LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, APRIL 11, 2022

PERSPECTIVE

California Privacy Rights Act of 2020 brings U.S. closer to European standards

By Ron Raether, Kamran Salour, Sadia Mirza, Robyn W. Lin and Mary Kate Kamka

California was the first state to enact a comprehensive state privacy bill with the California Consumer Privacy Act of 2018 ("CCPA"). Although the CCPA went into effect on January 1, 2020, it was significantly overhauled during California's November 2020 General Election, when the California Privacy Rights Act of 2020 ("CPRA" or the "Act") was adopted.

The CPRA amends the CCPA in several ways, including modifying the thresholds for what qualifies as a regulated "business"; introducing new consumer rights and data processing obligations, and creating the first state agency dedicated to enforcing privacy laws – the California Privacy Protection Agency (the "Agency"). The CPRA also largely moves the California privacy law closer to the direction of the EU General Data Protection Regulation, which is a trend we see with the passage of new state privacy laws in Colorado, Virginia, and Utah. The full text of the CPRA is available here.

This five-part CPRA series is intended to provide a detailed overview of the Act, and how it compares to its predecessor – the CCPA. The series is divided into the following:

1. Introduction and Overview
2. Consumer Rights
3. Notice and Disclosure Obligations
4. Data Processing Obligations
5. Litigation and Enforcement

At the conclusion of the series, Troutman Pepper will host a webinar on the CPRA on Wednesday, May 11, 2022. Registration information will be circulated later.

A. Effective and Operative Dates

While the CPRA technically took effect December 15, 2020 – five days after the Secretary of State filed the statement of vote for the November 3, 2020 General Election – the majority of its provisions will not become operative until January 1, 2023.

B. Lookback Period

Once the CPRA is operative, it will only apply to personal information collected by a business on or after January 1, 2022. The only exception to this rule relates to the "Right to Access." On January 1, 2023, California residents who submit a request to access their personal information may be entitled to access all personal information a business has collected about them, regardless of when that information was collected, subject to the Act's many exemptions.

C. Enforcement Date

The CPRA will not be enforced immediately. Rather, enforcement is set to commence July 1, 2023, and will apply only to violations occurring on or after that date. Notably, the provisions of the CCPA amended or reenacted by the CPRA will remain in full force and effect and will continue to be enforceable until the same provisions of the CPRA become operative and enforceable. Practically, this means that we may continue to see CCPA enforcement initiatives by the California Attorney General up until the CPRA is ready to be enforced.

D. Implementing Regulations and Delayed Wait Times

The CPRA established the Agency and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." The Agency's responsibilities include appointing a "Chief Privacy Auditor" to conduct audits of businesses to ensure compliance with the CPRA and updating existing regulations and adopting new regulations.

Section 1798.185 of the CPRA, which is one of the few provisions that became operative on December 15, 2020, identifies twenty-two (22) areas for which the Agency is required to adopt regulations. This includes:

Right to Correct. Establishing how often, and under what circumstances, a consumer may request a correction under Section 1798.106, including: (i) standards governing how a business responds to a request for correction; (ii) exceptions for requests to which a response is impossible or would involve disproportionate efforts; and (iii) requests for correction of accurate information.

– Opt Out Requests and Processing of Sensitive Information. Establishing rules and procedures to facilitate and govern the submission of a consumer opt-out request of the sale or sharing of personal information under Section 1798.120, and to limit the use of a consumer's sensitive personal information under Section 1798.121.

– Cybersecurity Audits. Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent.

– Risk Assessments. Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to submit to the Agency on a regular basis a risk assessment, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

– Automated Decision-Making Technology. Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision- making processes, as well as a description of the likely outcome of the process with respect to the consumer.

– Agency's Audit Authority. Issuing regulations to define the scope and process for the exercise of the Agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

While the CPRA initially set the deadline for adopting final regulation as July 1, 2022, the Agency's Director, Ashkan Soltani, recently announced that the long-awaited regulations to the CPRA would be delayed. In a recent public meeting, he stated: "Formal proceedings, including public hearings, will continue into Q3 with rulemaking being completed in Q3 or Q4 of 2022. While this puts us somewhat past the July 1 rulemaking schedule in the statute, it allows us to balance staffing of the agency while undertaking substantial information gathering to support our rules."

In remarks with the California Lawyers Association in October 2021, the Agency's Board Chair, Jennifer Urban, spoke on her own behalf and addressed the many logistical and legal impediments in getting the new administrative agency up and running in time to develop and adopt regulations by the deadline. The many challenges include hiring, rulemaking under

California's Open Meetings Act, and the capacity of the board to undertake the many efforts needed to position the Agency to begin enforcement. Further complicating the Agency's efforts is the obligation to develop a significant volume of unprecedented rules governing issues, such as those outlined above. These rules are expected to double the existing body of regulations under the CCPA.

Urban appears to be considering various options for extending the "particularly aggressive" CPRA statutory deadline for adopting final regulations. One potential option would be "extending when we might begin enforcing [the regulations] … so people have time to understand and implement the regulations." As an administrative agency, the Agency will have discretion regarding the timing of initiating investigations, holding hearings, and issuing administrative orders. Urban noted that the Agency will actively receive counsel on all of its options for a potential extension if necessary.

A. Covered "Businesses"

If your organization falls under the CCPA, then you know the CCPA primarily regulates "businesses." If you started your CCPA-compliance journey with Troutman Pepper, you may recall the infographic that breaks down the definition of a CCPA-regulated business, available here. In short, a CCPA-regulated "business" is any organization that (a) operates for the profit or financial benefit of its shareholders or other owners, (b) collects California consumers' personal information, (c) either alone or jointly with others, determines the purposes and means of the processing of consumers' personal information, and (d) meets one or more threshold requirements.

The CPRA maintains the general definition of a covered "business" but modifies the thresholds to be as follows:

– As of January 1, of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year;

– Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households (under the CCPA, the threshold was only 50,000); or

– Derives 50% or more of its annual revenues from selling or sharing consumers' personal information.

The CPRA also clarifies that entities that control or are controlled by regulated businesses, and that share common branding with such business, may only be regulated if the covered business shares consumers' personal information with the other entity.

Practically, the changes introduced by the CPRA will likely result in fewer companies falling within the scope of the CPRA, including smaller companies who no longer meet any of the CPRA's threshold requirements, and affiliated companies with whom regulated businesses do not share personal information.

B. Service Providers and Contractors

Under the CCPA, entities that process personal information on behalf of regulated businesses are referred to as "service providers." While the obligations imposed on businesses by the CCPA are direct, a service provider's obligations under the CCPA are generally defined by the business in the applicable service provider contract.

The CPRA modifies this construct in two ways. First, it introduces the concept of a "contractor," which is like a service provider but not identical. A service provider is one who processes personal information on behalf of a regulated business for a business purpose pursuant to a written contract, whereas a contractor is a person to whom a business merely makes personal information available for a business purpose pursuant to a written contract. Thus, the distinction between the two appears to be the purpose for which personal information is disclosed, i.e., is the entity "processing" the information on behalf of the business or has the information been merely disclosed for an alternative purpose (e.g., a business disclosing records to an auditor that may include certain personal information).

Second, unlike the CCPA, the CPRA does impose obligations and restrictions directly on service providers and contractors. This means that service providers and contractors may be directly liable for a failure to comply with the CPRA. These obligations and restrictions include:

– Responding to Consumer Requests. Assisting businesses in responding to consumer requests, including by correcting inaccurate information or enabling the business to do the same; deleting personal information or enabling the business to do the same; and providing personal information to the business within the service provider's or contractor's possession that may be the subject of a data access request.

– Imposing Downstream Obligations. Requiring service providers and contractors to notify their own downstream service providers and contractors to delete information that may be the subject of a deletion request unless this proves impossible or involves disproportionate effort.

– Processing of Sensitive Personal Information. Subject to certain exceptions, restricting service providers and contractors from using sensitive personal information for certain purposes after receiving instruction from a business that the consumer has limited such use.

–Information Security Requirements. Assisting businesses through appropriate technical and organizational measures in complying with the requirement to "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 disclosure in accordance with Section 1798.81.5."

A. Blanket Exemptions

The CPRA continues to regulate "personal information." Personal information generally refers to information that is or could be reasonably linked to a California resident. Like the CCPA, the CPRA excludes the following types of information from the purview of the Act:

– Publicly available information

– De-identified data

– Information regulated by the Fair Credit Reporting Act (FCRA)

– Information regulated by the Driver's Privacy Protection Act (DPPA)

– Information regulated by the Gramm-Leach-Bliley Act (GLBA)

– Information regulated by the Health Insurance Portability and Accountability Act (HIPAA)

B. Personal Information Collected in the Employment and Business- to-Business Context

There is some uncertainty as to how personal information collected in the employment and business-to-business (B2B) context will be treated under the CPRA. When the CPRA took effect, the exemptions under the CCPA for personal information collected in these contexts were immediately extended until January 1, 2023. After this date, it was expected that information collected in these contexts will be in scope for the CPRA.

On February 18, 2022, however, California lawmakers introduced two separate bills aimed to extend the employment and B2B exemptions either indefinitely (AB-2871) or until January 1, 2026 (AB-2891). However, neither bill has yet been signed into law. Both bills were referred to the Committee on Privacy and Consumer Protection on March 17, 2022. The California Legislature ends on August 31, 2022. If passed, these bills have the potential to maintain the status quo as set by the CCPA, until at least January 1, 2026 (i.e., personal information collected in these two contexts would continue to be exempt until this time). Otherwise, companies should be prepared to comply with the CPRA's requirement to treat personal information collected in the B2B/employee context the same as other protected information.

C. "Sensitive Personal Information" Introduced

The CPRA introduces the concept of "sensitive personal information," and imposes certain data processing obligations relating to such. This follows Europe's GDPR approach, which provides specific protections when "special categories of personal data are involved." Under the CPRA, sensitive personal information is a subset of "personal information." It excludes information that is "publicly available" (e.g., information that a business has a reasonable basis to believe is lawfully made available to the public by the consumer or from widely distributed media), and is limited to personal information that reveals:

– A consumer's social security, driver's license, state identification card, or passport number.

– 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.

– A consumer's precise geolocation.

– A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

– The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

– A consumer's genetic data. Sensitive personal information also includes:

– The processing of biometric information for the purpose of uniquely identifying a consumer.

– Personal information collected and analyzed concerning a consumer's health.

– Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

While we will detail the specific

data processing obligations relating to sensitive personal information in Part 2 (Consumer Rights) of this series, consumers will have the right to restrict a business's use of sensitive personal information to, among other things, that use which is necessary to perform the services or provide the goods or services requested; to certain "business purposes" identified in the Act; and as otherwise authorized by the CPRA regulations. Businesses that use sensitive personal information for purposes other than those specified in the CPRA will be required to provide consumers notice of such use and inform them of their right to limit the use or disclosure of their sensitive personal information.

The second part of this series will cover the new consumer rights created by CPRA, and how such rights differ in comparison to those offered by the CCPA. At a high level, Part 2 will touch on:

– Modifications made to the "Right to Access" specifically relating to the "lookback period;"

– Downstream obligations triggered by a "Request to Delete;"

– Addition of the "Right to Correct" personal information;

– Requirements relating to the "sharing" of personal information, including consumers' right to opt out of such sharing; and

– Limitations on the use and disclosure of "sensitive personal information."

The third part of this series will cover the notice and disclosure obligations imposed by the CPRA, and how such obligations compare to those imposed by the CCPA. As a preview, while both the CCPA and CPRA contemplate the same four types of notices (i.e., the privacy policy, notice at collection, notice of right to opt out, and notice of financial incentive), the content requirements for certain of these notices were modified to include additional requirements, including relating to data retention and data minimization.

The fourth part of this series will detail the data processing obligations imposed by the CPRA, and how such obligations compare to those under the CCPA. The article will focus on areas such as contract requirements for service providers and contractors, audits and risk assessments, information security, and disclosures relating to automated decision-making technology.

Like the CCPA, there is no private right of action for a violation of the CPRA. The CPRA has, however, split enforcement authority between the California Attorney General and the California Privacy Protection Agency. Part five of our series will take a deep dive into the enforcement provisions of the CPRA, providing a detailed overview of the AG's and Agency's enforcement authority under the Act, modification to the 30-day cure window, available statutory damages, and the limited private right of action for data breaches.

Ron Raether *and* **Kamran Salour** *are partners and* **Sadia Mirza**, **Robyn W. Lin** *and* **Mary Kate Kamka** *are associates at Troutman Pepper Hamilton Sanders LLP.*