The California Consumer Privacy Act Q & A

Q: What is the California Consumer Privacy Act (CCPA)?

A: CCPA is a law that aims to protect California consumers' rights by providing them with more control and choice with respect to their personal information and requiring companies to be more transparent in their handling of personal information.

Q: When does CCPA go into effect?

A: CCPA goes into effect on January 1, 2020. SB 1121, enacted in August 2018, made several changes to the law. Additional amendments are anticipated in October 2019, as discussed in more detail below. The law's 12-month look back period requires businesses to facilitate California consumers' rights regarding personal information collected in the 12 months prior to the law's effective date.

California's attorney general is charged with promulgating regulations to implement the law; the deadline for promulgation of the regulations is July 1, 2020.

Recently introduced bills seek to amend the CCPA. Legislative efforts include expanding the private right of action for any alleged violation of the law (not just a data breach).

Q: Who is regulated by the CCPA?

A: CCPA applies to for-profit entities that collect CA consumers' personal information, determine the purposes and means of processing that personal information, do business in the state of California, AND meet any one of the following thresholds:

(i) annual gross revenue in excess of $25 million (regardless of where it's earned);
(ii) buys, sells, or shares for commercial purposes the personal information of 50,000 or more CA consumers, households, or devices per year; or
(iii) 50% or more of annual revenues from selling consumers' personal information.

CCPA also applies to entities that control or are controlled by an entity that meets one of the above criteria and shares common branding.

There's no requirement for the business to deal directly with consumers for the law to apply. Additionally, certain rights within CCPA apply to businesses with respect to employees and/or their business contacts who are California residents. For both employees and business-to-business contacts, the law's exclusion of these two groups from certain rights sunsets after 1 year. If not directly subject to CCPA, a business may be subject to its requirements indirectly

through contract. Businesses subject to the CCPA must require that their third-party service providers use information in a way that allows the business to be compliant.

Q: Who is protected by the CCPA?

A: A "consumer" is any natural person who is a California resident (all individuals in California for other than a temporary or transitory purpose, and every individual domiciled in California who is outside the state for a temporary or transitory purpose). Geographic location may not be a reliable determinant of who is a "consumer" under CCPA, since California residents may be outside the state when interacting with a business.

AB 25, legislation passed in 2019 but not yet signed into law by the governor, modified requirements related to employee data. This means job applicant and employee data (if used solely for a business purpose, employee emergency contact data, or information used for benefits administration) is excluded from all CCPA rights, except the right to disclosure of usage of the information (798.100) and the data breach provisions (798.150). If an entity has employees or job applicants in California, they will have to develop employee disclosures and consider whether employee information is used for any purpose outside the limited uses of employee data set by AB 25.

Similarly, AB 1355, also passed in 2019 but not yet signed into law by the governor, modifies the CCPA to exclude personal information collected within the context of business-to-business relationships. Specifically, the amendment excludes personal information reflecting a communication or transaction between a business and consumer, where the consumer is acting as an employee, director, owner, officer or contractor of a company or government agency and the communications or transactions are in the context of that company or government agency conducting due diligence or receiving a product or service from the business.

Q: What information is protected by the CCPA?

A: "Personal information" is 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." Examples include:

- Identifiers such as name, address, online identifier, IP address, email address, account name, SSN, driver's license number, passport number
- Education, medical, or health insurance information
- Financial information, including personal property records, products or services purchased (or considered), and other consuming histories or tendencies
- Internet activity, including web browsing history
- Professional or employment-related information

- Geolocation data
- Inferences drawn from the consumer's information to create a consumer profile

Publicly available information from federal, state, or local government records is excluded from the definition of "personal information," when the information is used by the business for a purpose compatible with the purpose for which the data was made publicly available. AB 874, passed in 2019 but not yet signed by the governor, eliminates the qualifier regarding compatible purpose from the definition of "publicly available." Another modification by AB 874 (not yet signed into law by the governor) is to exclude deidentified or aggregate consumer information from the definition of "personal information."

Additionally, personal information collected and sold outside of California is excluded, if every aspect of that commercial conduct takes place wholly outside of California. To be exempt, the information must be collected while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.

Q: Are there exemptions from CCPA?

A: CCPA provides exemptions for personal information collected "pursuant to" the federal Gramm-Leach-Bliley Act (GLBA). GLBA requires that financial institutions (including insurers and providers of settlement services) provide disclosures regarding privacy practices, restricts sharing of personal information by financial institutions, and requires that financial institutions adopt safeguards to protect personal information.

The interplay between GLBA and the CCPA will require a detailed analysis, including which information is afforded the benefit of the exemption and which is not. CCPA contains a more expansive definition of "personal information" (including geolocation data, web browsing history, employment data, online identifiers, etc.), and not all information collected by a financial institution is collected "pursuant to" the GLBA .

For instance, GLBA does cover personal information collected by a settlement agent for a residential real estate settlement and personal information collected by a title agent or insurer for issuance of a title insurance policy covering residential property. A consumer's personal information collected in the context of a commercial transaction (including where residential property is purchased or sold for a commercial purpose) would not fall within the GLBA exemption, as GLBA covers only personal information provided to obtain a financial product or service *for personal or household use*.

Creditworthiness information subject to the Fair Credit Reporting Act (FCRA) and sold to or from a consumer reporting agency is also exempt from CCPA. Additionally, the CCPA "does not restrict" a business's ability to defend or to exercise legal claims or cooperate with government authorities.

These exemptions do not impact consumers' private right of action under CCPA in the event of a data breach.

CCPA contains other exemptions set forth in Civil Code Section 1798.145(a). Pursuant to this Code Section, CCPA cannot restrict a business's ability to comply with laws or legal process, cooperate in good faith with law enforcement, or exercise and defend legal claims, among other exemptions.

Q: What consumer rights are created by the law?

A: CCPA grants consumers:

- right to access personal information collected by the business;
- right to require the business's disclosure regarding collection, sale, and other disclosure of the consumer's personal information;
- right to deletion of personal information by the business and its vendors;
- right to opt out of the sale of personal information; and
- right to equal service and price, even if the consumer exercises his or her CCPA rights.

Q: What is the right to access?

A: CCPA allows consumers the right to access a copy of the personal information that the business collected about that consumer, free of charge. The information must be "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." The CCPA requires a business to provide two or more designated methods to receive requests for access, including a toll-free number and, if the business has a website, a website address. The AG must promulgate regulations to clarify what qualifies as a "verifiable" consumer request.

Q: What is the right to disclosure?

A: CCPA gives consumers the right to know what personal information the business collects, sells, and discloses about them, including the specific pieces of personal information the business has collected and the categories of third parties who purchased or received the information. Businesses must provide this information for the preceding 12 months in response to a consumer request, disclosing the categories of sources from which the data is collected, the business purpose(s) for collecting or selling the data, and the categories of third parties with which the data was shared.

A business is not required to provide the information more than twice in a 12-month period. The business has 45 days to respond to the request, at no charge to the consumer. The response time can be extended by up to 90 additional days where necessary, and the business must notify the consumer of the extension and the reason for it. In the event the business does not take action on the consumer request, it must advise the consumer of the reasons for not taking action within the 45-day period.

Beyond the specific consumer-requested disclosures, the business must also provide notice, before or at the point of collection, about what categories of personal information the business collects and what it intends to do with such information. A business may not collect additional categories of personal information or use collected personal information for unrelated purposes without providing notice.

Q. What is the right to delete?

A: A consumer can request that a business and its service providers delete the consumer's personal information. Exceptions to this requirement allow a business to keep the information if the data is necessary to protect against fraud or other illegal activity, to complete the requested business transaction, to comply with a legal obligation, or to enable internal uses that are reasonably aligned with consumer expectation.

Q. What is the right to opt-out?

A: CCPA prohibits a business from selling a consumer's personal information unless the consumer is given a right to opt out, via a clear and conspicuous "Do Not Sell My Personal Information" link on the business's homepage. "Selling" means any disclosing or making available to another business or a third party for monetary *or other valuable consideration*.

If a consumer opts out, a business must immediately stop "selling" the consumer's personal information and cannot contact the consumer to request permission to sell their information for a 12-month period. If a consumer is under 16, the business must receive opt-in consent; under age 13 requires parental authorization.

Note that there are exemptions to the right to opt out. The broad GLBA exemption may apply, as well as the exemptions set forth in Civil Code Section 1798.145(a). Pursuant to this Code Section, CCPA cannot restrict a business's ability to comply with laws or legal process, cooperate in good faith with law enforcement, or exercise and defend legal claims, among other exemptions.

Q. What is the right to equal service?

A: A business cannot discriminate against a consumer because the consumer exercised their rights under the CCPA (for example, by providing a different product or price or refusing service). CCPA authorizes businesses to offer financial incentive programs for collection of personal information, so long as consumers give informed consent and can revoke consent at any time. Businesses can also charge different prices or offer different product levels if the difference is "reasonably related to the value provided to the [consumer] by the consumer's data." A technical correction introduced by AB 1355, which awaits action by the governor, replaces the word "consumer" with "business" in Section 1798.125.

Q. What obligations on the business does CCPA create?

A. To comply, a business must:

- **Provide a privacy policy**, updated annually and accessible on its website, that:
    - describes consumers' rights and at least two methods to submit requests;
    - lists the personal information categories the business has collected about consumers in the past 12 months;
    - provides separate lists of the personal information categories the business has sold or disclosed for business purposes in the past 12 months, or statements that it has not sold or disclosed any consumer information.
- **Implement procedures to respond to verifiable requests**, free of charge and within 45 days (45-day period can be extended to 90 days with notice to consumer), for:
    - access
    - deletion
    - opt-out, or
    - information about collection, disclosure, or sale of personal information
- **Train employees** responsible for handing consumer inquiries about the business's privacy practices and compliance requirements.
- **Not sell consumer information** unless the consumer has received notice and an opt-out opportunity.
- **Delete** consumer information on request unless there is a basis within the California law to retain.

Q: What are the costs of non-compliance?

A: CCPA gives consumers a private right of action where the consumers' data is breached as a result of a data breach arising from a business's failure to implement and maintain "reasonable and appropriate security procedures and practices."

Statutory damages are between $100 - $750 per California resident per incident, or actual damages, if greater. CCPA requires a consumer to notify a business 30 days before filing an action for statutory damages. If the violation is cured, no claim may proceed.

The California Attorney General has been authorized to enforce the law. Penalties for noncompliance are up to $2,500 per violation and $7,500 for intentional violations. Businesses will not be liable for CCPA violations of their service providers, provided that the business did not have actual knowledge or reason to believe that its service provider intended to violate the CCPA when it disclosed personal information to the service provider.

Q: What affirmative steps should be considered for compliance?

A: A company should consider taking the following steps to comply with the CCPA as currently drafted:

- **Determine law's applicability:** Consult with counsel or a compliance firm.
- **Conduct data mapping**. To respond to consumer requests and provide privacy disclosures, a company must know what personal information is collected about California residents, all locations where it is stored, and what third parties or services providers with which the information is shared. The Company must also be able to access and modify the information to respond to consumer requests. As the law is currently written, effective 1/1/2020, consumers can make requests about the information gathered about then over the *preceding* 12 months; thus, consumers can ask about any information collected in 2019.
- **Make necessary operational changes**, including:
    - Implementing process to provide the privacy notice "at or before the point of collection" of information from California residents, providing notice of the categories of personal information collected and for what purpose.
    - Set up a toll-free number and web address for consumers to submit verifiable consumer requests.
    - Designate individuals to verify the identity of consumers making requests and respond to verifiable consumer requests.
    - Implement data deletion capabilities (within 45 days of request) where data is not subject to an exception within the law.

- Enable consumers to opt in and opt out of the sale of their information and posting "Do Not Sell My Personal Information" on websites (if "sale" is contemplated).

- **Updating privacy policy.** CCPA requires that the privacy policy include a statement of the consumer's rights under the CCPA, one or more methods for submitting CCPA requests to the business, and other disclosures regarding information collection, sale, and disclosure required by CCPA. The policy must also be updated at least once every 12 months. Determine whether to maintain one privacy notice for California residents containing these disclosures and one for other consumers, or whether to maintain one universal privacy notice.

- **Employee training**. All individuals who are responsible for handling consumer inquiries about the business's privacy practices or compliance must be knowledgeable of the business's CCPA obligations and how to direct consumers to exercise their rights under the CCPA.

- **Security practices and procedures.** Mapping security practices and procedures to California requirements to ensure "reasonable security practices and procedures" are in place to avoid civil liability for a data breach.

- **Contract and vendor management**. CCPA only permits sharing personal information with service providers where notice to the consumer of the sharing is provided, the vendor's use is limited to the purposes for which is was provided, and the service provider contract includes certain identified conditions. Contracts should also contemplate compliance with rights to delete and disclose data and vendor's cooperation with those requirements, regardless of where the vendor is located.