
California Enacts Sweeping Consumer Privacy Law

JULY 2, 2018

On June 28, 2018, California enacted the [California Consumer Privacy Act of 2018](#) (CCPA), a sweeping privacy law that provides consumers with broad notice, access, and deletion rights concerning many types of personal information and permits consumers to opt-out of the sale of their personal information. The law, introduced and passed within a week in order to head off an even stronger ballot initiative, takes effect on January 1, 2020, and applies to the hundreds of thousands of businesses above certain size thresholds that do business in California and that collect, sell, or disclose for business purposes consumers' personal information.¹

Key Provisions

The CCPA's key provisions include:

Disclosure of personal information collected. Covered businesses that collect personal information must, in response to a verified request from a consumer, disclose:

- (1) the categories of personal information the business has collected about that consumer;
- (2) the categories of sources from which the personal information is collected;
- (3) the business or commercial purpose for collecting or selling personal information;
- (4) the categories of third parties with whom the business shares personal information; and
- (5) the specific pieces of personal information the business has collected about that consumer. §§ 1798.110, 1798.130(a)(3).

Disclosure of personal information sold, or disclosed for a business purpose. Covered businesses that sell personal information or that disclose it for a business purpose, must, in response to a verified request from a consumer, disclose:

- (1) the categories of personal information that the business collected about the consumer;
- (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was

sold; or if the business has not sold consumers' personal information, it shall disclose that fact;

(3) the categories of personal information that the business disclosed about the consumer for a business purpose; or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact. §§ 1798.115, 1798.130(a)(4), (a)(5)(C).

Deletion of personal information. Covered businesses must, in response to a verified request, delete personal information of the requester and make sure service providers do as well, with certain exceptions. § 1798.105(a), (c)-(d).

Opt-out for sales of personal information. Covered businesses may not sell personal information without giving notice and a chance for affected consumers to opt out. Covered businesses must place a link on their website homepage titled "Do Not Sell My Personal Information" that redirects to a webpage that enables a consumer to opt-out of the sale of the consumer's personal information. The business cannot require consumers to create an account in order to opt-out of the sale of their personal information §§ 1798.120, 1798.115(d), 1798.135.

Opt-in for sales of personal information of those less than 16 years of age. Covered businesses may not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. § 1798.120(d).

Enhanced disclosures of privacy rights and practices concerning collection, sale, and disclosure of personal information. Covered businesses must disclose in their online privacy policy or California-specific description of consumer privacy rights consumers' rights under the CCPA and the methods for exercising those rights, as well as the categories of personal information the business collects, sells, or discloses for business purposes. The notices must be updated annually. These requirements extend beyond current privacy policy requirements set forth in the California Online Privacy Protection Act. § 1798.130(a)(5).

Methods for making verified consumer requests. Covered businesses are required to provide two or more methods for consumers to submit requests to exercise their rights as described above, including at a minimum a toll-free telephone number, and, if the business maintains a website, a website URL. Businesses must respond to requests for information within 45 days of receipt (though extensions are allowed under certain circumstances), must respond free of charge, and the disclosure must cover the 12 months preceding the request. The disclosure must be made in writing by mail or electronically at the consumer's option, and in a readily useable format to permit the consumer to transfer the information to another entity without hindrance. § 1798.130(a)(1)-(5).

Broadened definition of "personal information." As compared to the California On-line Privacy Act, the CCPA significantly broadens the definition of personal information to mean "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.” The definition includes, among other things: names and other identifiers such as IP addresses; account names; driver’s license and passport numbers; commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; biometric information; internet browser and search history, interaction with a website, application, or advertisement; location information; professional or employment-related information; educational information; and inferences drawn from any of the above information to create a profile about a consumer. § 1798.140(o)

Deidentified or aggregated information. The CCPA’s requirements do not apply to consumer information that is deidentified or in the aggregate. § 1798.145(a)(5).

Discrimination prohibited; financial incentives permitted. Covered businesses are prohibited from charging consumers who opt-out a different price or providing a different quality of goods or services, but businesses may offer financial incentives for the collection, sale, or retention of personal information on an opt-in basis. § 1798.125.

No contractual waiver. Consumers cannot contractually waive their rights, as any provision to that effect in a contract shall be deemed contrary to public policy and void. § 1798.192.

Limitations and relation to other laws. Obligations under the CCPA shall not restrict a business’s ability to comply with federal, state, or local laws, comply with civil, and criminal investigations and process, cooperate with law enforcement, or exercise or defend legal claims. The CCPA also does not apply with respect to personal information collected, sold, or for business purposes disclosed under certain federal laws, including protected health information under HIPAA and the HITECH Act and consumer reports under the Fair Credit Reporting Act. The CCPA also does not apply to personal information collected, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or Driver’s Privacy Protection Act “if it is in conflict with that law.” § 1798.145.

Penalties. The California Attorney General may enforce the CCPA’s privacy provisions. Violations carry penalties of up to \$2,500 per violation and up to \$7,500 for intentional violations. § 1798.155.

Private right of action for certain data breaches. Consumers whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to maintain reasonable security procedures appropriate to the nature of the information are afforded a private right of action (a) to recover damages in an amount not less than \$100 and not greater than \$750 per consumer per incident or actual damages, whichever is greater; (b) injunctive or declaratory relief; and (c) any other relief the court deems proper. In assessing the amount of statutory damages, the court is directed to consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant’s misconduct, and the defendant’s assets, liabilities, and net worth.

Consumers seeking to bring an action must provide the prospective defendant with 30 days’ written notice, identifying the specific provisions the consumer alleges have been or are being violated. In

the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, the consumer is not entitled to bring the action, unless the prospective defendant continues to violate the law. No such notice, however, is required prior to an individual consumer's initiating an action solely for actual monetary damages.

In order to bring an action, a consumer must notify the Attorney General within 30 days that the action has been filed. The Attorney General, upon receiving such notice shall, within 30 days, either (a) notify the consumer of the Attorney General's intent to prosecute an action; if the Attorney General does not prosecute within six months, the consumer may proceed with the action; or (b) refrain from acting within the 30 days, allowing the consumer to proceed. or notify the consumer that the consumer shall not proceed. § 1798.150.

Rulemaking. On or before January 1, 2020, the California Attorney General shall undertake a notice-and-comment rulemaking process to address implementation of the CCPA, including, among many other subjects, (1) updating as needed additional categories of "personal information" in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns; (2) updating as needed the definition of "unique identifiers" to address changes in technology, data collection, obstacles to implementation, and privacy concerns;² (3) adding additional categories to the designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business; (4) establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights. § 1798.185.

Conclusion

The CCPA is one of the most significant privacy laws ever enacted in the United States. It was enacted extremely quickly with little input from the business community. The business community will likely lobby for amendments to the CCPA before it takes effect, especially with respect to the private right of action, and, as such, the law that takes effect in 2020 may prove to be different than the law that was enacted last week. The required rulemaking process will also allow input from affected companies, and the delayed effective date gives companies some time to prepare for compliance. But the CCPA establishes substantial new obligations, in terms that are not always clear. Affected companies will need to begin assessing their responsibilities and methods for fulfilling them promptly.

1. See Rita Heimes & Sam Pfeifle, IAPP Privacy Advisor, *New California Privacy Law to Affect More than Half a Million US Companies* (July 2, 2018). The thresholds are: (a) has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted for inflation; (b) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (c) Derives 50 percent or more of its annual revenues from selling consumers' personal information. Cal. Bus. & Prof. Code § 1798.140(c)(1). All section references in text are to the Cal. Bus. & Prof. Code.

2. The law defines “unique identifiers” and “personal unique identifiers” as “a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.” “For purposes of this subdivision, ‘family’ means a custodial parent or guardian and any minor children over which the parent or guardian has custody.” 1798.140(x)