It’s Here: California Voters Approve the CPRA

Alysa Z. Hutnik, Aaron J. Burstein

November 4, 2020

On Tuesday, November 3, 2020, California voters passed ballot Proposition 24, the California Privacy Rights Act of 2020 (“CPRA”). Also known as CCPA 2.0, CPRA brings a number of changes to the CCPA, the majority of which will become operative on January 1, 2023. In addition to revising some of the definitions that are fundamental to commercial relationships under the CCPA (e.g., the definition of “sale” and “service provider”), CPRA provides additional consumer rights, incorporates data minimization and certain other principles from the General Data Protection Regulation, and establishes a new California Privacy Protection Agency, which will become the state’s privacy regulator and share enforcement oversight with the State Attorney General’s Office.

In a previous blog post about CPRA, we provided a general overview of the differences between CPRA and CCPA. Now that CPRA has passed, we provide a more detailed some of its key provisions:

Sharing and Selling.

The CPRA introduces the term “sharing” as distinct activity from “selling” personal information. Sharing is defined as disclosing or otherwise communicating a consumer's personal information for “cross-context behavioral advertising” – defined as ad targeting based on information obtained about a consumer across different apps or services – whether or not for monetary or other valuable consideration, including transactions between a business and a third party. Consumers have the right to opt out of the sharing of their personal information with third parties.

Why It Matters: Although California’s law will remain opt-out-based, the expansion to “sharing” may have a large impact on digital marketing contracts, and will expand businesses’ opt-out obligations. For instance, businesses that determined that their disclosures of personal information for ad-related purposes do not constitute “sales” because the exchanges do not involve valuable consideration may need to revisit those decisions. Businesses that engage in “selling” or “sharing” will also need to provide or update their opt-out links and processes to provide consumers with a “Do Not Sell or Share My Personal Information” choice.

Consumer Rights.

CPRA creates several new consumer rights and protections:

- *Right to Correct.* Under CPRA, consumers have the right to correct inaccurate personal information the business holds about them. This mirrors the right to correction under the GDPR.
- *Automated Decision Making.* Consumers also have a right to opt out of the use of their personal information for automated decision making, which includes “profiling” in connection with evaluations or decisions about to a consumer’s work performance, economic situation, health,

personal preferences, interests, reliability, behavior, location or movements. The consumer also has a right to access "meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."

- *Right to Restrict Use of Sensitive Personal Information.* CPRA also regulates the use of "sensitive personal information," which includes precise geolocation data, race, religion, sexual orientation, social security numbers, and certain health information outside the context of HIPAA. Consumers may limit the use and disclosure of sensitive personal information for certain "secondary" purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions.

- *Right to Data Portability*. Consumers may request that the business transmit specific pieces of personal information to another entity in a structured, commonly used and machine-readable format.

Why It Matters: Many businesses will likely need to implement new processes to accommodate these new consumer rights.

Service Providers and Contractors.

CPRA adds new requirements to qualify as a "service provider" and introduces the parallel category of "contractor." A business "makes available" personal information to a contractor; a service provider receives personal information from or on behalf of a business and processes the information on behalf of that business. The CPRA imposes substantively similar contractual and direct obligations on contractors and service providers, and also requires contractors to certify that they understand and will comply with such contractual obligations.

In addition, CPRA imposes a number of new requirements on service providers and contractors:

- *Data Silos.* Service providers and contractors must keep separate any data they obtain about a consumer in the course of assisting a business with advertising and marketing from other data they obtain about the consumer from other sources.

- *Marketing Services.* The CPRA clarifies that a service provider or contractor can provide advertising and marketing services, but not cross-context behavioral advertising.

- *Contractual Terms*. The business and service provider/contractor must enter into a written agreement that includes specific terms outlined in CPRA, similar in concept to GDPR Art. 28.

- *Subcontractors.* Service providers and contractors to notify businesses of any engagement with a sub-service provider or subcontractor and to bind those parties to the same written terms as between businesses and service providers.

Why It Matters: Companies will need to review their service provider/contractor terms to determine whether they include the requisite contractual terms, and review the scope of their services to ensure they do not provide cross-context behavioral advertising. These efforts come on the heels of updates to such agreements that many companies made relatively recently in response to CCPA obligations.

* * *

Finally, most CPRA provisions will become operative on January 1, 2023. However, a few provisions,

including the extension of the employee and B2B exceptions through the end of 2022, will become operative as soon as the administrative process of recording California's vote is complete. In the meantime, businesses must comply with the CCPA and its implementing regulations. (As discussed in this post, the California Attorney General has proposed several modifications to the regulations.) Please contact any of the attorneys in Kelley Drye's Privacy Group if you would like assistance in California privacy compliance.