

CENTURY CITY LAWYER

A PUBLICATION OF THE CENTURY CITY BAR ASSOCIATION

March 2019 Issue

[BACK TO NEWSLETTER](#)

Businesses Will Have Numerous New Privacy Obligations Under the CCPA

By: Starr Turner Drum



This past summer, California passed one of the strictest data privacy laws in the world, set to come into effect in stages between January 1, 2020 and July 1, 2020. The California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (the “CCPA”), is designed to give California residents – termed “consumers” – more control over the collection, use, and sharing of their personal information. “Personal information” is defined broadly in the CCPA as

“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.”

Applicability

The CCPA applies to for-profit entities that collect consumer personal information, determine the purpose and means of processing consumer personal information, and either:

- have annual gross revenues of over \$25 million;
- buy, receive, sell, or share for commercial purposes the personal information of more than 50,000 consumers, households, or devices annually; or
- derive more than 50 percent of their annual revenue from selling consumer personal information.

The predominant requirements of the CCPA relate to disclosure obligations and responding to consumer individual rights requests.

Disclosure Obligations

The CCPA mandates businesses provide specific disclosures in an online privacy policy:

- identifying the rights available to consumers under the CCPA;
- identifying the designated methods for consumers to submit individual rights requests;
- describing consumers’ right to opt out of the sale of their personal information and including a link to an online opt out mechanism;
- listing the categories of personal information collected by the business in the past twelve months;

- listing the categories of personal information sold by the business in the past twelve months (or if the business has not sold personal information in the past twelve months, a disclosure of that fact);
- listing the categories of personal information disclosed about consumers for a business purpose in the past twelve months (or if the business has not disclosed consumer’s personal information for a business purpose in the past twelve months, a disclosure of that fact).

Online privacy policies must be updated at least once every twelve months.

Individual Rights

Like the recently-enacted European General Data Protection Regulation (“GDPR”), the CCPA gives consumers individual rights to access, export, delete, and obtain information about their personal information. However the applicability and exceptions for individual rights differ substantially between the two laws. Importantly, under the CCPA businesses must facilitate consumers’ individual rights requests by implementing two or more submission mechanisms, one of which must be a toll-free telephone number.

For access requests under the CCPA, businesses will be required to deliver consumers their requested information either in hard copy by mail or electronically. If the information is provided electronically, it must be in a portable and, to the extent feasible, readily useable format.

Deletion requests under the CCPA apply only to personal information collected from the consumer—not to personal information collected from third parties. Unless subject to an exemption, businesses that receive deletion requests must delete the consumer’s information from their records and must direct any service providers to delete the requesting consumer’s personal information, as well.

Businesses must provide a compliant response within 45 days after receiving a consumer individual rights request. If the request is complex or the number of requests received is voluminous, businesses can have up to 90 additional days to respond, but must still notify the consumer of the reason(s) for the delay within 45 days of the initial request.

The CCPA also provides consumers a “right to opt out” of the sale of their personal information. Businesses that sell personal information must maintain a “clear and conspicuous” link on their homepage (or on a separate homepage to which California consumers are automatically directed), in online privacy policies, and in any other online California-specific description of consumer privacy rights titled “Do Not Sell My Personal Information.” The link must give consumers a description of their opt-out rights and enable them to opt out of the sale of their personal information.

Additionally, businesses cannot sell personal information collected from children under 16 unless they (or their parents for children under 13), have affirmatively authorized (i.e. opted-in to) the sale of their personal information.

Businesses may not deny goods or services, charge different prices for goods or services, provide different quality levels of goods or services, nor otherwise discriminate against consumers who exercise their individual rights under the CCPA. However, businesses are permitted to offer compensation or other financial incentives to consumers related to the collection, sale, or deletion of their personal information.

Enforcement

Regulatory penalties for violations of any provision of the CCPA can be up to \$2,500 for each unintentional violation and up to \$7,500 for each intentional violation.

Consumers can bring civil suits under the CCPA where their personal information “is subject to an unauthorized access and exfiltration, theft, or disclosure.” Statutory civil penalties for breach can be between \$100 and \$750 per consumer per incident or actual damages, whichever is greater.

Looking Ahead

The CCPA requires the California Attorney General to adopt additional regulations to further the purpose of the law before it goes into effect. The AG is conducting a series of public forums across the state in early 2019 to obtain feedback on the rulemaking process. Lawmakers have indicated that further amendments to the CCPA are forthcoming. Additionally, there is substantial congressional activity surrounding the enactment of a federal consumer privacy law that could preempt the CCPA. However, as businesses that have recently been through GDPR initiatives know, legal and technical implementations take time. Therefore, business should evaluate whether the CCPA applies to their operations and, if it does, begin the compliance process while staying up-to-date the law’s developments.

Starr Drum is a shareholder at Maynard, Cooper & Gale. Her practice focuses on global privacy and data security compliance. She can be reached at sdrum@maynardcooper.com.