Published on *The National Law Review* https://natlawreview.com

California Approves the CPRA, a Major Shift in U.S. Privacy Regulation

Article By:

Matthew A. Diaz

Kurt R. Hunt

On Nov. 3, 2020, California voters approved Proposition 24, marking a significant shift in the U.S. privacy landscape. Proposition 24 enacted the California Privacy Rights Act of 2020 (CPRA),[1] a major expansion of the existing California Consumer Privacy Act (CCPA), which many businesses continue to grapple with since becoming effective in January 2020. Most notably, the CPRA establishes a stand-alone privacy regulator, the first U.S. state to do so. The CPRA also boosts some of the CCPA's central privacy protections and expands the types of liability businesses may face for privacy or information security violations.

Background

Unlike the CCPA, the CPRA was a measure enacted directly by California voters. It started as a ballot measure this past summer, receiving sufficient signatures to be placed on the 2020 ballot. The CPRA is unique because it is not intended to replace the CCPA, which remains in effect—instead, the CCPA will eventually be incorporated into the CPRA, which will take effect on Jan. 1, 2023.

Scope

The CPRA includes a number of amendments and modifications to the CCPA, such as extending enforcement exemptions, defining the term "consent," and imposing additional privacy policy disclosures. This section will focus on four of the CPRA's most significant provisions: (1) expansion of California resident privacy rights; (2) new protections for "sensitive personal information"; (3) establishment of a California privacy regulator; and (4) expansion of the CCPA's private cause of action.

Expanded Privacy Rights

Aside from modifying the CCPA's existing consumer privacy rights, the CPRA creates a new consumer right: the Right to Correct Inaccurate Personal Information (i.e., the right to rectification).[2] This right states that a "consumer shall have the right to request a business that maintains inaccurate personal Information about the consumer correct such inaccurate personal

information…." However, this right is not absolute. It is limited based on the nature and purpose of the processing of personal information. As with other CCPA privacy rights, this new right will be effectuated through the use of verifiable consumer requests.

Sensitive Personal Information

The CPRA creates a new subcategory of personal information called "Sensitive Personal Information."[3] The concept of Sensitive Personal Information is new and broadly defined. The identifiers that qualify as Sensitive Personal Information under the CPRA include:

- Government-issued identifiers (e.g., social security number, driver's license number, passport number);
- Financial information (e.g., financial account information, credit/debit card information);
- Precise geolocation information;
- Biometric information and genetic information;
- Racial or ethnic origin, religious or philosophical beliefs, or union membership;
- Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation; and
- The contents of a consumer's mall, email, and text messages, unless the business is the intended recipient of the communication.

Businesses processing Sensitive Personal Information will be subject to additional requirements, and consumers will have the affirmative right to limit use of their Sensitive Personal Information.[4]

New Privacy Regulator

Possibly the most noteworthy provision of the CPRA is the establishment of the California Privacy Protection Agency (Agency).[5] Although the Federal Trade Commission and state attorneys general currently regulate privacy violations as "unfair or deceptive trade practices," this is the first time a U.S. government agency (federal or state) has been formed with the sole purpose of regulating consumer data privacy. The Agency will replace the California attorney general as chief enforcer of consumer privacy and will be vested with full "power, authority, and jurisdiction to implement and enforce" the CCPA and CPRA when it takes effect.

The Agency will assume rulemaking and enforcement authority from the California attorney general no later than July 1, 2021. The Agency will further have the authority to conduct hearings and subpoena witnesses related to violations of the CCPA and CPRA.

Expanded Data Breach Liability

A less noteworthy change, but nonetheless significant, is an expansion of the CCPA's private right of action related to data breaches. Under the CPRA, this private right of action will include the compromise of email addresses in combination with a password or security Q&As that might grant

access to a user's account.[6]

Effective Date

The CPRA does not take effect until Jan. 1, 2023; however, it will have a "look-back" period to Jan. 1, 2022. The CPRA further extends the current employee personal information exemption until Jan. 1, 2023. Provisions related to the establishment of the California Privacy Protection Agency, the establishment of a Consumer Privacy Fund, and requirements to adopt new privacy regulations take effect immediately.[7]

[1] The California Privacy Rights Act of 2020, CA Proposition 24 (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf (hereinafter, Proposition 24).

[2] *Id*. at Sec. 6.

[3] *Id*. at Sec. 14.

[4] *Id*. at Sec. 10.

[5] *Id*. at Sec. 24.

[6] *Id*. at Sec. 16.

[7] *Id*. at Sec. 31. "Subdivisions (m) and (n) of Section 1798.145, Sections 1798.160, 1798.185, 1798.199.10 through 1798.199.40, and 1798.199.95, shall become operative on the effective date of the Act."

National Law Review, Volumess X, Number 322