COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2020
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.