Overview

For over two years businesses have spent considerable energy preparing for and complying with the California Consumer Privacy Act (CCPA). Businesses now have more work to do after California voters overwhelmingly approved Proposition 24, the California Privacy Rights Act (CPRA), which completely reshapes and overhauls the CCPA. Fortunately, most of the CPRA’s changes, including those that expand the rights of consumers and require affirmative action from businesses, do not become effective until January 1, 2023 and apply only to personal information collected on or after January 1, 2022. Nonetheless, given the scope of the changes effected by the CPRA, businesses should begin familiarizing themselves with the CPRA so they can sensibly plan to effectuate changes in their policies and procedures over the next year. Unfortunately, one of the most significant changes worked by the CPRA is the elimination of the 30-day “cure period” businesses have under the CCPA to fix any violations identified by the California Attorney General. This means a failure to comply with California’s complicated and often ambiguous requirements will likely become much more costly.

The CPRA’s most significant changes are summarized below.

Rights Related to “Sensitive Personal Information”
The CPRA creates a new category of data called "sensitive personal information" defined as:

- "Personal information that reveals":
  - "A consumer's social security, driver's license, state identification card, or passport number."
  - "A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account."
  - "A consumer's precise geolocation."
  - "A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership."
  - "The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication."
  - "A consumer's genetic data."
  - "The processing of biometric information for the purpose of uniquely identifying a consumer."
  - "Personal information collected and analyzed concerning a consumer's health."
  - "Personal information collected and analyzed concerning a consumer's sex life or sexual orientation."
  - "Publicly available" information is excluded from the definition of "sensitive personal information."

Notwithstanding this comprehensive definition, "sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer" is not subject to the special rights and restrictions associated with sensitive personal information under the CPRA and is to be treated only as personal information thereunder.

A consumer is able to limit the use of her or his sensitive personal information to purposes that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services" and other purposes authorized by the CPRA and regulations promulgated thereunder.

A consumer is also able to limit the disclosure of her or his sensitive personal information beyond certain purposes authorized by the CPRA and regulations promulgated thereunder.

A business that uses or discloses sensitive personal information beyond certain purposes authorized by the CPRA and regulations promulgated thereunder must provide notice to consumers that their sensitive personal information will be used or disclosed for additional purposes and that the consumer has the right to limit the use or disclosure of her or his sensitive personal information.

Point of Collection Notices and Retention of Personal Information

- The CPRA expands the existing point-of-collection notice requirement of the CCPA by requiring that a business disclose information about (1) the sale or sharing of personal information and (2) the retention of personal information. The CPRA also applies this expansive point-of-collection notice requirement to the collection of sensitive personal information.

- Additionally, "[a] business' collection, use, retention, and sharing of a consumer's personal information [must] be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

Agreement Related to the Sale or Disclosure of Personal Information

- When a business sells or discloses personal information to a third party, service provider, or contractor, it must enter into an agreement specifying that (1) the personal information is sold or disclosed "only for limited and specified purposes," (2) the third party, service provider, or contractor must comply with the CPRA, (3) the business is able to ensure that the third party, service provider, or contractor uses and transfers the personal information "in a manner consistent with the business' obligations under" the CPRA (4) the third party, service provider, or contractor must notify the business if they cannot meet their obligations under the CPRA, and (5) the business has "the right, upon notice...to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information."

New Consumer Rights

- The CPRA
A consumer is provided with the right to correct inaccurate personal information pursuant to a verifiable consumer request.

A consumer is provided with the right to opt-out of the sharing of their personal information with third parties (as opposed to the present CCPA right to opt out of only the “sale” of personal information). Notably, the definition of “sharing” includes the disclosure of personal information for “cross-context behavioral advertising, whether or not for monetary or other valuable consideration…” The CPRA defines “cross-context behavior advertising” as “the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.”

A consumer is able request that a business provide information in response to a request to know from beyond the 12 months preceding the request (which is the current period covered by such a request under the CCPA) “unless doing so proves impossible or would involve a disproportionate effort.” The CPRA does not specify how far back the consumer’s request may go, so it is possible a business will have to search as far back as it possibly can in response to such requests. However, this provision applies only to personal information collected on or after January 1, 2022 and does not “require a business to keep personal information for any length of time.”

A business must update their existing privacy policy disclosures to refer to these new rights afforded by the CPRA in addition to the right to receive a more expansive point of collection notice and the right to limit the use and disclosure of certain sensitive personal information.

Loyalty and Rewards Programs

- The CPRA explicitly states that it “does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with” the CPRA.

Sale of Personal Information

- Pursuant to one of the exceptions to the CCPA’s definition of sale of personal information, when “a consumer uses or directs a business to” either “disclose personal information” or “interact with” third parties, a business no longer has to ensure that the third parties do not “also sell the personal information.”
- The use or sharing of personal information with a service provider for a business purpose is no longer exempted from the definition of sale of personal information.

Security Breaches Involving Personal Information

- The CPRA expands the types of information covered under the private right of action for security breaches to include “email address[es] in combination with a password or security question and answer that would permit access to the account.” Presently, CCPA only includes “nonencrypted and nonredacted personal information, as defined in” Cal. Civ. Code 1798.81.5(d)(1)(A).[1]

30-Day Cure Period and Penalties

- Critically, the CPRA removes the existing 30-day period businesses have to cure most alleged violations of the statute. Presently, businesses have 30 days to cure violations of the CCPA and escape potentially hefty fines of $2,500 for each violation and $7,500 for each intentional violation. Additionally, under the CPRA, violations involving the personal information of consumers under the age of 16 will also result in a $7,500 penalty. There must be “actual knowledge” that the consumer is under the age of 16 for the $7,500 penalty to apply.
- Businesses will still have the opportunity to cure violations of Section 1798.150 (regarding Personal Information Security Breaches) within 30 days, to the extent violations are curable. Section 1798.150 permits private plaintiffs “[t]o recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.”
- However, in investigating a potential violation, the newly created California Privacy Protection Board (which will be entrusted with enforcing the CPRA) may take into account “voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of [a] complaint” made by any person.
- Additionally, at least 30 days prior to the California Privacy Protection Board’s consideration of an alleged violation of the CPRA and before determining whether there is probable cause to believe the CPRA has been violated, a business must be provided with “a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing a CPRA violation occurred.
- “When the agency determines there is probable cause for believing [the CPRA] has been violated, it [must] hold a hearing to determine if a violation has or violations have occurred.”
The CPRA makes additional changes to the CCPA, which will come into effect five days after the California Secretary of State certifies the referendum result, including the establishment of a new California Privacy Protection Board, which will implement and enforce the CCPA (and, eventually, the CPRA) and provide the Attorney General with expansive power to issue further regulations under the CCPA. The initial appointments to the California Privacy Protection Board are to be made within 90 days of its creation. "On and after the earlier of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities," the California Privacy Protection Board will assume responsibility for issuing regulations.

CPRA also extends, until January 1, 2023, exemptions from most of the CCPA’s requirements for personal information collected as part of a B2B transaction or collected from employees and job applicants. Under existing law, the exemptions would have expired on January 1, 2022.

As businesses continue to refine their CCPA compliance strategies, they should do so with the CPRA in mind. Although its effective date is more than two years away, businesses would be well served by familiarizing themselves and starting to address the CPRA sooner rather than later.


(A) An individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(iv) Medical information.

(v) Health insurance information.”

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.”

Practices
Privacy & Cybersecurity
Retail & E-Commerce