Articles + Publications | November 10, 2020

Californians Pass CPRA, Expanding Consumer Privacy Protections

WRITTEN BY

Ronald Raether, Jr. | Wynter L. Deagle | Sharon R. Klein | Alex C. Nisenbaum | Brett A. Dorman | Karen H. Shin

California voters passed Proposition 24 in last week's general election to adopt the California Privacy Rights Act of 2020 (CPRA), which amends the California Consumer Privacy Act of 2018 (CCPA) in several ways intended to enhance consumer privacy protections. The CPRA becomes effective on January 1, 2023, except for certain provisions that will take effect on January 1, 2021. In the interim, the CCPA will remain in full force and in effect.

At a high level, the CPRA brings California's landmark privacy law closer to the E.U.'s General Data Protection Regulation (GDPR). For instance, the CPRA introduces GDPR-like principles, requiring that a business's collection, use, retention, and sharing of personal information 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." The CPRA also creates new consumer privacy rights, new obligations for businesses and service providers, and the first state regulatory agency dedicated to enforcing privacy laws.

The CPRA also:

- redefines "business" under the CCPA to those that, alone or in combination, annually buy or sell *or share* the personal information of 100,000 (instead of 50,000) or more consumers or households, or derive 50% or more of their annual revenues from selling *or sharing* consumers' personal information, in addition to for-profit entities with annual gross revenues of $25 million;

- creates a new right to correct inaccurate personal information (similar to that of the GDPR's right to rectification);

- creates a new right to limit the use of "sensitive personal information" (*e.g.,* social security numbers, financial and health information, racial or ethnic origin, sexual orientation, precise geolocation, genetic data, and other biometric information), and requires businesses to provide a new, separate link titled, "Limit the Use of My Sensitive Personal Information";

- creates the right to opt out of the sharing of personal information for cross-context behavioral advertising;

- requires, upon receipt of a verifiable request to delete, businesses to notify service providers and all third parties to whom the business has sold or shared personal information to delete such personal information, subject to

certain exceptions;

- imposes certain obligations directly on “service providers” and newly defined “contractors” (in contrast to the CCPA, where vendor obligations exist primarily through contract), including requiring service providers and contractors to (1) notify businesses of any engagement with a sub-service provider or subcontractor and to bind those parties to the same written contract that is otherwise arranged between businesses and service providers or contractors; (2) cooperate and assist businesses in responding to consumer requests; and (3) prohibit combining any personal information received from a business with personal information from other sources or collected on its own behalf, subject to certain exceptions;

- expands the CCPA’s private right of action for breaches of nonencrypted, nonredacted personal information to the unauthorized access or disclosure of an email address and password or security question that would permit access to an account if the business failed to maintain reasonable security;

- includes heightened administrative fines for mishandling children’s data, coupled with the clarification that individuals under 16 must opt in for a business to sell “or share” their personal information; and

- makes the 30-day cure period discretionary for administrative enforcement actions. Instituting reasonable security procedures will not constitute a cure.

Like the CCPA, there will be a six-month delay between the CPRA’s effective date and its enforcement, with enforcement actions commencing on July 1, 2023. With the exception of a business’s right-to-know obligations, the CPRA only applies to personal information collected by a business on or after January 1, 2022. However, the following CPRA provisions go into effect on January 1, 2021:

- **Employee and B2B Exemptions:** The CCPA was amended in October of 2019 to exempt certain personal information related to employment and business-to-business (B2B) communications and transactions. With those limited exemptions set to expire on January 1, 2021, the governor signed AB 1281 into law on September 29, extending the exemptions to January 1, 2022. However, since AB 1281 would only take effect if California voters did not approve the CPRA, now with the CPRA’s approval, the CPRA employment and B2B exemptions will now extend until January 1, 2023.

- **New Enforcement Agency:** The CPRA establishes the California Privacy Protection Agency (CPPA), a five-member board appointed by California’s governor, attorney general, Senate Rules Committee, and speaker of the assembly, to implement and enforce the CCPA and CPRA through administrative action, including audits and fines, while leaving civil enforcement in the courts to the attorney general.

- **Rulemaking:** The CPRA requires the CPPA to adopt, amend, and rescind regulations on 22 topics — relating to definitions, exemptions, technical specifications for opt-out preference signals, automated decision-making, cybersecurity audits and risk assessments, and monetary thresholds for “business” eligibility — to carry out the purposes and provisions of the CCPA, including specifying record keeping requirements for businesses to ensure CPRA compliance. Final regulations must be adopted by July 1, 2022 or within six months of the CPPA, providing the attorney general with notice that it is prepared to assume rulemaking responsibilities.

In the meantime, businesses should focus on complying with the CCPA, including building in flexibilities to modify and clarify proposed enforcement regulations for example. For example, on October 12, 2020, Attorney General Xavier Becerra released a third set of Proposed Modifications (Proposed Modifications) to the regulations implementing the CCPA. For additional information on the Proposed Modifications, see Troutman Pepper's article here. Businesses should also closely monitor any CPRA developments, as things may change between now and January 1, 2023.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber