 months. §§ 1798.110, .115, .130.

Consumers have the right to request disclosure from a business that collects or sells their personal information of the categories and specific pieces of information collected, the types of information sold to third parties, the business or commercial purpose for which the information was collected, and the types of third parties with which the business shares or to which it sold personal information, and such disclosures must be provided free of charge and in a readily usable format. §§ 1798.100, .110, .115, .130. A consumer also has the right to request that a business delete "any personal information about the consumer which the business has collected from the consumer." § 1798.105(a).

In order to effectuate the right of consumers to request disclosure of that information, businesses must provide two or more designated methods for submitting requests for information, which must include a toll-free phone number and a website address (if the business maintains a website). § 1798.130. Businesses must respond to verified requests within 45 days of receipt of the request.[2] Furthermore, each business must provide, in its online policies or on its website, a "description of consumers' rights" under the Act, and a list of the types of personal information collected, sold, and disclosed for a

[2] A business may extend that deadline by 45 days, but only once and only on notice to the requesting consumer.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

business purpose in the preceding 12 months. § 1798.130. Each business must update that information every 12 months.

The CCPA provides consumers a right to "opt out" of the sale of their personal information. A business seeking to sell the personal information of a consumer who is age 16 or older must provide notice to that consumer that their personal information may be sold, as well as an opportunity to opt out. The CCPA-mandated opt-out mechanism must include a link entitled "Do Not Sell My Personal Information," which must be conspicuously and clearly placed on the business's homepage, and must describe the rights and provide a link to the opt-out mechanism in the business's online privacy policy. § 1798.135(a). Under the Act, if the consumer does not affirmatively opt out and the requisite notice is provided, the consumer's personal information may be sold to third parties. In respect of consumers under 16 years old, a business may not sell personal information absent an affirmative opt in, effectuated by the consumer or, in the case of a consumer who is younger than thirteen, the consumer's parent or guardian. § 1798.120(c). This opt-out mechanism differs from the GDPR, which requires affirmative consent prior to the sale of personal data, regardless of the age of the data subject. This highlights the compliance challenges that lie ahead.

If a consumer opts out and no exceptions apply, the business is generally prohibited from selling that consumer's personal information to a third party. Consumers who opt out are also given the right not to be discriminated against because of that determination. A business may not deny goods or services, charge different prices, or alter the quality of goods or services provided to consumers who opt out of the sale of their personal information, and the CCPA prohibits financial incentive practices that are "unjust, unreasonable, coercive, or usurious in nature." § 1798.125. A business may, however, offer financial incentives to consumers who permit the sale of their personal information, "including payments to consumers as compensation," and may offer different prices to consumers in certain specified circumstances (which are somewhat vague and will require interpretative guidance). *Id*.

Any contractual provision purporting to waive or limit consumer rights under the CCPA is unenforceable and void as contrary to public policy (§ 1798.192), and thus a business cannot seek to bury waiver language in its terms and conditions.

Enforcement of the CCPA

The CCPA provides for public enforcement actions for any violations of the Act, with regulatory and enforcement authority in the hands of the California Attorney General, who must promulgate implementing regulations on or before July 1, 2020. The Attorney General is authorized to assess

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

penalties of $2,500 per violation, or $7,500 per intentional violation, against businesses which fail to cure violations within 30 days of notification. § 1798.155. Penalties collected under the CCPA will be deposited into a newly-created Consumer Privacy Fund, which will be used to offset enforcement costs. *Id.*

The CCPA also authorizes private civil actions as a result of data breaches and disclosures, but not for any and all violations of the Act. Specifically, "[a]ny consumer whose nonencrypted or nonredacted personal information" is accessed, stolen, or disclosed without authorization "as a result of [a] business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," may file a civil action against that business for money damages or injunctive relief. § 1798.150(a). A consumer seeking to file a civil action against a business must first give that business 30 days' written notice of the specific provisions alleged to have been violated, and, if within 30 days, the business cures the violation, the consumer may not initiate a civil action. *Id.*

Available statutory damages in a private action are the greater of either (i) between $100 and $750 "per consumer per incident" or (ii) actual damages. *Id.* In assessing statutory damages, the CCPA specifies that a court shall consider any of the following: "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." *Id.* It is not clear at this point how "per incident" will be defined or interpreted, which makes it difficult to estimate maximum potential damages.

Additional Exceptions and Exemptions

In addition to the exemption for non-profits and small businesses, and for transactions taking place wholly outside of California, there are also several other exceptions and exemptions under the Act. For example, the obligations imposed on businesses shall not restrict a business's ability to comply with federal, state, or local laws; comply with civil, criminal, or regulatory inquiries or investigations; and cooperate with law enforcement agencies. § 1798.145. In addition, the Act does not apply where compliance would violate an evidentiary privilege or where businesses handle personal data pursuant to and in accordance with certain federal privacy-related frameworks (such as health information pursuant to the Health Insurance Portability and Accountability Act, personal information used by credit reporting agencies under the Fair Credit Reporting Act, and personal financial information under the Gramm-Leach-Bliley Act, among others). *Id.*

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

II. Potential Federal Consumer-Privacy Legislation

Consumer advocates have been joined by legislators and even technology industry leaders in insisting on some form of unified federal consumer privacy regime and accompanying regulatory framework.

Technology industry leaders have been aggressively lobbying for a federal framework that would preempt state law, including the CCPA, in an effort to avoid the compliance challenges associated with a patchwork of state laws. The United States Senate Committee on Commerce, Science, and Transportation ("Commerce Committee") held hearings in September and October 2018, during which industry stakeholders urged federal action on the issue. Those stakeholders, which included major ecommerce, social-networking, and telecommunications companies, argued that the time is ripe for a standardized set of rules across the nation. Technology companies generally prefer less restrictive privacy laws and argue that compliance with privacy laws will divert significant resources away from innovation and invention which is fundamental to their survival. Filings on the part of some industry stakeholders to the Federal Trade Commission made similar arguments.

Lawmakers from the Senate and House of Representatives from both parties have proposed federal bills which vary in scope and levels of protection, such as the Data Care Act which was recently introduced in December 2018 by a group of Democratic senators. Some lawmakers seem hesitant to use the GDPR or the CCPA as templates for a federal consumer-privacy scheme, expressing concern about the potential consequences of excessive rule-making authority being given to an agency charged with implementing any new legislative scheme. Other lawmakers look to the GDPR as a convenient and appropriate model for the U.S. which is already applicable to many U.S. entities.

In the October 2018 hearings, consumer advocates testified before the Senate Commerce Committee. While some advocates urged Congress to adopt the GDPR or CCPA as models, others decried the CCPA as poorly drafted and cautioned Congress against adopting a one-size-fits-all approach to data privacy. Nevertheless, all consumer advocates appeared to agree that any federal legislation should provide a floor, and not a ceiling, for consumer protection.

The Federal Trade Commission ("FTC") is the primary federal agency regulating consumer privacy and data security, and thus will likely be the agency tasked with implementing and enforcing a federal consumer-privacy law. The FTC held hearings on December 11-12, 2018 on the subject of data breaches and data security, and is scheduled to hold additional hearings on February 12-13, 2019 on

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

the subject of consumer privacy—"to examine the FTC's authority to deter unfair and deceptive conduct in data security and privacy matters."[3]

While the issue is being considered in Congress, the Trump administration has also begun working to develop a nationwide set of consumer privacy rules or policies. U.S. Commerce Department officials have reportedly taken numerous meetings with industry stakeholders (including Facebook, Google, AT&T and Comcast) to discuss the implementation of a federal data-privacy regime. And the National Telecommunications and Information Administration ("NTIA"), an agency of the Commerce Department, recently requested public comment "on a proposed approach to consumer data privacy designed to provide high levels of protection for individuals, while giving organizations legal clarity and the flexibility to innovate."[4] The NTIA sought comment relating to its approach—which focuses on transparency as to how personal information is collected, used, shared, and stored; the right to control one's personal information; minimizing the collection, use, storage and sharing of personal data; and the responsibility on organizations to safeguard personal data and prevent disclosure or harmful uses of personal data. The FTC's November 2018 comments on the NTIA approach emphasized a balancing of the consumer's interest in privacy with business interests in innovation and competition.

At this point, there is uncertainty as to whether and when a federal data privacy law will become reality, what the possible legislation would look like, who would enforce it, and what safeguards and enforcement mechanisms would be instituted. However, as pressure mounts in light of the CCPA's enactment and a Democratic majority takes over the House of Representatives, it will be interesting to see if federal lawmakers will ultimately enact nationwide data privacy regulations, rules, and laws.

III. Considerations for 2019 and Beyond

The CCPA is landmark legislation that is already affecting the data privacy landscape in the U.S. While it does not become operative until January 1, 2020, there may be further amendments in 2019, and the California Attorney General has until mid-2020 to promulgate implementing regulations. Businesses should pay attention to it now. At a minimum, businesses should assess whether they are covered by the CCPA, stay abreast of developments, and begin to formulate a strategy for compliance.

---

[3] Press Release, FTC Announces Sessions on Consumer Privacy and Data Security As Part of its Hearings on Competition and Consumer Protection in the 21st Century (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.

[4] *See* 83 Fed. Reg. 48,600 (Sept. 28, 2018); Press Release, NTIA Seeks Comment on New Approach to Consumer Data Privacy (Sept. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

This is particularly important and complex given that certain requirements differ from the GDPR, and thus businesses may need to modify or update their compliance policies, mechanisms, and practices to ensure compliance with all applicable laws.

There is the possibility that U.S. states other than California will enact legislation modeled after the GDPR or CCPA, but with some differences, thus further complicating the patchwork of privacy regulations that makes compliance burdensome and difficult. We may also see action at the federal level to create a uniform privacy law or framework.

Businesses are encouraged to consult legal counsel to assist in assessing whether they are subject to the CCPA (or GDPR, or other applicable privacy law or regulation), interpreting the relevant provisions, and creating and implementing a privacy policy and strategy to ensure compliance.

This publication was authored by Carter Ledyard partner **Matthew Dunn** and associate **James S. Arrabito**. For more information concerning the matters discussed in this publication, please contact Mr. Dunn (212-238-8706, mdunn@clm.com), another member of Carter Ledyard's Cybersecurity practice group, or your regular Carter Ledyard attorney.
