BRACEWELL

INSIGHTS

CPRA Countdown: It's Time to Brush Up on California's Latest Data Privacy Law

December 17, 2021

*By: **Matthew G. Nielsen** **Lucy Porter***

On November 3, 2020, California voters approved Proposition 24, a ballot initiative which enacted the ***California Privacy Rights Act*** ("CPRA"). The CPRA amends the California Consumer Privacy Act ("CCPA"), the most sweeping consumer data protection law in the U.S. This client alert highlights the differences between the CCPA and CPRA, the newly created agency charged with enforcing the CPRA, and steps businesses can take to begin their compliance efforts.

Background

In 2018, California lawmakers hurried to pass the CCPA, a consumer protection statute intended to enhance the privacy rights of California residents. Since the law passed, the CCPA's regulations have been criticized as vague and difficult to comply with. The CPRA is expected to address some of these issues. The CPRA significantly modifies the CCPA by expanding individual rights, introducing new GDPR-style governance measures, and establishing a new enforcement agency, among other things.

What's changed?

1. New Enforcement Agency

Arguably one of the biggest changes in the CPRA is the creation of the California Privacy Protection Agency ("Privacy Agency"). The Privacy Agency will have the full administrative power, authority, and jurisdiction to implement and enforce the CCPA and CPRA. The agency is empowered to impose a fine of $2,500 for each violation of the CPRA or $7,500 for each intentional violation or each violation involving a minor. Prior to this act, the CCPA was being enforced by the California Office of the Attorney General.

The CPRA eliminates the CCPA's 30-day notice and cure provision, but the Privacy Agency has discretion to provide a business with a time period in which to cure the alleged violation—taking into consideration a lack of intent to violate the CPRA and voluntary efforts to cure the alleged violation prior to being notified of a complaint.

2. Covered Businesses

The CPRA modifies the CCPA's definition of "business," changing which entities are covered. On the one hand, the CPRA increases the CCPA collection threshold from 50,000 consumers or households to 100,000, and it removes devices from this count. This change will provide relief for small businesses. On the other hand, the CPRA expands coverage to include entities that derive 50% or more of their annual revenues from selling or *sharing* consumers' personal information are now covered, regardless of whether they receive monetary compensation. While the act of *sharing* consumer personal information has been added, the 50% threshold remains unchanged. Other changes include joint ventures or partnerships and self-certifying entities.

Finally, in addition to the categories of "third-party vendors" and "service providers" under the CCPA, the CPRA adds "contractor" as a distinct class of regulated entities. A contractor is a third party to whom the business makes consumer personal information available to for business purposes. As with service providers, contractors must now enter into a written contract and agree to take appropriate steps to protect covered electronic data.

3. Sensitive Personal Information

One of the most significant changes from the CCPA is the creation of a new classification of personal information—sensitive personal information. This is a subcategory of PI that includes:

- Social Security, driver's license, state ID, or passport numbers
- Financial account information
- Precise geolocation
- Racial of ethnic origin
- Sex life or sexual orientation
- Religious or philosophical beliefs
- Union membership
- Nonpublic communication
- Genetic, biometric, and health data

Collection of sensitive personal information requires additional disclosure, opt-out, and use requirements. The distinct treatment includes granting consumers the right to limit disclosure and use of sensitive personal information except as necessary to perform the services. Companies must provide a link on their website titled "Limit the Use of My Sensitive Personal

Information" in addition to the CCPA's required opt-out link so that consumers may exercise this right.

4. New and Expanded Consumer Privacy Rights

The CCPA extended rights to California residents that went far beyond existing consumer privacy rights in the US: the right to know, the right to access, the right to delete, and a private right of action with statutory damages. The CPRA expands some of these rights and adds new ones.

- **Expanded Right to Know/Right to Access**. The CPRA expands this right beyond the CCPA's normal 12-month look-back period as long as doing so is not "impossible" or does not involve a "disproportionate" effort. The CPRA expands the CCPA's requirement to provide the categories of third parties to whom it discloses personal information to include the categories of service providers and contractors to whom it discloses information.

- **Expanded Right to Delete**. The CCPA allows California residents the right to request that a business delete their personal information if it is no longer needed to fulfill one of the statutory purposes. The CPRA expands this right, requiring businesses to send the request to delete to third parties that have bought or received the consumer's personal information, so that all parties must comply with the request.

- **Right to Opt-Out**. The CCPA allows consumers the right to opt-out of businesses selling their data to third-parties. The CPRA expands this right to include the *sharing* of personal information, in addition to selling. Businesses now must provide notice to consumers when their information will be shared and also notify them of their right to opt-out.

- **Opt-in Rights for Minors.** The CCPA requires businesses to obtain opt-in consent to sell the personal information of a California minor under the age of 16. The CPRA expands this right, mandating that businesses wait 12 months before asking a minor for consent in selling or sharing their personal information after the minor has declined.

In addition to expanding several CCPA rights, the CPRA also introduces several new consumer privacy rights:

- **Right to Correct Information**. California consumers now have the right to request that a business correct any inaccurate personal information.

- **Right to Limit Use and Disclosure of Sensitive PI**. California consumers now have the right to limit the use and disclosure of sensitive personal information to uses necessary to perform services or provide goods reasonably expected by an average consumer. Service providers and third parties are also required to adhere to this limitation.

- **Right to Access Information About Automatic Decision Making**. Like the GDPR, consumers now have the right to access information about how companies use automated decision-making technology. The CPRA allows consumers the right to opt-out of any automated decision-making processes.

- **Right to Data Portability**. California consumers now have the right to request that businesses transfer personal information to another entity, to the extent it is technically feasible.

5. Adoption of Certain GDPR Principles

The CPRA has codified the following GDPR-inspired provisions:

- **Data Minimization**. The CPRA restricts personal information collected by businesses to that which is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected." This section also prevents companies from avoiding CPRA obligations by sending personal information out of state or through third parties, contractors, or service providers. When a business collects personal information and passes it on to another entity for a business purpose, the CPRA also requires an agreement to be entered into that specifies the limited purposes of the given personal information. The receiving parties also must comply with the CPRA obligations and provide the same level of privacy while the information-sharing business is allowed to take reasonable steps to help ensure that the information is transferred appropriately.

- **Purpose Limitation**. The CPRA allows businesses to collect personal information only for "specific, explicit, and legitimate disclosed purposes" that are disclosed in advance to consumers.

- **Data Retention Limitation**. The CPRA contains data retention limitations that, like the GDPR, require that businesses disclose to consumers "the length of time the business intends to retain each category of personal information or if that is not possible the criteria used to determine such period . . . ."

- **Reasonable Security**. The CPRA expressly addresses security and security breaches, which is another GDPR-inspired provision. If a business violates its duty to implement and maintain proper security procedures and practices than consumers may have a civil action to recover damages, injunctive or declaratory relief, or any other relief the court deems proper.

6. Private Right of Action

The CPRA's expansion of the private right of action is arguably one of the most important provisions for businesses, given the recent rise in data breaches. The CCPA gives California consumers the private right to take legal action if their nonecrypted or nonredacted personal

information becomes exposed because a business failed to implement reasonable security measures. The CPRA expands that private right of action to include unauthorized access to email addresses and passwords or security questions.

Looking Ahead

These are just a few of the changes the CPRA is making to the world of data and privacy compliance. Although all aspects of the CPRA do not take full effect until January 1, 2023, companies that do business in California should start laying the internal groundwork for CPRA compliance throughout the course of 2021 and 2022. To prepare for the CPRA, organizations can take proactive steps such as:

- **Determine If You Are Subject To The CPRA**. Some businesses that were not subject to the CCPA will be impacted by the CPRA, and vice versa.

- **Consumer Requests**: Businesses should ensure they have sufficient internal processes for handling consumer requests and identify how to expand such processes to enable consumers to exercise new and expanded rights under the CPRA.

- **Update Privacy Policies**. Businesses should review and consider what updates should be made to their initial collection notice and website privacy notice to reflect new requirements, including those regarding sensitive personal information and the new/expanded rights.

- **Data-Mapping and Audits**. Businesses should consider conducting a data-mapping exercise to identify the types of data the organization stores, how it flows throughout the organization, who has access to the data, and the impact of a potential breach.

- **Review agreements with third parties**. Businesses should audit agreements with third parties to determine whether a data protection addendum is needed to bring the agreement into compliance with the CPRA.

Finally, it is important to remember that the CCPA is still very much in effect and will remain so until 2023. In the meantime, Bracewell attorneys are ready to help companies ensure compliance with the CCPA and CPRA.

This alert is the last in Bracewell's series reviewing the 2021 data privacy legislation landscape. Our previous alerts include a ***general overview***, ***the Colorado Privacy Act***, and ***Virginia's Consumer Data Protection Act***.