CLIENT ALERT

CCPA 2.0? California Adopts Sweeping New Data Privacy Protections

Nov.06.2020

On November 3, 2020, California voters approved California Proposition 24, also known as the California Privacy Rights Act of 2020, or CPRA. The CPRA expands protections afforded to personal information, building off of the California Consumer Privacy Act (CCPA), which took effect in January of this year. While some of the CPRA changes will take effect immediately, most will not become enforceable until July 1, 2023, and apply only to personal information collected after January 1, 2022.

Key Changes to CA Privacy Law

At 54 pages long, the CPRA makes numerous changes to the CCPA, ranging from minor revisions to the introduction of new concepts and the creation of several new consumer rights. Some of the most impactful changes are discussed below. A series of future client alerts will explore the nuances of these changes in greater detail.

Sensitive Personal Data

The CPRA establishes new rules for a category of "sensitive personal information," which includes, for example, genetic data and religious or philosophical beliefs, and is defined as personal information that reveals:

(1)

A. a consumer's social security, driver's license, state identification card, or passport number;
B. 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;
C. a consumer's precise geolocation;
D. a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
E. the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; and
F. a consumer's genetic data; and

(2)

A. the processing of biometric information for the purpose of uniquely identifying a consumer;
B. personal information collected and analyzed concerning a consumer's health; or
C. personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

This definition is among the most impactful changes in the CPRA, given the breadth of data that it sweeps in, along with the creation of new disclosure and opt-out rights associated with "sensitive personal information." These changes will likely require covered businesses to dive into their data, map it, and ensure they are compliant.

In addition, the CPRA creates a right for consumers to "limit use and disclosure of sensitive personal information." Similar to existing CCPA opt-out rights, beginning in 2023, consumers may direct businesses that collect sensitive personal information to limit its use to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer" or to perform a small subset of specifically identified exempt services. Significantly, exemptions to the opt-out will include short-term, transient advertising, and "performing services on behalf of the business," but not general advertising and marketing, nor long-term profiling or behavioral marketing technologies.

Consent

The CPRA adds a new definition of "consent" that imposes first-of-its-kind requirements in the U.S. that are similar to those in the European Union General Data Protection Regulation (GDPR), defining consent as:

> "any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose."

This definition explicitly excludes acceptance of general or broad terms of use, or the continued use of a product, from qualifying as "consent."

For businesses that rely on consent consistent with the GDPR, these requirements should be familiar, but this requirement will be new for many U.S. businesses that previously relied on consent obtained via privacy policy or terms of service incorporated by reference, or "implied" by continued use of a service.

"Sharing" Personal Information

The CPRA creates a new definition for "sharing" personal information and requires businesses that "share" personal information to offer an opt-out similar to the opt-out already required under the CCPA for the "sale" of personal information, thus increasing risk and compliance burdens for businesses.

Under the CRPA, "sharing" personal information means:

> sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

This new provision will likely require businesses that engage in online advertising and social media to revisit whether their business practices constitute "sharing" under the CPRA.

Clarifications to the Definition of "Business"

In another key change, the CPRA raises one of the thresholds established in Cal. Civ. Code Section 1798.140(c) governing when an entity qualifies as a "business" subject to the CCPA. Under the new definition, an entity qualifies as a "business" if it "annually buys, sells, or shares the personal information of 100,000 or more consumers or households." The updated definition raises the annual threshold from 50,000 to 100,000 consumers or household, and no longer includes "devices" in that total. The CPRA also adds the requirement that an entity which "controls or is controlled by a business" must share consumers' personal information with the "business" to qualify as a business itself.

Changes to "Service Providers"

The CPRA makes significant alterations to the definition of "service provider" – a key concept under the CCPA largely analogous to the role of data processors under the GDPR. The CPRA explicitly prohibits service providers (now defined as "persons" rather than legal entities organized for profit) from selling *or sharing* personal information, and more explicitly prohibits service providers from combining information received from or on behalf of a business with personal information received from other sources, including the service provider's own interactions with a consumer.

The CPRA also imposes an explicit obligation on service providers to assist businesses in complying with any verifiable consumer requests that businesses may receive, with the specific assistance based on the nature and purpose of the processing activity.

The additions to the definition of service provider tighten further the previously imposed standard, which prohibited service providers from "retaining, using, or disclosing" the personal information received from businesses "for any purposes other than the specific purpose of performing the services." Service providers will need to ensure that any use of data, including how data is stored and used internally, shared, and sent to any sub-processors, is documented in the applicable written agreement.

New Disclosure Requirements

In addition to existing disclosure requirements under the CCPA, under the CPRA, businesses must disclose to consumers:

- The categories of sensitive personal information collected, if any, and the purposes for which sensitive personal information is collected or used, and whether such information is sold or shared.
    - For businesses that collect sensitive personal information, a clear and conspicuous link on the businesses' home page titled "Limit the Use of My Sensitive Personal Information" is also required. This may be combined with the existing requirement for businesses that sell personal information to include a link titled "Do Not Sell My Personal Information."
- The length of time a business intends to retain each category of personal information collected, including sensitive personal information, or alternatively, the criteria used to determine such a period.
- The categories of personal information "shared" with third parties or "sold."

Businesses that have already invested in CCPA compliance will need to review their existing notices and disclosures to ensure timely compliance with these new CPRA disclosure requirements.

Update to the Private Right of Action

The CPRA expands the existing private right of action for data breaches under the CCPA. Specifically, the CPRA provides a private right of action for the unauthorized access or disclosure of an email address and password or security question that would permit access to an account, along with access to a consumer's "non-encrypted and non-redacted personal information" if the access is attributed to a business's failure to maintain reasonable safeguards.

This change adds significant litigation risk under the private right of action for email service providers that qualify as "businesses" under the CPRA, as well as any other businesses that maintain full account credentials for email systems.

California Privacy Protection Agency

The CPRA authorizes the creation of the California Privacy Protection Agency (CPPA) as a new, separate agency within the California state government. The CPPA will replace the California Attorney General's office as California's privacy regulator. The new agency will take up the Attorney General's rulemaking authority on the later of July 1, 2021, or six months after it notifies the Attorney General that it is prepared to begin rulemaking.

Removal of the 30-Day Cure Period

While the newly-created CPPA will retain the discretion to allow businesses to cure alleged violations, the CPRA removes the explicit provision of the CCPA that always gave businesses a 30-day window to cure alleged noncompliance before being subject to administrative enforcement.

This change makes effective, early compliance a more critical area of focus of businesses, as there is no longer a guaranteed opportunity to remedy alleged noncompliance before facing a fine should a business be subject to regulatory attention.

Preemption

The CPRA specifies that it "supersedes and preempts all rules, regulations, codes, ordinances, and other laws" adopted by local or municipal governments in California "regarding the collection and sale of consumers' personal information by a business."

Extending Exemptions for Employee Data, Business to Business Data

The CPRA immediately extends the CCPA's existing partial exemptions for information relating to businesses' employees, and job applicants, as well as information collected from consumers in a "business to business" context. These exemptions were set to expire on January 1, 2021 in the original statute, and will now continue until at least January 1, 2023. The CPRA's passage moots a previously-passed amendment that would have extended the employee and business to business exemptions into 2022.[1]

AB 713, which codified exemptions for information already covered by the Confidentiality of Medical Information Act (CMIA) and the Health Insurance Portability and Accountability Act (HIPAA), was not directly affected by the CRPA.

Other Notable Changes

- The CPRA adds a requirement that businesses receiving a verified consumer request to delete personal information must not only direct service providers to delete that information, but also "all third parties to whom the business has sold or shared such personal information," unless such notice proves impossible or involves disproportionate effort.
- The CPRA creates at Cal. Civ. Code Section 1798.106 a new "Right to Correct Inaccurate Personal Information" that allows consumers to submit verifiable requests to businesses that maintain inaccurate personal information about consumers to correct such inaccuracies.

---

[1] The CPRA's passage triggers a conditional provision of AB 1281, which was signed into law in September 2020 to extend the employee and business-to-business exemptions into 2022, invalidating that bill.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kristin J. Madigan, CIPP/US
Partner – San Francisco
Phone: +1 415.365.7233
Email: kmadigan@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com