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

California Privacy Rights Act Passes - Dramatically Altering the CCPA

Article By:

Brian H. Lam

Voters in California have passed Proposition 24, commonly referred to as the California Privacy Rights Act of 2020 ("CPRA"). Less than a year after the CCPA became effective, the voters' approval of the CPRA will provide significant new rights to California consumers, create new compliance obligations for covered businesses, establish a new enforcement agency, and provide for data minimization and retention obligations, among other aspects. Below, we provide an overview of certain important aspects.

1. How Long Before the CPRA Becomes Effective?

The CPRA becomes effective January 1, 2023. Provisions that apply to covered business collection of personal information will apply to personal information collected on or after January 1, 2022. However, the exceptions for certain business-to-business activity and employees were extended by the CPRA immediately upon it passing to January 1, 2023. As it stands, both of these exceptions will end when the CPRA becomes effective on January 1, 2023.

2. Liability and Enforcement Expanded

The CPRA creates the California Privacy Protection Agency ("CalPPA"), which will have administrative authority and the ability to enforce the CPRA, including certain audit rights. It is likely that the creation of the CalPPA, will lead to additional enforcement of the CPRA beyond what we have seen with the CCPA. Further the CPRA has effectively expanded liability as well.

- **Triples Fines for Children's Privacy:** CPRA will triple the CCPA's fines where the collecting and selling information of children under the age of 16 violated the CCPA. This would be in addition to those obligations and fines the entity might face under the Children's Online Privacy Protection Act, which regulates website and online services that are directed to, or have actual knowledge that they are collecting information from, a child under 13.

- **Ability to "Cure" a Breach Reduced:** The CPRA clarifies that "the implementation and maintenance of reasonable security procedures and practices … following a breach does not

constitute a cure with respect to that breach."

- **Private Right of Action Expanded:** The private right of action now includes the compromise of a consumer's email address along with a security question or password that would permit access to the consumer's account.

3. Alters Requirements for an Entity to Qualify as a Covered Business

An entity will be considered a covered business under the CPRA if it is a for-profit entity that determines the means and processing of consumers' personal information, does business in California, and meets any one of the following conditions:

- Annual gross revenues over $25 million measured from January 1st for the previous calendar year. No clarification was provided regarding if the existing $25 million revenue requirement is intended to cover only revenue for California, or revenue overall.

- Annually buys, sells, or shares personal information of 100,000 or more consumers or households. This increased the threshold from 50,000 under the CCPA.

- Derives 50% or more of its annual revenue from selling or "sharing" personal information. Sharing is a newly created term, discussed in more detail below.

Additional scope changes:

- **Joint Ventures**: A joint venture may be found where the "joint venture or partnership composed of businesses in which each business has at least a 40 percent interest."

- **Common Control**: As before, entities can also be regulated as a business by being a commonly controlled entity. The CPRA has narrowed this coverage by limiting it to entities that are controlled by a covered business where an "average consumer" would understand that the two entities are commonly owned, and "with whom the business shares consumers' personal information."

- **Voluntary Certification**: An entity that does business in California can choose to certify to the CalPPA that it agrees to be bound by the CPRA.

4. Data Minimization and Data Retention Requirements

The CPRA introduces new principles involving data minimization and data retention.

- **Data Minimization:** Under the CPRA, the collection, use, and sharing of personal information must be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed…" Similarly, it also provides that personal information may not be used in such a way as to be "incompatible with the disclosed purpose for which the personal information was collected" without providing notice to the

consumer.

- **Retention Limitation**: The CCPA did not explicitly address data retention. Under the CPRA personal information may not be retained for longer than is "reasonably necessary" for the disclosed purpose.

5. Initial Notification Burden Increased

Under the CPRA, Businesses must now, at or before the point of collection, identify (a) whether collected information may be sold or shared, (b) any categories of the newly defined term "sensitive personal information" collected, and (c) any retention periods or, "if that is not possible, the criteria used to determine such period."

6. New Category of Personal Information Called "Sensitive Personal Information" Created

Under the CPRA, certain new rights and compliance burdens will attach to a new category of personal information called "sensitive personal information." Sensitive personal information will include financial information, account log-in credentials, a consumer's identification numbers (e.g., Social Security number, driver's license number, etc.), precise geolocation, racial and ethnic information, personal communications, and information about one's sex life or sexual orientation, and genetic data, biometric or health information, among other aspects.

7. Consumer Rights: New Rights Provided, Existing Rights Modified

The CPRA provides important new rights to consumers.

- **Restrict Disclosure and Use of Sensitive Personal Information**: The CPRA will require a covered business to limit its use of "sensitive personal information" to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," when a consumer exercises this right via the use of a "Limit the Use of My Sensitive Personal Information" link or a "single, clearly-labeled link … if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information."

- **Correct Personal Information**: The CPRA affords consumers the ability to correct inaccurate personal information.

The CPRA modifies existing consumer rights.

- **Deletion Right**: Covered businesses must provide notice to service providers, those entities that meet the newly created term "contractors", and third parties with whom the business has sold or shared personal information, to delete personal information upon receipt of a verifiable

consumer request, with certain exceptions. Service providers and contractors are also required to pass the deletion request along the chain if certain conditions are met.

- **Right to Know Time Period Increased**: Where personal information was collected after January 1, 2022, consumers will be able to make a request to know further back than the existing 12 month lookback period where doing so would not "involve a disproportionate effort" or be "impossible" for the covered business.

- **Expands Existing Opt-Out Right to Include "Sharing" of Personal Information:** The existing opt-out right for the sale of personal information will be expanded to include the "sharing" of personal information. Under the CCPA there were differences of opinion as to what would constitute a sale. The CPRA attempts to resolve this issue by defining sharing as the transfer or making available of 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." Effectively, this means that companies which do not currently provide opt-out rights for third-party behavioral advertising technologies will be required to incorporate their use of such technologies and implement a "Do Not Sell or Share My Personal Information" link.

8. New Compliance Burdens

- **Reasonable Security Required:** Covered businesses must "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosures." While this obligation did not explicitly exist under the CCPA, it was required for certain personal information under existing California Law under Civ. Code Sec. 1798.81.5(a).

9. Additional Vendor Contract Requirements

- The CPRA creates the new term "contractors," defined as persons to whom a business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business.

- Among other things, an agreement must be put in place that (a) provides that the information sold or disclosed by the covered business is "only for limited and specified purposes"; (b) obligates the service provider, contractor, or third party to comply with the CPRA and "provide the same level of privacy protection as" required by the CPRA; (c) require the service provider, contractor, or third party to notify the covered business if it can no longer meet its CPRA obligations; and (d) allow the business to "take reasonable and appropriate steps to stop and remediate unauthorized use of personal information" and to ensure the downstream receiving entity uses the personal information in a "manner consistent with the business's obligations" under the CPRA.

- Further, for contractors, the covered business must, among other aspects, via an agreement, prohibit the contractor from (a) selling or sharing personal information provided to it; (b) using or disclosing the personal information for any purpose other than those business purposes

outlined in the contract; and (c) combining the personal information with data received or collected through other means, subject to certain exceptions.

10. Additional Compliance Burdens

- **High Risk Activities will Require Privacy Impact Assessments and Cybersecurity Audits:** The CPRA requires the issuance of regulations regarding mandatory risk assessments and cybersecurity audits for high risk activities. The risk assessments will have to be submitted to the new California Privacy Protection Agency on a "regular basis." The concept of a "regular basis" is not defined in the CPRA and is likely to be expanded upon in the implementing regulations.

- **Regulatory Audits**: The CalPPA under certain circumstances will have the right to audit entities for compliance with the CPRA. As the current CPRA text does not provide a lot of detail, it is likely that regulations will expand upon this area.

- **Automated Decision Making**: Under the CPRA new regulations will be provided "governing access and opt-out rights with respect to a business's use of automated decision-making technology, including profiling…." There is little detail currently as to exactly what this will entail, and we expect the regulations to expand upon this point.

11. Steps CCPA Covered Businesses Should Take Now To Prepare For CPRA

If you are currently a CCPA covered business, here are some steps we recommend you take now.

- Review revised requirements for an entity to qualify as a covered business under the CPRA.

- Consider how the various new concepts will apply to your business model. This would include the data minimization and retention requirements, new consumer rights, use of sensitive personal information, use of automated decision making, potential regulatory audits, conducting of any high risk activities that may require a privacy impact assessment, and other aspects.

- Decide if CPRA obligations will be rolled out only for California consumers. This decision has likely already been made for CCPA obligations, however new issues created by the CPRA may make this siloed compliance more difficult.

- Based on this analysis, begin planning for and allocating budget for resources to bring any current CCPA program into compliance with the CPRA.

National Law Review, Volume X, Number 311