THOMSON REUTERS
PRACTICAL LAW™

Expert Q&A: The California Privacy Rights Act of 2020 (CPRA)

by Practical Law Data Privacy Advisor

Status: **Published on 09 Nov 2020** | Jurisdiction: **California, United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-027-7456**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

An Expert Q&A with Morrison & Foerster's Purvi G. Patel and Mary Race, examining California's passage on November 3, 2020 of Proposition 24, a ballot initiative to enact the California Privacy Rights Act of 2020 (CPRA). The CPRA amends and expands the California Consumer Privacy Act of 2018 (CCPA).

On November 3, 2020, Californians passed Proposition 24, a ballot initiative to enact the California Privacy Rights Act of 2020 (CPRA). The CPRA amends and expands California's first-of-its-kind consumer privacy law, the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199).

Practical Law asked Purvi G. Patel, a leading privacy and class action litigation partner from Morrison & Foerster's Los Angeles office, along with her colleague in the Privacy & Data Security practice group, Palo Alto-based associate Mary Race, to discuss how the CPRA changes California's current privacy laws and what businesses should start doing to prepare for the new law.

What is the CPRA?

The California Privacy Rights Act of 2020 (CPRA) is a law that amends the recently-enacted California Consumer Privacy Act of 2018 (CCPA). Like the CCPA, the CPRA protects the privacy rights and interests of consumers, which it defines as all California residents. Broadly speaking, the CPRA expands the scope and applicability of the CCPA while introducing new privacy protections that extend above and beyond those included in the CCPA and its implementing regulations. The CPRA also establishes a new enforcement body, the California Privacy Protection Agency, and requires additional rulemaking on a number of issues. The CPRA's substantive obligations imposed on businesses become operative on January 1, 2023, and enforcement can begin on July 1, 2023.

Does the CPRA change the scope of covered businesses?

The CPRA slightly alters the scope of covered businesses. While the CPRA maintains the CCPA's existing monetary threshold for application of annual gross revenue over $25 million dollars in the preceding calendar year, it changes some of the other thresholds to cover entities that either:

- Alone, or in combination, annually buy, sell, or share the personal information of 100,000 or more consumers. This represents an increase from the CCPA's 50,000 consumer threshold and deletes the CCPA's commercial purpose limitation, which could change the scope of covered businesses.
- Derive 50 percent or more of their annual revenue from selling or sharing consumers' personal information. The CPRA introduces "sharing" as a new term, defined as disclosing personal information to third parties for cross-contextual behavioral advertising purposes (see How does the CPRA change or expand consumers' rights?)

The CPRA also expands the definition of covered businesses to cover joint ventures or partnerships composed of other covered businesses that each have at least a 40 percent interest in the entity.

How does the CPRA change or expand consumers' rights?

The CPRA changes and expands consumers' rights to control the collection, use, and disclosure of their personal information in a number of ways, including:

- **Expanding the Right to Know.** The CPRA removes the CCPA's 12-month lookback period for access requests and gives consumers the right to make requests that extend beyond the 12 months preceding the request.
- **Modifying the Right to Delete.** The CPRA:
  - allows a business to deny a deletion request if maintaining the personal information is reasonably necessary to accomplish one of the specified grounds;
  - adds a new ground for denying a deletion request where retaining personal information is reasonably necessary to fulfill the terms of a written warranty or product recall conducted in accordance with federal law; and
  - combines two previously listed denial grounds—internal uses reasonably aligned with the consumer's expectations and business relationship and internal uses compatible with the context in which the consumer provided the information—into one. While internal uses must now meet both requirements to qualify for the exception, in practice the change is unlikely to impact a business's ability to deny a deletion request.

The CPRA also creates new consumer rights:

- **The Right to Correct.** This allows consumers to request that a business correct any inaccurate personal information it maintains about that consumer.
- **The Right to Opt-Out of Sharing Personal Information**. This allows consumers to prevent businesses from sharing their personal information, where sharing is defined as disclosing personal information with third parties for cross-contextual behavioral advertising purposes. It also prohibits businesses from sharing the personal information of a child under 16 without receiving opt-in consent. Unlike selling personal information under the CCPA, sharing personal information under the CPRA does not require any type of monetary or other valuable consideration in exchange for the personal information.

  Many of the new requirements for sharing personal information are similar to the CCPA's requirements around the sale of personal information. For example, a business must clearly disclose that it shares personal information, provide an opt-out link on its website, honor opt-out requests, and send those opt-out requests on to third parties with whom the business previously shared personal information.
- **The Right to Restrict Sensitive Information Processing**. This allows consumers to ask a business to restrict its use and disclosure of their sensitive personal information (see What is sensitive personal information and what additional obligations does the CPRA impose on businesses that collect or use it?).

What is sensitive personal information and what additional obligations does the CPRA impose on businesses that collect or use it?

The CPRA adds a new category of "sensitive" personal information and provides consumers with rights to opt out of a business's use and disclosure of their sensitive information.

The CPRA's broad definition of sensitive personal information goes beyond what most existing US laws consider sensitive and covers:

- Information typically considered sensitive in the US, such as:
  - Social Security Number;
  - driver's license number;
  - passport number;
  - financial account and payment card information;
  - precise geolocation; and
  - health and biometric information.
- Expanded sensitive information categories, such as:
  - race;
  - ethnicity;
  - religion;
  - union membership;
  - private personal communications, such as chats between community members; and
  - sex life or sexual orientation.

Businesses must:

- Disclose the types of sensitive personal information that they collect and the collection purposes.
- Comply with consumer requests to restrict the business's use and disclosure of their sensitive personal information, thereby permitting the business to use sensitive personal information only for limited business purposes defined in the CPRA (see How does the CPRA change or expand consumers' rights?).

- Provide a clear and conspicuous link on their website homepage, entitled "Limit the Use of My Sensitive Personal Information," that enables a consumer or other authorized agent to limit the use or disclosure of the consumer's sensitive personal information.

Do I need to change my CCPA notices at collection, privacy policy, or other privacy-related disclosures? If so, how?

Yes. The CPRA requires additional disclosures to consumers that will impact both a business's notice at collection and privacy policy. Privacy disclosures will need to describe:

- The retention period or retention criteria for each category of personal information collected.
- Details regarding the processing of sensitive personal information.
- The new correction right.
- Whether personal information is sold or shared.

Businesses must also publicly commit to not reidentify deidentified personal information.

Do I need to review or change my contracts with service providers or other third parties? If so, how?

Yes. The CPRA adds specific types of provisions that businesses must include in third party contracts that involve selling, sharing, or disclosing personal information, including with service providers, contractors, or third parties. Contractor is a newly-defined term in the CPRA that resembles the CCPA's definition of a service provider.

Required contract terms may include provisions that:

- State the business sells or discloses the personal information only for limited and specified purposes.
- Obligate the third party, service provider, or contractor to comply with the CPRA and require them to provide the same level of privacy protection that the CPRA requires.
- Grant the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information in a manner consistent with the business's obligations under the CPRA.
- Require the third party, service provider, or contractor to notify the business if it determines that it can no longer meet its obligations under the CPRA.
- Grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

Does the CPRA continue the CCPA's temporary exceptions for workforce personal information and business-to-business communications?

Yes, the CPRA extends the CCPA's temporary partial exceptions for certain workforce personal information and business-to-business communications through January 1, 2023. Workforce members include applicants, employees, owners, directors, officers, medical staff members, and independent contractors. Importantly, the extensions only apply until the CPRA's operative date and expire just as the CPRA's substantive obligations become operative. For more on these exceptions, see Practice Note, Understanding the California Consumer Privacy Act (CCPA): Temporary Exemptions.

Does the CPRA change the CCPA's consumer private right of action?

The CCPA's private right of action for certain data breaches remains largely the same, except the CPRA adds account credentials to the subset of personal information to which the CCPA's private right of action applies, namely those involving personal information described in one subsection of California's data breach notification statute (Cal. Civ. Code § 1798.81.5(d)(1)(A)). The CPRA's subset of personal information now includes an email address in combination with a password or security questions and answers that would permit access to the account. While this brings additional information within the private right of action's scope, the practical impact is not significant, as California's data breach notification statute already includes such account credentials (Cal. Civ. Code § 1798.81.5(d)(1)(B)).

The CPRA also specifies that a business cannot cure a data breach by subsequently implementing and maintaining reasonable security procedures and practices pursuant to Cal. Civ. Code § 1798.81.5.

What other key changes does the CPRA make?

Four other important changes to highlight include:

- **Data Minimization.** The CPRA expands the circumstances in which businesses must minimize their activities involving personal information, such as requiring businesses to collect, use, retain, and share personal information only as "reasonably necessary and proportionate" to its intended purposes.
- **Service Providers.** The CPRA imposes more direct obligations on service providers, including specific requirements to cooperate with businesses in responding to consumers' access, correction, and deletion requests.
- **Data Security**. The CPRA explicitly requires businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information that they handle in order to protect it from:
  - unauthorized or illegal access;
  - destruction;
  - use;
  - modification; or
  - disclosure.

  The CPRA does not define reasonable security procedures and practices.
- **Significant Risk Processing.** Businesses that process personal information in a manner presenting a significant risk to consumers' privacy or security must perform an annual, independent cybersecurity audit and submit an annual privacy risk assessment to the newly created California Privacy Protection Agency.

What is the California Privacy Protection Agency?

The CPRA creates a new state government agency vested with full administrative power, authority, and jurisdiction to implement and enforce the CPRA, called the California Privacy Protection Agency. The Agency, along with the California Attorney General, is authorized to investigate potential CPRA violations and bring CPRA-related enforcement actions (see Who will enforce the CPRA?). The Agency will also take over the California Attorney General's current role of issuing regulations under the CPRA and CCPA.

Other Agency tasks include:

- Protecting fundamental privacy rights.
- Promoting public awareness and understanding of privacy rights, risks, and obligations.
- Providing guidance to both businesses and consumers regarding their CPRA rights, duties, and obligations.

The Agency will be governed by a five-member board appointed by the Governor of California, the California Attorney General, the California Senate Rules Committee, and the Speaker of the California Assembly.

Who issues regulations under the CPRA and what type of regulations should businesses expect?

While the California Attorney General is currently tasked with issuing CPRA regulations, once formed, the California Privacy Protection Agency will take on this responsibility. The CPRA sets a July 1, 2022 deadline for issuing final regulations.

Businesses should expect to see regulations issued on a range of topics, including:

- Responding to a consumer's request to:
  - correct inaccurate information;
  - opt-out of sharing personal information or limiting sensitive personal information uses; or
  - access personal information beyond the CCPA's 12-month lookback period.
- Performing a required cybersecurity audit and submitting risk assessments to the Agency.
- The use of automated decision-making technology, including profiling, related to access and opt-out rights.
- The scope and process of the Agency's audit authority.
- Requirements for an opt-out preference signal, if the business elects to use an opt-out preference signal for consumer requests not to sell or share personal information or to limit use of sensitive personal information.
- Further defining terms such as:
  - specific pieces of personal information obtained from the consumer;
  - precise geolocation; and
  - intentionally interacts.

Who will enforce the CPRA?

The CPRA provides for joint enforcement by the:

- Newly created California Privacy Protection Agency, which enforces the CPRA through administrative proceedings (see What is the California Privacy Protection Agency?).
- The California Attorney General, who remains empowered to investigate CPRA violations and seek civil penalties.

To mitigate potential jurisdictional conflicts, the CPRA provides that:

- A business will not be required to pay both an administrative fine and a civil penalty for the same violation. The Attorney General cannot bring a civil action against the same business for the same violation after the Agency has issued:
  - a decision with respect to a complaint or administrative fine; or
  - an order based on a violation of the CPRA.
- The Attorney General may instruct the Agency to stay an administrative action or investigation so the Attorney General can proceed with its investigation or civil action, and the Agency cannot further pursue the administrative action or investigation unless the Attorney General subsequently determines not to pursue its own investigation or civil action.

The CPRA also:

- Removes the 30-day cure period from the Attorney General's enforcement process.
- Broadens the circumstances in which the highest fine of $7,500 per violation is applicable, for example, violations involving minors under 16 years of age now trigger the higher $7,500 per violation penalty.

Does amending the CPRA require a new ballot initiative?

Not necessarily. The CPRA specifically provides that it can be amended by a statute if:

- The statute is passed by a vote of a majority of the members of each house of the California Legislature and signed by the Governor of California.
- The amendments are consistent with and further the purpose and intent of the CPRA.

Any other amendments, or a repeal, would require voter approval.

How does the CPRA handle conflicts with other state or sector-specific privacy laws?

Like the CCPA, the CPRA provides complete or partial exceptions from its coverage for certain information protected or governed by specific federal or California privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Confidentiality of Medical Information Act (CMIA), the Gramm-Leach-Bliley Act (GLBA), the Financial Information Privacy Act (SB1), the Fair Credit Reporting Act (FCRA), and the Driver's Privacy Protection Act (DPPA). Likewise, the provisions of the CPRA relating to children under 16 years of age only apply to the extent they are not in conflict with the federal Children's Online Privacy Protection Act (COPPA).

The CPRA does not apply where it is preempted by, or in conflict with, the California Constitution. However, the CPRA's provisions prevail over any conflicting legislation enacted after January 1, 2020.

When does the CPRA take effect?

The CPRA becomes operative on January 1, 2023, and is enforceable by the California Attorney General and the California Privacy Protection Agency on July 1, 2023. With the exception of consumer access requests, which may cover personal information collected under a longer look-back period, the new provisions of the CPRA will apply to personal information collected on or after January 1, 2022.

What steps should businesses take now to prepare for the CPRA's operative date?

While the CPRA's operative date of January 1, 2023 may seem far away, businesses should consider ramping up CPRA compliance preparations sooner rather than later. Businesses may find it useful to start by assessing their current state of compliance with CCPA's existing requirements and then determining how and to what extent the CPRA will require additional or altered compliance efforts. This can help businesses prioritize and budget

for those areas where more effort may be required, for example, in relation to sensitive personal information and new rights around correction and opting out of sharing.

For more on California's privacy and data security laws in general, see Practice Note, California Privacy and Data Security Law: Overview. For CCPA-related resources, see California Consumer Privacy Act (CCPA) Toolkit.