HUSCH BLACKWELL

California Consumer Privacy Act Guidebook

David M. Stauss, CIPP/US, CIPT, FIP
Partner
Husch Blackwell

Table of Contents

*The Certified Information Privacy Professional / United States (CIPP/US), Certified Information Privacy Technologist (CIPT) and Fellow of Information Privacy (FIP) certifications, are conferred by the International Association of Privacy Professionals. Colorado does not certify lawyers as specialists in any field.

HUSCH BLACKWELL

What is the California Consumer Privacy Act of 2018?

In July 2018, the California legislature enacted a first-in-the-nation consumer privacy act entitled the California Consumer Privacy Act of 2018 (CCPA). The CCPA is notable both because it provides California residents with significant privacy-related rights and because it will require covered entities to undertake significant compliance efforts.

What Entities Are Subject to the CCPA?

The CCPA applies to "businesses," which is defined as for-profit legal entities that collect consumers' personal information, or on behalf of which such information is collected, and that alone or jointly with others, determine the purposes and means of the processing of the personal information and that either:

$25,000,000

Have annual gross revenues in excess of $25,000,000

50,000

Alone or in combination, annually buy, receive for the business's commercial purpose, sell, or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices

50%

Derive 50% or more of their annual revenues from selling consumers' personal information

Because the law defines "consumer" as a California resident, the second and third categories should be interpreted to relate to California—and not nationwide—numbers.

The definition of business also includes any entity that controls or is controlled[1] by a business that shares "common branding"[2] with the business.

[1] "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

[2] "Common branding" means a shared name, servicemark, or trademark.

Are There Any Exceptions?

Yes. For example, the CCPA exempts personal information that is subject to HIPAA and the Gramm-Leach-Bliley Act. However, the exemptions do not apply to other personal information maintained by a business. Therefore, businesses need to perform a gap analysis to identify what personal information is covered by the CCPA.

Does the CCPA Apply to Businesses That Do Not Have a Physical Presence in California?

Yes. The definition of "business" states that it is any entity that "does business in the State of California." This would include online retailers that sell to California residents but do not have a physical presence in the state.

Who Holds the Rights?

Short answer: California residents.

Long answer: The CCPA applies to "consumers," which is defined as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." 18 CCR § 17014 defines "resident" as "(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose." The regulation provides guidance on what constitutes a "temporary or transitory purpose."

For purposes of complying with the CCPA, businesses should keep in mind that the law's definition is focused on current California residency ("who is a California resident") and not on the individual's residency when he or she became known to the business. The CCPA is silent on how businesses will verify residency other than to charge the Attorney General's office with promulgating regulations. Cal. Civ. Code § 1798.185(a)(7) ("On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations for the purposes of . . . [e]stablishing rules and procedures . . . to govern a business's determination that a request for information received by a consumer is a verifiable request . . . .").

To What Types of Information Does the CCPA Apply?

Short answer: Almost anything.

Long answer: The law defines "personal information" incredibly broadly as 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." The law lists the following categories of information that qualify as personal information:

- Identifiers such as a real name, alias, postal address, unique personal identifier,[3] online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Any categories of personal information described in Section 1798.80(e).[4]
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.[5]
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

If that list is not already long enough, the Attorney General's office has the authority to identify additional categories of personal information as part of its rulemaking authority.

Conversely, personal information does not include publicly available information, which is information that is lawfully made available from federal, state or local government records.

[3] "Unique identifier" or "Unique personal identifier" is defined to mean "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." "Probabilistic identifier" is defined to mean "the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.".

[4] Section 1798.80(e) defines "personal information" to mean "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

[5] "Biometric information" is defined to mean "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."

What Privacy Rights Does the CCPA Provide to California Residents?

The CCPA requires entities doing business in California to:

- Make specific disclosures on their web pages about what "personal information" they collect[6] about consumers (i.e., California residents) and how that information is shared with third parties.
- Respond to verifiable consumer requests to provide the specific pieces of personal information the business has collected on the consumer for the twelve-month period prior to the request.
- Provide an online mechanism for consumers to opt-out of having their personal information "sold" to third parties.
- Allow consumers to request that their personal information be deleted.
- Not discriminate against consumers for exercising their rights.

What is a Verifiable Consumer Request?

The CCPA requires businesses to make available two or more designated methods for submitting requests for information. This must include a toll-free telephone number and a web site address (if the business maintains a website). The requested information must be provided to the consumer, free of charge, within 45 days of the request. The business can extend this time period by another 45 days if it provides notice to the consumer.[7]

How Does the Right to Access Personal Information Work?

The CCPA grants consumers the right to make verifiable requests to businesses to disclose to the consumer the "categories and specific pieces of personal information" that the business has collected about the consumer. A business must provide the information it has collected for the prior twelve months and free of charge.

The method by which businesses must provide this information is unclear. Section 1798.100(d) states that the "information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance." In turn, Section 1798.130(a)(2) states that the disclosure "shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without

[6] "Collects," "collected," or "collection" is defined to mean "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."

[7] It is worth noting that another provision of the CCPA states that the deadline to respond can be "extended up to 90 additional days where necessary."

hindrance." Synthesizing those two provisions, businesses can respond to verified requests through the consumer's online account (if one exists) or provide the consumer the option of having the information provided by mail or electronically.

The CCPA also grants consumers the right to request that a business disclose:

- The categories of personal information it has collected about that consumer;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting or selling personal information; and
- The categories of third parties with whom the business shares personal information.

"Business purposes" and "commercial purposes" are defined terms. For example, commercial purposes "means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction."

What about Businesses That "Sell" Personal Information to Third Parties?

Businesses that "sell" personal information to other entities are subject to a number of restrictions and disclosure obligations. Importantly, the CCPA defines "sell" to include any transfer of personal information for monetary or "other valuable consideration."[8] Unfortunately, the CCPA does not define what constitutes "other valuable consideration." A broad reading could include almost any transfer of personal information when a business receives any type of benefit.

Upon request by a consumer, a business that sells personal information to "third parties" must 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; and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Consumers also have the right to opt-out of the selling of personal information to third parties. (Additional restrictions apply if the consumer is less than 16 years old.)

[8] "Sell" is defined to mean "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

How Does the "Right to be Forgotten" Work?

The CCPA states that consumers "shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer." A consumer will exercise this right by making a verifiable request. The business must delete the consumer's personal information from its records "and direct any service providers to delete the consumer's personal information from their records."

But the "right to be forgotten" is not absolute, and the CCPA provides that a business does not have to honor such a request if the personal information is necessary to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- Comply with a legal obligation.
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

What is the Difference between a "Third Party" and "Service Provider"?

One significant distinction the CCPA creates is between "third parties" and "service providers." For example, Section 1798.110(a)(4) states that a consumer has the right to request that a business disclose the categories of third parties (not service providers) with whom the business shares personal information. Further, the opt-out provision applies to the sale of personal information to third parties (not service providers). Conversely, a business that receives a request to be forgotten must direct any service providers (but not third parties) to delete the consumer's personal information.

The CCPA defines "service provider" to mean a for-profit legal entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."

In turn, "third party" is defined as a person who is not any of the following:

- The business that collects personal information from consumers under this title.
- A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:
  - Prohibits the person receiving the personal information from:
    - Selling the personal information.
    - Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
    - Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
  - Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

Will My Business Need to Revise its Online Privacy Notice?

Yes. The law requires entities to list specific information in their online privacy policies, including:

- a description of the consumers' rights as discussed above;
- a list of the categories of personal information that the business has collected about consumers in the preceding 12 months;
- a list of the categories of personal information it has sold about consumers in the preceding 12 months; and
- a list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months.

If applicable, a business also must provide a clear and conspicuous link on its homepage titled "Do Not Sell My Personal Information," which should lead to a web page enabling a consumer—or a person authorized by the consumer—to opt out of the sale of the consumer's personal information. That information also should be provided in the business's online privacy policy.

How Will the CCPA Be Enforced?

The California Attorney General's office is charged with enforcing the CCPA's privacy-related rights and is authorized to seek statutory damages of $2,500 for each violation or $7,500 for each intentional violation.[9]

What about the Statutory Damages Provision?

The CCPA establishes a private right of action for data breaches caused by a failure to implement and maintain reasonable security procedures and practices. The CCPA provides for statutory damages ranging between $100 and $750 "per consumer per incident." The CCPA is the first legislation in the country to provide for private litigant statutory damages for data breaches. This will allow plaintiffs' attorneys to bring class actions for significant statutory damages as well as attorneys' fees and costs.

[9] The California Attorney General's office has requested that the legislature amend the CCPA to allow private litigants to sue for violations of the privacy-related rights and not just for data breaches.

What are Some Relevant Dates?

January 1, 2019	Twelve-month lookback period begins
January 8 2019 to March 5, 2019	Attorney General's office hosts public forums to solicit comments on regulations
March 8, 2019	Deadline to submit written comments to the Attorney General's office
September 13, 2019	Last day for any bill to be passed by the California legislature prior to interim recess
October 13, 2019	Last day for Governor to sign or veto bills passed on or before September 13
Fall 2019	Proposed regulations published by Attorney General's office
Fall 2019 to Winter 2020	Anticipated comment period on proposed Attorney General regulations
January 1, 2020	CCPA becomes operative
July 1, 2020	Attorney General's office may not bring enforcement actions until six months after the publication of final regulations or July 1, 2020, whichever is sooner