COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2024
A New Decade in Data Privacy: Complying with the CCPA

By Lisa J. Sotto and Danielle Dobrusin[1]

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, whose General Data Protection Regulation[2] (GDPR), came online in 2018. While companies doing business in the European Union worked to become compliant with the 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[3] (CCPA), was passed in June 2018. Enforcement of the law began on July 1, 2020.

In November 2020, California voters approved the California Privacy Rights Act of 2020 (CPRA), which significantly amended and expanded the CCPA. This article uses the term "CCPA" to refer to the CCPA as amended by the CPRA.

Most of the CPRA's substantive provisions became operative on January 1, 2023, with enforcement beginning on July 1, 2023. On March 29, 2023, the California Office of Adminstrative Law approved the California Privacy Protection Agency's (CPPA) proposed CPRA regulatons.[4] The regulations will come enforceable March 29, 2024.[5] The CPRA requires additional regulations to be issued on a variety of topics, including with respect to cybersecurity audits, risk assessments, automated decision-making, and profiling.

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 (3) offer practical tips on how to comply.

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 personal information and imposing obligations on certain businesses that handle it. Nonetheless, there are key differences in the components and workings of these laws, such that a company already in compliance with the GDPR cannot 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 purposes and means of processing that personal information, in addition to meeting any one of the following criteria:

- As of January 1 of each calendar year, had an annual gross revenue exceeding $25 million;[6]
- Alone or in combination, annually buy, sell, or share (as defined below) personal information of 10,000 or

more consumers or devices;[7] or

- Derive 50% or more of annual revenue from selling or sharing consumers' personal information.[8]

When reviewing these criteria, it is important to note that subsidiaries or entities (1) that control or are controlled by a business and share common branding with a business and (2) with whom a business shares consumers' personal information are also covered. Additionally, the CCPA applies to (1) a joint venture or partnership in which each business has at least a 40% interest and (2) any person that does business in California and that voluntarily certifies to the CPPA that it is in compliance with and agrees to be bound by the CCPA.[9]

Broadly, the CCPA grants rights to California consumers (i.e., residents) and imposes obligations on covered entities regarding how they process 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.[10]

Specifically, the CCPA defines personal information as information that "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, unique personal identifiers (including a device identifier; an Internet Protocol address; and cookies, beacons, pixel tags, mobile ad identifiers, or similar technology), 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 is an area where the CCPA appears to go beyond the GDPR, which generally focuses only on individuals. There are a few key exclusions, however, of which businesses should be aware. For example, although the CCPA previously did not apply to personal information collected in the human resources or business-to-business contexts, these exemptions expired on January 1, 2023.

In determining the most efficient use of a 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. Prior to the CPRA, violations of the CCPA's substantive provisions were enforceable by California's Office of the Attorney General. The CPRA, however, established the CPPA to enforce the law.[11]

The CCPA fixes statutory damages of $2,500 for each violation, or $7,500 for each intentional violation, with the CPPA issuing these fines.[12] Although the CCPA previously provided businesses a 30-day cure period before fines could be assessed, the CPRA does not guarantee a cure period and instead gives the CPPA discretion regarding whether to provide a business with an opportunity to cure an alleged violation.

In addition to attorney general enforcement, the CCPA includes a limited private right of action for Californians in certain 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 or actual damages, whichever is greater.[13] 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 scope of the CCPA. For example, the law does not restrict a business's ability to collect, sell, or share 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 certain other federal regulations, including the Health Insurance Portability and Accountability Act of 1996, the Gramm–Leach–Bliley Act, the Fair Credit Reporting Act, or the Driver's Privacy Protection Act.[14]