A new decade in data privacy: Complying with the CCPA

By Charles Fleischmann and Ephraim Hintz

Charles Fleischmann (charles.fleischmann@huschblackwell.com) is an attorney with Husch Blackwell in Washington, DC, USA, and Ephraim Hintz (ephraimhintz32@gmail.com) is an attorney with Polsinelli in Denver, Colorado, USA.

Following daily headlines of data breaches and companies using or maintaining individuals’ data in less than desirable ways, governments around the globe have increasingly taken notice and started passing laws governing the rights of individuals with respect to their data, and the way others can permissibly use it.

Leading the pack was the European Union (EU), whose General Data Protection Regulation[1] (GDPR), came online in 2018. While companies doing business in the EU worked to become compliant with GDPR, various states in the US recognized that the federal government lacks much, if any, of the framework around this issue. As a result, several states have contemplated passing their own data privacy laws and regulations.

The most significant of these laws, the California Consumer Privacy Act (CCPA),[2] was passed in June of 2018. As California wrestled with the specifics of how compliance and enforcement would work, the state delayed the effective date of the CCPA until January 1, 2020. While the CCPA will be effective as of this article’s publication, enforcement is not set to begin until July 1, 2020.

As a result, the goals of this article are to (1) inform businesses whether they fall within the CCPA’s reach; (2) provide an understanding of the basics of the law, and the remaining areas of uncertainty; and (3) offer practical tips on how to comply for those affected businesses.

The CCPA in a nutshell

Dubbed California’s version of the GDPR, the CCPA shares a basic framework with its European predecessor, creating new rights for Californians with respect to their data, and imposing obligations on those businesses that handle it. Nonetheless, there are some key differences in the components and workings of these laws, such that a company already in compliance with the GDPR cannot simply assume compliance with the CCPA, or vice versa.

To state the obvious, the scope of coverage is different, focusing on California residents rather than Europeans. Specifically, the CCPA covers for-profit entities that do business in California, collect California residents’ “personal information,” and determine the means of processing that personal information, in addition to meeting any one of the following criteria:

- Have an annual gross revenue exceeding $25 million;
- Buy, receive, sell, or share, for commercial purposes, personal information of 50,000 or more consumers, devices, and households; or
- Derive 50% or more of annual revenue from selling consumers’ personal information.

When reviewing these criteria, it is important to note that subsidiaries or entities that are controlled by a business and share common branding with a business are also covered.

Broadly, the CCPA protects California consumers (i.e., residents) and holds covered entities accountable on how
they gather, receive, sell, or share a California consumer’s personal information. In terms of what constitutes “personal information,” the CCPA’s definition is extremely broad—in some respects broader than the GDPR’s.

Specifically, the CCPA defines personal information as information that reasonably identifies; relates to; describes; is reasonably capable of being associated with; or could reasonably be linked, directly or indirectly, with a particular consumer or household. Examples of personal information subject to the CCPA include, but are not limited to, names, mailing addresses, Social Security numbers, online identifiers, passport numbers, financial information, email addresses, driver’s license numbers, and biometric information.

The bottom line is that the CCPA covers all personal information that can be linked to a household or individual in California. The linkage to a household specifically is an area where the CCPA appears to go beyond the GDPR, which tends to focus only on individuals. However, there are a few key exclusions that businesses should be aware of. Specifically, the CCPA does not apply to personal information collected by a business from a person acting as a job applicant, employee, owner, director, officer, medical staff member, or contractor.

In determining the most efficient use of your business’s limited resources, understanding the CCPA’s enforcement mechanisms and penalties, as well as California’s enforcement priorities, can become almost as important as understanding what is required to comply. CCPA enforcement can occur via the California Attorney General’s Office or via private right of action/class action lawsuit.

The CCPA fixes statutory damages of $2,500 for each violation, or $7,500 for each intentional violation, with the California Attorney General issuing these fines. However, before the attorney general can bring an action for violation of the CCPA, a business must be given 30 days’ notice to cure the violation, with fines being assessed if the issues are not resolved. While the notice provision provides some level of protection for businesses, implementing a “cure” within 30 days, especially if it fundamentally alters a company’s data governance practices, could be an onerous task.

In addition to attorney general enforcement, the CCPA includes a private right of action for Californians in data breach scenarios. If a data breach occurs and the business failed to implement and maintain reasonable security procedures and practices, a private right of action could cost as much as $100–$750 per consumer per incident. Class action lawsuits are also contemplated—a class of consumers can sue a business stemming from a data breach when the business egregiously does not establish reasonable safety measures to prevent the data breach.

Nonetheless, there are a few key exclusions with respect to the enforcement of the CCPA. The law does not restrict a business’s ability to collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place outside of California. Additionally, the CCPA does not apply to information that is subject to other federal regulations, including the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, or the Driver’s Privacy Protection Act.

While the state’s enforcement priorities are far from clear at this stage, we can certainly expect the attorney general to try and notch a few high-publicity “big wins” early to show that the law is being strongly enforced. Additionally, due to the private right of action for data breaches, companies experiencing a breach should expect and take precautions for these sorts of actions. Because the harm to consumers is easier to quantify with a breach, and because of the high-profile nature of some breaches, we can certainly expect these incidents to be a top enforcement priority at the attorney general level as well.

**Consumers’ rights under the CCPA**

The CCPA establishes data-privacy rights for California consumers. The CCPA protects individuals who are domiciled in California and are outside of the state for a temporary purpose, and any individuals in California for other than a temporary purpose. Simply put, California residents hold the rights under the CCPA.

The CCPA expressly creates five rights for California consumers: the right to know, the right to access, the right to be forgotten, the right to opt out of sales, and the right to equal service.
The right to know

Probably the most obvious right that consumers hold under the CCPA is the right to know, at or before the point of collection, what personal information a business collects and the purposes for which the personal information will be used. At or around January 1, 2020, consumers probably received a bevy of emails from companies providing collection notice complying with this right. Covered entities will also need to update their privacy notices to place any prospective consumer on notice that the entity collects personal information and the purpose of such collection. CCPA-compliant privacy notices will list the categories of personal information the business collects, sells, or discloses to a third party for the business’s purpose.

The right to access

Under the CCPA, in conjunction with the right to know, consumers have the right to access a business’s records concerning what personal information is collected and the business purpose for disclosing such information. Upon a consumer’s request, a business must disclose the categories of personal information collected, the business purpose for collecting such information, the categories of third parties with whom the business shared the personal information with, and the specific pieces of personal information the business collected about the interested consumer.

If a business sells or discloses personal information for the business’s purpose, consumers have the right to request the business disclose the categories of personal information collected about the consumer, categories of personal information sold to the third parties, and categories of personal information disclosed about the consumer for the business’s purpose.

The right to be forgotten

Simply put, consumers have the right to request a business and service providers delete their personal information. However, this right only applies to personal information collected from the consumer, not a secondary source. Similar to the GDPR’s right to erasure, the right to be forgotten is subject to exceptions. Exceptions to this right include: it is necessary to maintain personal information to provide a good or service the consumer requested; personal information is needed for scientific, historical, or statistical research; or the personal information is necessary for detecting security incidents. Businesses should consult legal counsel when determining whether a CCPA exception applies at the time a consumer submits a verifiable request to delete his or her personal information.

The right to opt out of sales

The CCPA grants consumers the right to direct a business to not “sell” their personal information to third parties. Businesses should be aware the CCPA defines “sale” more broadly than the normal use of the term. Under the CCPA, “sale” means a transfer of personal information to another business or third party for monetary or other valuable consideration. Businesses will need to examine each relationship they have with a third party, especially third parties contracted as service providers.

After a consumer opts out of any future, potential sales, a business will then need to obtain express authorization to sell the consumer’s personal information. A caveat to the right to opt out for non-minors is a minor’s right to opt in to any sale. A business must not only comply with the collection requirements in the Children’s Online Privacy Protection Act, but must also comply with the CCPA’s right to opt in for minors by obtaining consent from the minor if the minor is between 13 and 16 years old and consent from the minor’s guardian if the minor is under 13 years of age. Because of the steep consequences, businesses should pay close attention to their interactions with minors.

The right to equal service
The right to equal service prohibits businesses from discriminating against consumers for exercising their CCPA rights. However, a business can permissibly incentivize a consumer to not exercise their rights (e.g., right to opt out; right to be forgotten). Under the right to equal service, a business can deny service to a consumer that does not want the business to collect the consumer’s personal information. However, under this right, a business cannot refuse to do business with a consumer simply because the consumer exercises an express CCPA right.

**California attorney general’s proposed regulations**

The attorney general published proposed regulations on October 10, 2019. (These regulations should be in force by the time this article is published.) These proposed regulations presumably will resemble the final regulations. Ultimately, the proposed regulations categorize the CCPA rights into statutory articles.

**Article 2 § 999.305**

Article 2 mandates that businesses, at or before the time of collection, inform consumers what categories of personal information the business will collect and the purpose for collecting such information. A business must only collect and use the personal information it previously disclosed to the consumer. When a business discloses the personal information it is collecting or using (either through a privacy policy or notice), it must only use general, straightforward language. The business should avoid using any technical jargon that a layman cannot understand.

**Article 3 § 999.305**

Article 3 establishes methods a business must implement to ensure its consumers are able to submit requests to know and delete. In fact, a business needs to provide two or more methods for a consumer to submit a request. These methods can vary from setting up a toll-free telephone number, operating a website, creating an interactive web form accessible through the website, or even creating a mobile application for consumers to access on their mobile devices. Regardless of the method, California law will require a business to allow for requests and will require acting upon a request in a timely fashion.

**Article 4 § 999.323**

To avoid any potential security incidents, California law will mandate that a business verify a consumer’s identity prior to complying with a request to know or delete. Under Article 4, a business shall establish, document, and comply with a reasonable method of verifying that the person making a request is the consumer from whom the business has collected personal information. Potential methods consist of security questions, requesting and matching information to the personal information maintained by the business, biometric scan, and/or signing a legally binding verification document.

**Article 6 § 999.323**

As mentioned above, the CCPA prohibits businesses from implementing discriminatory practices against consumers for exercising their rights under the CCPA. And, Article 6 codifies the prohibition on discriminatory practices. An important aspect of this Article is the fact that the CCPA does not prohibit businesses from favoring consumers with valuable personal information. A business can offer a price difference if it is reasonably related to the value of the consumer’s data. This price difference is a benefit to the at-issue consumer and does not discriminate against other consumers for exercising their rights. In addition, the CCPA allows the continuance of loyalty programs. A business that offers a discounted price to consumers for signing up for a loyalty program does not discriminate against consumers not in the loyalty program. Of course, the business will need to provide clear and unambiguous notice to the members of its loyalty program if the business collects members’ personal information and the purpose for collecting it.
Practical ways to comply with the CCPA

Complying with the CCPA is an incredibly vast undertaking that requires hours of investigation, documenting, meetings, and drafting notices. For most entities, the goal is to comply with the CCPA in a cost-effective manner. If your entity falls into this category, here is the bare minimum your business must do to comply with the CCPA.

Employ legal counsel

Your business might have a sophisticated in-house legal team at its disposal. However, you will want to hire outside legal counsel to examine your business’s data privacy framework, unless your in-house team possesses data privacy expertise. Unbiased legal counsel will be able to immediately point out areas of data privacy concern within your business (e.g., insufficient privacy notices and policies, lack of data breach safeguards, warning against collecting too much information) without any conflicting interests. Outside legal counsel will likely also have resources (e.g., data inventory tools) to effectively, efficiently speed up the process of your business becoming compliant with the CCPA and other applicable state data privacy laws.

Complete a data collection inventory

The first step of complying with the CCPA is determining what, when, how, and why your business collects personal information. This will require your business’s IT, marketing, sales, debt collection, and any other relevant departments to provide a summary of all the personal information each department collects, maintains, stores, or transfers to a service provider. Without completing this step, your business will be unable to comply with the CCPA, because under the CCPA, your business will need to provide notice to consumers of what information is collected, the purpose for collection, and whom the information is transferred or sold to.

Draft new privacy policies and notices

Once your entity has a general understanding of the personal information it collects, you can now start drafting your online privacy policies and notices. These policies and notices must inform the consumer that your business collects his or her personal information, the purpose for collecting the personal information, and what your business does with the personal information after collection. In addition, your business, through these notices, must inform the consumer of what cookies are enabled on your business’s website. The CCPA also requires privacy policies and notices to alert consumers to their rights under the CCPA: right to know, right to be forgotten, right to opt out, right to access, and right to equal service. Since the CCPA’s objective is to create data privacy transparency, consumers have a right to understand their rights as soon as they visit a business’s website.

Establish or update a data-privacy security framework

As mentioned, under the CCPA, the California attorney general or consumers can subject a business to substantial penalties for failing to implement reasonable data privacy safeguards. Covered entities should draft and implement a substantial security framework and establish an emergency plan. This security framework should include limiting access to personal information, creating a two-step security authorization process to access personal information, establishing mandatory data privacy trainings, and issuing all employees copies of your business’s data privacy plan. Lastly, your entity should create and train all relevant employees on its applicable data security emergency plan. This plan should inform each employee of his duties during a security incident, the protocol for remediating a security incident, and the procedure for complying with statutory obligations after an incident takes place.

Conclusion

Above are the broad strokes of the CCPA and its anticipated application to the business world; of course, there are
technicalities and stumbling blocks that businesses can encounter, in addition to the fact that the attorney general’s proposed regulations have yet to be finalized. Certainly following the tips provided above can help keep your company in compliance, but experienced legal counsel is the best method for minimizing your business’s exposure when dealing with the CCPA, GDPR, or other data privacy laws and regulations.

Takeaways

- The CCPA’s effective date was January 1, 2020, with enforcement set to begin on July 1, 2020.
- The CCPA is the first law in the United States to create consumer data privacy rights.
- Europe’s GDPR differs from the CCPA in several key ways, and compliance with one does not equate to compliance with the other.
- Enforcement can occur through the California Attorney General’s Office or, in data breach scenarios, via a California consumer’s private right of action.
- Under the CCPA, before or at the time of collection, businesses must inform California consumers what personal information the business is collecting from the consumers.