



News & Types: 商事／競争／取引関連情報

カリフォルニア州消費者プライバシー法の概要

12/19/2019

Practices: 商事／競争／取引, 知的財産テクノロジー

The California Consumer Privacy Act, or “CCPA” for short, is a comprehensive data privacy law which was enacted in June 2018 and will go into effect on January 1, 2020 that will have broad-reaching implications for businesses around the world that do business in California. The CCPA is grounded in the California Constitution’s right of privacy, and is a specific response to intensifying concerns about California residents’ ability to properly protect their privacy in a world in which technology and the collection and sale of personal information increasingly drive commerce.

This Article is intended to provide a brief overview of some of the CCPA’s key provisions and how businesses can start preparing for CCPA compliance on Day One. However, it should be noted that, as of the date of this article, some aspects of the CCPA, which may affect its scope or enforceability, have not yet been finalized.

WHO AND WHAT DOES THE CCPA APPLY TO?

At a fundamental level, the CCPA regulates how “businesses” handle the “personal information” of “consumers.” The CCPA applies to businesses that are for-profit entities that (1) do business in California, (2) collect the “personal information” of “consumers,” and (3) meet one of the following three thresholds: (i) have annual gross revenues in excess of \$25 million; (ii) alone or in combination, buy, receive, sell or share the personal information of 50,000 or more California residents, households, or devices; or (iii) derive 50% or more of its annual revenues from selling California residents’ personal information. Regarding the \$25 million revenue requirement in (i) above, the CCPA does not explicitly state that it is limited to California-derived revenue, and for that reason it should be assumed it refers to worldwide revenue.

A “business” under the CCPA also includes “any entity that controls or is controlled by” a business and “that shares common branding” with that business. The CCPA defines “control” or “controlled” as a matter of ownership, voting power, or majority board control. “Common branding” means “a shared name, servicemark, or trademark.” Because the CCPA does not distinguish between domestic and foreign entities under its definition of “business,” it appears that a foreign parent company with a controlling interest in a U.S.-based subsidiary subject to the CCPA with common branding would itself also be subject to the CCPA.

The CCPA’s protections apply to “consumers,” whom the CCPA defines as individuals who reside in California. This broad definition of “consumers” covers not only a business’s individual customers, but also the business’s employees and its business contacts who reside in California.

The “personal information” subject to the CCPA consists of any 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.” Some categories of consumer data constituting personal information

include, but are not limited to, “personal identifiers” such as an individual’s name, postal address, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers. Personal information can also include “commercial information,” which includes records of products or services purchased, obtained, or considered, or other purchasing histories or tendencies. Further categories of personal information include biometric information, internet or other electronic network activity information such as browsing history and search history, and professional or employment-related information.

WHAT DOES THE CCPA DO?

The CCPA creates certain rights for consumers regarding how their personal information is handled by businesses. Under the CCPA, consumers have the right to:

1. Know what categories of personal information a business collects about consumers, and if that information is shared with other entities. Consumers can submit “verifiable consumer requests” to a business, which require the business to provide more information on and produce to the consumer the specific pieces of personal information that the business has collected on that consumer.
2. Request that the business delete the personal information it holds about the consumer. However, this right is subject to certain exceptions under which a business can refuse a consumer’s request for deletion.
3. “Opt out” of a business’s sale of the consumer’s personal information to third parties. In this case, “sale” is defined to include the transfer of personal information for “monetary or other valuable consideration.”
4. Non-discrimination for exercising any of a consumer’s rights under the CCPA.

In addition to these rights, the CCPA also provides a private right of action to consumers in the event that a business sustains a data breach that discloses personal information. Under the private right of action, consumers may recover statutory damages on an individual or class action basis in an amount not less than \$100 and not greater than \$750 per consumer per incident or actual damages, whichever is greater.

WHAT DOES THE CCPA REQUIRE BUSINESSES TO DO?

To ensure the above-named rights of consumers are upheld, the CCPA requires all covered businesses to disclose the following information to consumers at or before the point that personal information is collected:

- What categories of personal information are collected, and for what purposes the personal information will be used.
- Whether the business sells personal information or discloses personal information for a business purpose to a third party, and if so, what categories of personal information it sells/discloses and the categories of third parties to whom it sells/discloses personal information.
- That consumers may request a disclosure of the specific pieces of personal information the business has collected on the consumer within the previous 12 months.
- That consumers have the right to request deletion of their personal information collected by the business, subject to certain exceptions.

- That consumers will not be discriminated against for exercising any of their rights under the CCPA.

Additionally, businesses that sell consumer information must offer consumers the right to “opt-out” of such sales.

Businesses that do not directly sell to individual consumers, but that have employees or business contacts in California, will have slightly reduced obligations during the first year of the CCPA (until January 1, 2021) concerning the personal information collected from these individuals. For example, although a business must still inform its California employees at or before the point of collection what categories of personal information are collected and for what purposes it will be used, the employees will not have the right to request deletion of their personal information. Similarly, a business’s California business contacts will have the right to “opt-out” of sales of their personal information, but not to delete that information. Both employees and business contacts may still sue the covered business in the event of a data breach, however.

WHAT CAN BUSINESSES DO TO PREPARE FOR THE CCPA?

Covered businesses should, at a minimum, take action to (1) determine what personal information they collect from consumers, their purpose for collecting the information, and what data security practices are in place to protect the information; (2) make the necessary disclosures regarding how they handle consumers’ personal information in a CCPA Privacy Notice; (3) provide methods for consumers to make requests, through a website form or email address and (unless the business interacts with consumers strictly online) a toll-free telephone number, for disclosure and deletion of the specific pieces of personal information the business has collected on them; and (4) develop internal procedures for evaluating and responding to consumers’ requests for disclosure and deletion. Furthermore, businesses are encouraged to review any third-party vendor contracts involving data sharing to ensure that each vendor is also compliant with the CCPA.

As mentioned in the introduction of this Article, certain aspects of the CCPA have not yet been finalized. For instance, the California Attorney General is currently in the process of finalizing regulations to provide further guidance regarding compliance with and enforcement of the CCPA. Enforcement of the CCPA will not begin until six months after the final regulations are published or July 1, 2020, whichever is sooner. Also, the CCPA has already been amended several times since its enactment in June 2018, and further amendments may be coming in the near term. Businesses should continue to closely monitor these ongoing developments and ensure that any new developments in the CCPA are accounted for in their own CCPA compliance plans.

CONCLUSION

In closing, the CCPA’s broad provisions extend to cover businesses with nearly any kind of business presence in California, regardless of whether they traditionally derive revenues from the sale of their customers’ personal information. With the January 1, 2020 date fast approaching, businesses will need to start taking steps now to prepare for being CCPA-compliant from Day One.