

# California Privacy Developments: The CPRA

Privacy & Cybersecurity Newsletter

## WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

---

Having set a new standard for privacy in the United States with the California Consumer Privacy Act of 2018 (the “CCPA”), California has again raised the bar for consumer privacy with the California Privacy Rights Act (the “CPRA”), which was passed by referendum on November 3, 2020. Effectively an amendment to the CCPA, the CPRA introduces some new rights for California residents; imposes new obligations on businesses; adds new terms and requirements; creates a regulatory agency; and extends two important (albeit partial) exemptions. The CPRA will become effective January 1, 2023.

## New Definitions

The CPRA (Section 14) introduces several new terms to CCPA Section 1798.140 that require businesses to track more closely their data and third party relationships, the most important of which are “contractor” and “sensitive personal information.”

**Contractor** means a person to whom the business makes available a consumer’s personal information for a business purpose pursuant to a written contract with the business provided that that contract contains certain required provisions that prohibit the contractor from: (i) selling or sharing the personal information; (ii) retaining, using, or disclosing the personal information outside the business relationship or for a purpose other than to support the contracted services; and (iii) combining the personal information with other information it collects (except in limited circumstances). A contractor must also certify that it understands and will comply with the CPRA’s restrictions, and must agree to permit the business to monitor its compliance with the contract’s terms on at least an annual basis.

Essentially, the distinction among the definitions of contractor, service provider and third party are that the third party is any person who is *not* a contractor or service provider, but with whom the business intentionally interacts and that collects personal information from the consumer as party of the consumer’s current interaction with the business. The contractor and service provider are similar in that they are both required to enter into contracts with CPRA mandated provisions that are largely identical. The difference is that contractors have additional obligations when compared to the service provider, as the contractor must (1) certify to the business that it understands the CPRA’s restrictions on use and disclosure, and (2) permit the business to monitor compliance with the contract.

**Sensitive personal information** is a subset of personal information that includes: (i) SSN, driver’s license or other government ID number; (ii) account log-in credentials or financial (e.g., bank, credit or debit) account number with access code or PIN; (iii) precise geolocation; (iv) race or ethnicity, religious or philosophical beliefs or union membership; (v) contents of personal (not business) mail, email or text messages; or (vi) genetic data. It also

includes: (i) biometric information used to identify a consumer; (ii) health information; or (iii) information concerning sex life or sexual orientation.

## **New Consumer Rights and Obligations**

The CCPA extended rights to California residents that went far beyond existing rights in the United States: a right to know, a right of access, a right to delete (or right to be forgotten), and a private right of action with statutory damages. The CPRA expands some of these rights, and adds new ones, and thereby expands the related obligations of businesses.

**Expanded Right to Know.** The CPRA (Sections 7, 8, & 12) extends the right to know to require additional disclosures, such as disclosures relating to the collection and use of sensitive information. In addition, the CPRA extends the right to know to include disclosure of retention periods or policies for each category of personal information and extends the look-back period for information subject to the right to know.

**Restriction to Appropriate Purposes.** The CPRA (Section 4) also restricts collection, use, retention and sharing of personal information to those activities that are “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context” of the collection.

**Written Contracts for Sale or Sharing.** Businesses that sell or share personal information must have written contracts in place that: (i) specify that the personal information is sold or disclosed only for limited and specified purposes; (ii) obligate the recipient to comply with CPRA obligations; (iii) enable the business to take reasonable and appropriate steps to ensure that the recipient complies with CPRA obligations; (iv) require that the recipient notify the business if it can no longer satisfy its CPRA obligations; and (v) grant the business, upon receiving such notice, the right to take steps to stop and remediate unauthorized use of the personal information (Section 15).

**Reasonable Security.** The CPRA (Section 16) includes a specific requirement to implement reasonable security “appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification or disclosure in accordance with Section 1798.81.5.”

**Push-Down of Right to Delete.** Under the CPRA (Sections 5 & 12), service providers and contractors have a statutory (in addition to contractual) obligation to comply with the consumer’s right to delete, including an obligation to cooperate with the business in honoring the consumer’s right.

**NEW Right to Correct.** The CPRA (Section 6) provides consumers with a new right to correct inaccuracies in their personal information.

**NEW Right to Limit Use and Disclosure of Sensitive Personal Information.** The CPRA (Section 10) grants a new right of consumers to limit the use 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 obligated to adhere to the limitation.

**Extension of 12-month Look-Back.** The CCPA’s 12 month look-back, requiring the business to disclose and

deliver upon request the personal information collected during the prior 12-month period, may be extended, upon the consumer's request, subject to the adoption of regulations, for information collected on or after January 1, 2022 (Section 12). The business would not have to comply if doing so would be impossible, or would involve a disproportionate effort.

**Expansion of Do Not Sell Right.** The CPRA (Sections 9 & 10) expands the CCPA's do not sell right to include a consumer's right to limit the sharing and use, as well as selling, of personal information, and the use of sensitive information. This limitation permits consumers to restrict the use of their sensitive personal information to uses (i) necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services, (ii) for four specific business purposes, or (iii) as authorized by regulations passed which relate to this right. The four specific business purposes permitted are: (1) helping to ensure security and integrity; (2) short term transient use; (3) performing services on behalf of the business; and (4) activities to verify the quality or safety of, or to improve a service or device offered by the business.

### **Extension of Important Exemptions**

Of critical importance to businesses are the CCPA's so-called "employee" (or more aptly "personnel") and "B2B" exemptions (Section 15). Although these exemptions are limited in scope, these two exemptions relieve businesses from most of the CCPA's requirements with respect to their own personnel (employees, officers, directors, contractors and others) and their contacts with other commercial relationships. These two exemptions were scheduled to sunset January 1, 2021, but the CPRA will extend both to January 1, 2023.

\* \* \* \* \*

With its refinement and addition of terms, consumer rights and business obligations, the CPRA represents a new, higher standard for consumer privacy rights in the U.S.

### **RELATED INDUSTRIES + PRACTICES**

- [Privacy + Cyber](#)