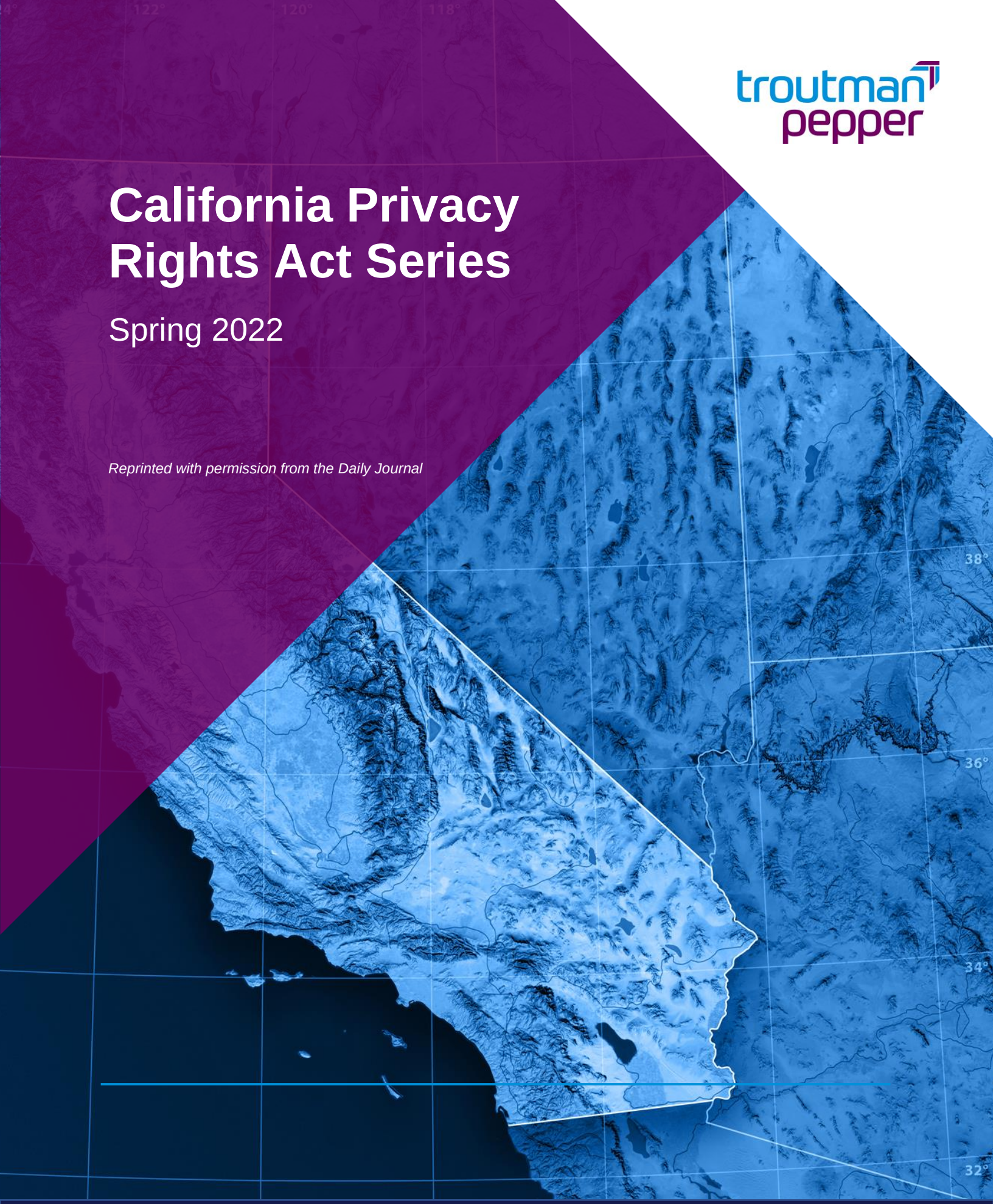
California Privacy Rights Act Series

Spring 2022

Reprinted with permission from the Daily Journal



troutman.com

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.*

LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, APRIL 20, 2022

MCLE

CPRA series part two: Consumer rights

By Ron Raether, Kamran Salour, Sadia Mirza, Whitney Shephard and Gerar Mazarakis

Most privacy laws derive from the same core foundational principles, namely the Fair Information Practice Principles (FIPPs). This includes the California Consumer Privacy Act of 2018 (CCPA), California Privacy Rights Act of 2020 (CPRA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), Health Insurance and Portability and Accountability Act of 1996 (HIPAA), Driver's Privacy Protection Act (DPPA), and even Europe's General Data Protection Regulation (GDPR).

Intended as guidelines that represent how organizations should collect and use personal information, the FIPPs recommend certain safeguards to ensure data collection practices are fair, and businesses are transparent about their privacy practices. In part, the FIPPs establish a framework for allowing consumers to have more control over how their information is collected and used. To this end, the Individual Participation Principle states that individuals should have the right to access, correct and delete their personal information.

Building on the Individual Participation Principle, the passage of the CCPA made California the first state to provide consumers with individual rights to give them more control over the personal information that businesses collect about them. Less than two years later, the CPRA adds certain consumer rights not available under the CCPA and amends certain CCPA consumer rights to provide additional rights to consumers.

Right to Access

Both the CCPA and CPRA grant consumers the "right to access." The CPRA expands this right by requiring businesses to disclose the business or commercial purposes for sharing consumers' personal information under certain circumstances.

While often referred to as the "Right to Know," the CCPA grants consumers the right to obtain from a business, subject to certain exceptions:

1. The categories of personal information it has collected about that consumer;
2. The categories of sources from which the personal information is collected;
3. The business or commercial purpose for collecting or selling the personal information;
4. The categories of third parties with whom the business shares personal information; and
5. The specific pieces of personal information collected about that consumer.

Right	CCPA	CPRA
Access	✓ Yes	✓ Yes
Delete	✓ Yes	✓ Yes
Correct Inaccuracies	× No	✓ Yes
Opt out of sale of PI	✓ Yes	✓ Yes
Opt out of sharing of PI	× No	✓ Yes
Limits on the processing of sensitive PI	× No	✓ Yes
Data Portability	✓ Yes	✓ Yes
No Discrimination	✓ Yes	✓ Yes

The CCPA and CPRA define "business" as an entity that alone, or jointly with others, determines the purposes and means of the processing of personal information, and that meets certain threshold criteria. For additional information about what qualifies as a "business" under the CPRA, please see Part One of this series, which ran in the Daily Journal on April 11.

The CCPA imposes a 12-month lookback from the time of the request. Therefore, consumers can access the personal information the business has collected about them within the 12 months before the date of their request. The CPRA will extend that 12-month window indefinitely requiring businesses to provide access to all categories and specific pieces of personal information collected unless the personal information is subject to an exception, or "unless doing so proves impossible or would involve a disproportionate effort." Neither "impossible" nor "disproportionate effort" is defined by the CPRA, providing some flexibility for businesses.

The CPRA affords consumers an additional right: the CPRA requires businesses to disclose the business or commercial purposes for sharing consumers' personal information. "Sharing" refers to disclosures by a business to a third party for cross-context behavioral

advertising, regardless of whether any money is exchanged. This new term is a welcome addition as it clarifies that these types of disclosures do not trigger the definition of "sale," which was a contentious issue under the CCPA.

For business covered by the GLBA, this right is broader than the "affiliate marketing rule" in that it allows consumers to opt out of the sharing of their personal information with any third party for certain advertising purposes (not just those affiliated with the business), but it is worth noting that businesses are not as limited in their ability to share personal information under the CPRA as they are under the GLBA.

Right to Delete

Both the CCPA and CPRA grant consumers the "right to delete." The CPRA expands this right by requiring businesses to notify service providers, contractors, and third parties of a consumer's deletion request.

Under the CCPA, California residents have the right to request that a business delete the personal information a business collected from the consumer. Upon receipt of a deletion request, businesses are required to delete the consumer's personal information from its records (subject to certain exemptions), and direct their service providers to do the same. The CCPA and CPRA refer to the entity that processes personal information on behalf of a business as a "service provider."

The CPRA expands the "right to delete" as it relates to service providers, contractors, and third parties. In addition to "notifying" (previously "directing") service providers to delete personal information subject to a deletion request, the CPRA requires businesses to notify "contractors" to delete the personal information, "and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort." The CPRA does not define what qualifies as a "disproportionate effort," leaving some flexibility for businesses but also requiring discipline and proper documentation.

The CPRA also places direct obligations on service providers and contractors that have been notified of a deletion request by the business to in turn notify any service providers, contractors, or third parties who may have accessed such personal information from or through the service provider or contractor. While cooperation between contracting tiers may have been necessary under the CCPA to effectively respond to deletion requests, the CPRA now makes a failure of service providers and contractors to have such operational mechanisms in place a direct violation of the law.

Right to Correction

The CCPA does not provide consumers with the "right to correction." The CPRA does contain a right to correct inaccurate information. It provides consumers with the right to "request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information …." Further, if such a request is received, a business is required to "use commercially reasonable efforts to correct the inaccurate information." Businesses are also required to disclose a consumer's right to request correction of inaccurate personal information in their California privacy policies.

While the CPRA does not further define what qualifies as "commercially reasonable efforts," businesses may want to rely on other privacy laws for guidance and use them as a tool to leverage instruction. This includes, for example, the FCRA, which requires consumer reporting agencies to correct or delete inaccurate, incomplete, or unverifiable information.

Right to Opt Out of Selling and Sharing of Personal Information

While the CCPA gives consumers the right to opt out of the "sale" of their personal information, the CPRA expands and clarifies this right with the introduction of a new opt out right, namely the right to opt out of the "sharing" of personal information under certain circumstances.

Under both the CCPA and CPRA, a "sale" is any disclosure of personal information to a third party "for monetary or other valuable consideration," unless the disclosure fits into one of the enumerated exceptions (e.g., there is an exception for transfers that are part of a merger or acquisition). This broad definition raised several questions for businesses engaged in behavioral advertising, namely as to whether the use of third-party cookies and similar tracking technologies triggered the definition of "sale."

The CPRA resolved this issue by introducing the concept of "sharing," which refers to transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business, even when no money is exchanged. If a disclosure qualifies as a "share," it will no longer be deemed a "sale" of personal information. Practically, however, both the sharing and selling of personal information trigger similar obligations. Among other things, businesses engaging in this type of processing activity must implement a conspicuous "Do Not Sell or Share My Personal Information" link on their internet homepages, which gives consumers the ability to opt out of the sale or sharing of their personal information.

Sensitive Personal Information

The CCPA does not limit the processing of "sensitive personal information." The CPRA provides that "consumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk to the consumer, and they should have meaningful options over how it is collected, used, and disclosed." The CPRA therefore expands the CCPA's definition of personal information to include "sensitive personal information," and imposes related data processing obligations.

A. Definition of "Sensitive Personal Information"

Although the CPRA suggests the unauthorized use or disclosure of "sensitive personal information" creates a heightened risk to consumers, it is worth noting the definition of "sensitive personal information" includes information well beyond those covered by California's data breach notification law. Indeed, sensitive personal information has been broadly defined to mean personal information revealing any of the following about a consumer:

- Social security, driver's license, state identification card, or passport number;
- 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;
- Precise geolocation;
- Racial or ethnic origin, religious or philosophical beliefs, or union membership;
- Contents of mail, email and text messages unless the business is the intended recipient; or
- Genetic data.

Sensitive personal information also includes the processing of biometric information to uniquely identify a consumer; personal information collected and analyzed concerning a consumer's health; and personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Because the definition goes beyond California's breach notification law, "sensitive personal information" has no bearing on Section 1798.150 of the CCPA/CPRA, which allows consumers to recover statutory damages in the event of a breach if certain steps are followed. Indeed, Section 1798.150 remains limited to "personal information," as that term is defined by California's breach notification law (not as defined by the CCPA/CPRA).

B. Right to Limit Use and Disclosure

Consumers have the right to restrict businesses' use of sensitive personal information: (i) to use that is necessary to perform the services or provide the goods requested; (ii) to certain "business purposes" identified in the Act; and (iii) as otherwise authorized by the regulations adopted under the CPRA. Businesses that use and disclose sensitive personal information for any other purpose must provide consumers with the ability to opt out of such use and disclosure. As with the right to opt out of the sale and sharing of personal information, businesses may offer this right through a new, separate link titled "Limit

the Use of My Sensitive Personal Information" posted on the business's internet homepage or, at the business's discretion, by utilizing a single, clearly-labeled link that allows a consumer to both 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.

After receiving direction from a consumer to not use or disclose sensitive personal information except for an authorized business purpose, a business is prohibited from using or disclosing the consumer's sensitive personal information for any other purpose, unless the consumer subsequently consents to the additional purposes. Likewise, service providers and contractors may not use sensitive personal information for purposes other than business purposes after being instructed by the business to do so.

Right to Data Portability

The CCPA gave consumers data portability rights by requiring businesses to disclose a copy of the consumers personal information in response to a verifiable request. The copy must be "in a readily usable format that allows the consumer to transmit [the] information from one entity to another without hindrance." Modifying the CCPA's data portability right, the CPRA mandates that the copy of the consumer's personal information be provided to the consumer in a format an average consumer would easily understand. Also, to the extent technically feasible, the information must be provided "in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance."

Businesses looking for further instruction as to what format is needed to comply with the CPRA's requirement should again consider relying on other privacy laws for instruction. The GDPR may prove useful here as it includes a similar right to data portability, as well as the FCRA, which requires consumer reporting agencies to provide consumers with the information included in their files.

Right to No Discrimination

Both the CCPA and CPRA grant consumers the "right to no discrimination." The CPRA expands this right with respect to employees and loyalty programs.

The CCPA prohibits businesses from discriminating against consumers for exercising their CCPA rights. While not defining discrimination, the CCPA provided a nonexclusive list including the following:

- Denying goods or services to the consumer;
- Charging different prices or rates for goods or services;
- Providing a different level or quality of goods or services; or
- Suggesting the consumer will receive a different price, rate, level, or quality of goods or services.

The CPRA maintains the "Right to No Discrimination" but clarifies two points. First, under the CPRA, retaliating against an employee for exercising their rights is a form of discrimination. This will likely remain regardless of whether personal information collected in the employment context becomes regulated data under the CPRA. For a detailed discussion relating to this point, see Part One of this series.

Second, this right does not prohibit businesses from offering loyalty, rewards, premium features, discounts, or club card programs. Conveniently following this language, however, is the CCPA/CPRA's "Notice of Financial Incentive" provision, which makes it permissible to offer financial incentives for the collection and use of personal information, provided that certain notice and opt-in requirements are met.

What to Expect from Anticipated Regulations?

While the CPRA gives businesses much to do to prepare for the January 1, 2023, operative date, businesses must still await completion of the anticipated regulations. The regulations are not expected to be complete until the third or fourth quarter of 2022. The anticipated regulations concerning consumer rights are expected to include the following:

- Access Rights. Regulations to define the term "specific pieces of information obtained from the consumer" to maximize a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful, such as system log information and other technical data.
- Opt Out Rights. Rules to facilitate and govern the submission of requests to opt out of the sale or sharing of personal information, including compliance with a consumer's opt-out request, and the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out.
- Right to Correct. Rules establishing how often, and under what circumstances, a consumer may request a correction of their personal information, 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 the correction of accurate information.
- Limitations on Processing of Sensitive Personal Information. Rules to facilitate the submission of consumer requests to limit the use of sensitive personal information, including higher authentication (identity verification) standards.
- Automated Decision-Making Technology. Rules governing access and opt-out rights concerning 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 for the consumer.

Ron Raether *and* **Kamran Salour** *are partners;* **Sadia Mirza** *and* **Gerar Mazarakis** *are associates and* **Whitney Shephard** *is an attorney at Troutman Pepper Hamilton Sanders LLP.*

LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, MAY 12, 2022

MCLE

CPRA series: Part III - Notice and disclosure obligations

By Ron Raether, Kim Phan, Grady Howe, Lissette Payne and Sadia Mirza

As we explained in an earlier installment, most privacy laws derive from the Fair Information Practice Principles (FIPPs). The FIPPs provide, in part, that consumers should be given notice of how their information will be used and shared, before their personal information is collected, to allow consumers to make an informed choice.

The California Consumer Privacy Act of 2018 (CCPA) imposes several notice and disclosure obligations on covered businesses. While the California Privacy Rights Act of 2020 (CPRA) did not modify when businesses are required to provide notice, it did make several important changes to the CCPA, which include changes to the following:

Updates to Notice at Collection

The CCPA requires that businesses provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used ("Notice at Collection").

The CPRA increases the amount of information that must be provided in the Notice at Collection. Prior to Jan. 1, 2023, the effective date of the CPRA, businesses will need to update their notices at collection to address the new and modified information to be provided to consumers. Under the CPRA, information provided in the Notice at Collection must include the following:

(1) Whether the collected personal information is sold or shared. Under the CCPA, companies that sold consumers' personal information data must disclose that practice. Under the CPRA, the definition of "selling" remains the same as it was under the CCPA, which includes various forms of sharing/disclosures of personal information by a business to another business or third party for valuable consideration. However, the CPRA extends the Notice at Collection disclosure obligations to include whether any categories of personal information are shared. Notably, the definition of "sharing" includes any disclosure of personal information for "cross-context behavioral advertising," which includes targeted advertisements based on a consumer's interactions with other businesses, websites, applications, or services. For further information on selling and sharing (and the distinction between the two), please see Part 2 of this series.

(2) Sensitive Personal Information. Under the CCPA, businesses must include in the Notice at Collection the categories of personal information collected about consumers. The CPRA creates a new category of personal information – "sensitive personal information." As such, under the CPRA, the Notice at Collection disclosure obligations are extended to include the categories of any sensitive personal information collected and the purposes for collection of such sensitive personal information.

(3) Data Retention. Under the CPRA, businesses must include in their Notice at Collection the length of time each category of personal information, including sensitive personal information, will be retained. If it is not possible to state how long the data will be retained, businesses must include the criteria used to determine the retention period. Either way, no personal information is allowed to be retained for longer than is reasonably necessary for the disclosed purpose in the Notice at Collection.

From a practical perspective, the modifications to the Notice at Collection will require many businesses to revisit their data maps to ensure they are capturing the information not previously required by the CCPA (i.e., sensitive personal information, data retention periods, whether information is being "shared," etc.). While there is still some hope the CPRA will exclude personal information collected in the employment context (see Part One for additional information), businesses should plan on reviewing their Notices at Collection relating to employee data to determine what modifications will be required, if any.

Updates to Notice of Financial Incentive

Under the CCPA, a business must disclose the material terms of any financial incentive the business offers to consumers as compensation for the collection or sale of personal information. The CPRA extended this disclosure obligation to also include the material terms of any financial incentive the business offers to consumers for the sharing or retention of their personal information as well.

Updates to Privacy Policy

Under the CCPA, businesses' privacy policies must provide a comprehensive list of their online and offline practices regarding the collection, use, disclosure, and sale of personal information, as well as the rights of consumers regarding their personal information. Additionally, businesses must develop and post a privacy policy that informs consumers about the existence of, and guidance on how to exercise, their CCPA rights.

The CPRA modifies certain rights provided for in the CCPA, while also adding several others. The extended and additional rights include:

(1) Right to opt out of the sale and sharing of personal information. As mentioned above, the CPRA requires a business to provide a notice to inform consumers of their right to direct a business that "sells" their personal information to stop selling their personal information. Information on the right to opt out of the sale as well as the new right to opt out of the sharing of personal information, and the method for exercising these rights, must be included in a CPRA compliant privacy policy.

Furthermore, under the CCPA, a business that sold consumer data must disclose that information and include a "Do Not Sell My Personal Information" link on its homepage. Accordingly, the CPRA adds that the "Do Not Sell" link referenced above must be edited to "Do Not Sell or Share My Personal Information."

With regards to the sharing of consumers' personal information, the CPRA also requires that the privacy policy disclose a list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories

that most closely describe the personal information sold or shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(2) Right to limit the use and disclosure of sensitive personal information. The CPRA requires businesses, upon request by a consumer, to limit the use and disclosure 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. Businesses that use and disclose sensitive personal information for any other purpose must provide consumers with the ability to opt out of such use and disclosure.

(3) Right to Correct/Rectification. The CPRA provides consumers the right to request that inaccurate information held on them is corrected. Information on the right to correct/rectification, and the method for exercising this right, must also be included in the privacy policy.

The CCPA regulations, 11 CCR §§ 999.308, had also expanded the content to be included in privacy policies, which were enacted into law by the CPRA by requiring in the statute that privacy policies include the following information:

(1) The categories of sources from which consumers' personal information is collected.

(2) The business or commercial purpose for collecting or selling consumers' personal information, and under the CPRA also for sharing consumers' personal information.

(3) The categories of third parties to whom the business discloses consumers' personal information.

The CPRA did not otherwise impact the other content requirements for privacy policies as set forth in the CCPA regulations.

Disclosure Updates in Response to Requests to Know

The CCPA allows consumers to submit a "Request to Know" for a business to disclose its collection and treatment of the consumer's personal information during the past twelve months, which includes the following:

(1) The categories of personal information the business collected about the person;

(2) The categories of sources from which the personal information was collected;

(3) The business or commercial purpose for collecting or selling the personal information;

(4) The categories of third parties with whom the business shares personal information; and

(5) The specific pieces of personal information it has collected about that consumer.

The CPRA modifies these disclosures in the following ways:

(1) Businesses must now provide information about the business or commercial purpose for sharing personal information. "Shared" is defined as providing personal information to a third party for cross-contextual behavioral advertising.

(2) Clarifies that if the consumer requests that the business disclose the required information beyond the 12-month period, then the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. This change will only apply to data collected on or after January 1, 2022.

(3) Directly requires service providers and contractors to aid businesses in responding to a verifiable consumer request.

(4) Clarifies that businesses must provide specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance.

(5) Clarifies that personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

Changes to Opt-Out Preference Signals

The CPRA contemplates the creation of an "opt-out preference signal," which would indicate consumers' intent to opt-out of a business' sale or sharing of their personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both. The CPRA indicates that the signal would be sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in future regulations. Businesses would be able to elect whether to utilize opt-out links or the opt-out preference signal to satisfy their CPRA obligations. The CPRA does not clearly define an "opt-out signal," but time will tell if it will be treated as synonymous with what was described in the CCPA regulations as a "user-enabled global privacy control." There, the CCPA regulations defined such a mechanism as "a browser plug-in or privacy setting, device setting, or other mechanism that communicates the consumer's choice to opt-out."

What to Expect from Anticipated Regulations?

As discussed in the previous installments of this series, the California Privacy Protection Agency is now responsible for updating existing regulations and adopting new regulations concerning the CPRA. Relevant to notice and disclosure obligations, the CPPA is expected to issue regulations to:

(1) Ensure that the notices and information are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer;

(2) Define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data;

(3) Require 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; and

(4) Harmonize the various notices to consumers to promote clarity for consumers.

The timeline for adopting these new regulations under the CPRA was set for July 1, 2022. The CPPA has already stated that it will miss the deadline. Under the CCPA, businesses had almost two years between when the CCPA was enacted and when the Attorney General was empowered to bring enforcement actions for CCPA non-compliance. Similarly, the CPRA provides businesses a little more than two years to adjust their existing practices to comply with the new obligations in the law. On Jan. 1, 2023, the CPRA will go into effect. Beginning July 1, 2023, the CPPA will begin enforcing the new obligations added by the CPRA. By this date, business notices, policies and other required disclosures should be fully compliant with the requirements of the CPRA to avoid the risk of an enforcement action. However, it remains to be seen when the regulations will be finalized, including when businesses will be required to comply with any such regulations.

Ron Raether and Kim Phan *are partners, and* **Grady Howe, Lissette Payne** *and* **Sadia Mirza** *are associates at Troutman Pepper Hamilton Sanders LLP.*

LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, MAY 23, 2022

MCLE

CPRA Series: Part IV

Data Processing Obligation

By Ron Raether, James Koenig, Kamran Salour, Sadia Mirza, Graham Dean, Edgar Vargas, and Kamran Salour

The California Privacy Rights Act ("CPRA") will significantly impact how entities process personal information requiring covered businesses to review and update their existing vendor agreements. The CPRA also includes additional requirements for specific data processing activities that may present heightened risks regarding consumers' data security and privacy. Part 4 provides an overview of these new requirements and includes practical advice for businesses to consider as they roll out their CPRA compliance programs.

Understanding the Relevant Terminology

As discussed in previous articles in this series, the term "business" refers to an entity "that collects consumers' personal information" and "determines the purposes and means of the processing of consumers' personal information." The CPRA uses this terminology to refer to what many other privacy regimes call the controller.

With the CPRA, external entities that process a business's personal information will fall into one of three categories: (i) service providers, (ii) contractors, (iii) third parties. The term "service provider" refers to persons that receive consumer personal information from/on behalf of a business, which carry out processing activities on behalf of a business for a business purpose under a written contract. One of the significant differences between the California Consumer Privacy Act ("CCPA") and CPRA is the CPRA's introduction of the term "contractor." This term refers to persons "to whom the business makes available a consumer's personal information for a business purpose" under a written contract. Unlike service providers, contractors do not carry out processing activities on behalf of the business. 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 to the entity for an alternative purpose (e.g., a business disclosing records to an auditor that may include certain personal information). Persons that do not qualify as a covered "business," "service provider," or "contractor" are referred to as "third parties." Notably, selling or sharing (for purposes of cross context behavioral advertising) personal information with third-parties triggers disclosure requirements for covered businesses as well as consumer opt-out rights.

The term "contractor" is a welcomed change. Before the enactment of the CPRA, the CCPA forced many privacy practitioners to describe contractors as "restricted third parties" or "1798.140(w)(2) persons" —due to an unwritten and compli-

CPRA Contractual Requirements for Service Providers and Contractors

	Contractors	Service Providers
Selling & Sharing Restrictions	May not "sell" or "share" personal information.	
Processing PI	May not retain, use, or disclose personal information: (i) for any purposes other than those specified in the contract, or (ii) outside of the direct business relationship.	
Combining PI	May not combine personal information received from the business with other personal information received on behalf of another person or collected through its interactions with the consumer, except as otherwise permitted by statute or regulation.	
Sub-Processors	Must notify businesses when sub-processors are processing personal information and must bind these sub-processors to the same processing obligations.	
Complicance Certification	Must provide certification that the contractor understands the four restrictions listed above.	No certification requirement.
Compliance Monitoring	Must permit compliance monitoring by the covered person.	No compliance monitoring requirement.

cated exception. The CPRA eliminated that ambiguous language in the CCPA definition of third party and filled the logical gap by incorporating the "contractor" terminology and concept.

Understanding these terms is essential for several reasons. The CPRA's opt-out rights apply to third parties but do not apply to contractors or service providers. Furthermore, subtle differences in the definitions and requirements for contractors and service providers (described below) may impact an entity's ability to process data.

Contract Requirements for Service Providers and Contractors

While the required contract provisions needed to establish service provider and contractor relationships are very similar, there are subtle differences that businesses must consider. As indicated in the chart below, the different contractual requirements revolve around compliance certification and monitoring. These differences seem to be driven by the CPRA drafters' desires to ensure checks are in place to govern the slightly broader range of processing activities in which contractors may engage. Businesses are not required to include these terms in their contracts with third parties.

New 1798.100(d) Requirements

In addition to the requirements discussed above, Section 1798.100(d) of the CPRA includes five items that must be included in the applicable business contracts. These requirements apply to third parties, service providers, and contractors (collectively, "Data Recipients"). Specifically, this new subsection requires agreements to:

(1) Specify personal information is sold or disclosed by the business only for limited and specified purposes;

(2) Obligate the Data Recipient to comply with applicable CPRA obligations, which includes providing the CPRA-level of privacy protection to covered information;

(3) Grant the business rights to take reasonable and appropriate steps to help to ensure that the Data Recipient uses the personal information transferred in a manner consistent with the business's CPRA obligations;

(4) Obligate the Data Recipient to notify the business if it determines that it can no longer meet its CPRA obligations; and

(5) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information.

Other CPRA-Related Considerations for Data Processing

A. Audits and Risk Assessments

Section 1798.185(a)(15) of the CPRA requires the California Privacy Protection Agency (CPPA) to issue specific regulations for businesses "whose processing of consumer's personal information presents significant risk to consumers' privacy or security" under which such businesses must:

(A) 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; and

(B) Submit to the CPPA on a regular basis a risk assessment with respect to their processing of personal information, including identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing.

While specific examples of "significant risk" have yet to be provided, the CPRA states that the regulations should ensure both the "the size and complexity of the business" and "the nature and scope of processing activities" should be considered. Businesses in need of further instruction may also look to Europe's General Data Protection Regulation (GDPR) for guidance, which imposes a requirement on covered entities to conduct similar "data protection impact assessments" when data processing activities are likely to result in a "high risk to the rights and freedoms of natural persons."

B. Information Security

In addition to the aforementioned cybersecurity audit requirements, the CPRA requires that all covered businesses engaged in the collection of personal information "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."

Not surprisingly, the CPPA has not been tasked with further defining "reasonable security procedures" as what qualifies as reasonable will be unique to each organization, and will depend on factors such as the products and services offered (e.g., on-prem vs. SaaS solutions), nature of data collected, the size of the organization, available resources, and the like. As such, businesses should continue to rely on guidelines and frameworks when making decisions (e.g., NIST Cybersecurity Framework, Top 18 CIS Controls (previously the Top 20 CIS Controls), etc.). Notably, the California Attorney General has even provided its view that the Top 18 CIS Controls represent the "minimum level of information security that all organizations that collect or maintain personal information should meet," which suggests that such controls represent the baseline for "reasonable security procedures and practices," at least in California.

C. Disclosures Related to Automated Decision-Making

The CPRA requires the CPPA to issue 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."

While automated decision-making is not defined in the CPRA, the term profiling is defined to include "any form of automated processing of personal information […] to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

In the absence of issued regulations, the CPRA does not directly obligate businesses to disclose their use of automated decision-making technology or provide any related opt-out rights. Regardless, given the direction in which privacy laws are headed (i.e., increased transparency and reducing the likelihood of discriminatory outcomes), businesses using automated decision-making technology should get ready. Steps businesses can take now include:

- Identifying the data used or created through automated decision-making technology;
- Creating summaries of the logic used for automated decision-making technology;
- Preparing policies and procedures explaining the likely outcome of these covered activities; and
- Creating procedures to allow for manual decision-making in instances where a consumer has exercised their opt-out rights.

Businesses that are heavily reliant on automated decision-making technologies may also want to consider adjusting their processes to include some level of human intervention. In Europe, under the GDPR, even a minimal amount of human intervention is sufficient to exempt a process that would otherwise be regulated as automated decision-making.

What's Next?

All covered businesses should begin reviewing their vendor contracts to determine whether amendments are needed to comply with the new contractual requirements discussed above. Covered businesses should also consider whether they are acting as a service provider, contractor, or third party in some contexts. For instance, a software provider may, on one hand, be a covered business when processing its employees' personal information (see Part One of this Series for further information about the status of the employee data exemption under the CPRA) and, on the other hand, be a covered service provider regarding the personal information it processes on behalf of its customers. In these instances, businesses should prepare contractual language that covers both roles, and may also want to clarify in its privacy policies its dual positions.

In some instances, contracts that arguably meet the CPRA's requirements should also be updated as a matter of best practice. For example, businesses with contracts containing broad obligations regarding the vendor's assistance with data privacy compliance matters should consider seeking more specific terms covering the Section 1798.100(d) obligations. Of course, contracts governing data-intensive processing activities should be the first priority. Businesses should also consider amending their standard template agreements or data protection addendums to address the CPRA's requirements.

Businesses should also begin evaluating the nature of their data processing activities to determine which new CPRA requirements may apply. In addition to updating contracts, initial efforts should focus on processing activities that may be considered high-risk, as well as processing that may constitute automated decision-making, bearing in mind the regulations are expected to address both of these issues so some flexibility in compliance procedures will be required.

Ron Raether, James Koenig *and* **Kamran Salour** *are partners;* **Sadia Mirza,** *and* **Graham Dean** *are associates and* **Edgar Vargas** *is an attorney at Troutman Pepper Hamilton Sanders LLP.*

LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

THURSDAY, MAY 26, 2022

PERSPECTIVE

CPRA Series: Part V - Litigation and Enforcement

By Josh Davey, Daniel Waltz, Ron Raether, Jim Koenig, Sadia Mirza, and Kamran Salour

Introduction

As discussed in the previous installments of our series on the California Privacy Rights Act of 2020 (CPRA or the Act), the CPRA is leading the charge in how many regulators and companies address privacy, creating new consumer rights and imposing new obligations on businesses covered by the Act. Along with these new rights and obligations come new enforcement mechanisms – including the creation of the California Privacy Protection Agency (the Agency) – the first regulatory agency in the United States dedicated to consumer privacy issues – and the expansion of private enforcement through litigation. Although the CPRA's substantive provisions go into effect on Jan. 1, 2023, the Act contains a "lookback" provision to Jan. 1, 2022, which means that companies must be prepared for potential enforcement activity for the decisions they are making today.

In this fifth and final installment of our series on the CPRA, we provide an overview of expected enforcement activity, both by the Agency as well as through private enforcement. We also provide compliance guidance to businesses that will be governed by the CPRA.

CPRA Enforcement by the Agency

Shared Enforcement Authority with California Attorney General

Created to regulate consumer data privacy and enforce state privacy laws, the Agency's five-member board was appointed on March 17, 2021, and Ashkan Soltani was selected as the Agency's first Executive Director on October 4, 2021.

The Agency has the authority to investigate possible violations of the CPRA upon the sworn complaint of any person or on its own initiative, and to bring an administrative action to enforce violations. However, this authority is discretionary, and the Agency may choose not to investigate a complaint. In addition, the Agency is charged with cooperating with other privacy enforcement agencies, including those in other states, territories and countries.

Although the Agency has the power to "[a]dminister, implement, and enforce" the Act "through administrative actions," the California Attorney General retains civil enforcement powers, and can seek an injunction and/or penalties in a civil action. While enforcement authority is shared, the Agency is expected to take the lead on administrative enforcement once the agency has achieved enforcement readiness and final regulations are adopted. Under the Act, enforcement is set to begin July 1, 2023, and will apply to violations occurring on or after that date. Until that time, the Attorney General is expected to continue enforcement under the existing CCPA regulations. With the resources of both agencies in action, we anticipate robust enforcement of the CPRA and a potential increase in regulatory enforcement actions and more intense scrutiny of business practices.

Elimination of Cure Period

The CPRA eliminates the 30-day cure period that currently applies to CCPA enforcement by the Attorney General, and instead grants both the Attorney General and the Agency discretion whether to offer a cure period. The Act identifies several factors that the Agency "may" consider in deciding whether to permit a cure period, including the business's lack of intent to violate the Act as well as voluntary efforts undertaken by the business to cure the violation. The CPRA authorizes the Agency to impose fines ranging from $2,500 to $7,500 per violation (the same as the CCPA) regardless of any opportunity for cure, subject to the enforcement process set out in the Act.

Litigation and Enforcement	CCPA (2020)	CPRA (2023)
Private Right of Action for Violations of the Act	No	No
Private Right of Action for Data Breaches	Yes	Yes
Data Breach Cure Period	Yes	Yes
AG Enforcement Action	Yes	Yes
Enforcement Cure Period	Yes	Discretionary
Agency Enforcement Action	No	Yes
Agency Cure Period	N/A	Discretionary, notice of probable cause hearing required
Effective Date	January 1, 2020	January 1, 2023
Enforcement Date	July 1, 2020	July 1, 2023
Look-back Date	Jan. 1, 2019	Jan. 1, 2022
Retroactive	No	No
Requirement to Adopt Implementing Regulations	Yes	Yes
Rulemaking Subject to Open Meetings Act	No	Yes
Number of Mandates for Creation of Regulations	7	22
Number of Pages of Final Regulations	23	TBD

Procedure for Administrative Enforcement

The CPRA provides that administrative enforcement by the Agency will use a "probable cause" standard, and that the service of the probable cause notice constitutes the commencement of the administrative action. Entities alleged to have violated the Act must be given at least 30 days' notice, be provided with a summary of the evidence, and be informed of their right to be present

and have counsel at any proceeding held by the Agency. The Agency has the power to obtain subpoenas in aid of any enforcement proceeding. Administrative actions under the CPRA generally must be commenced within five years of the violation, although the Act provides exceptions to this limitation in the event of fraudulent concealment of information or in the case of delay in responding to a subpoena issued in the course of such proceeding. The Act further provides for judicial review of Agency enforcement decisions "in an action brought by an interested party to the complaint or administrative fine" under an abuse of discretion standard.

Penalties

If, after a hearing, the Agency determines that a violation has occurred, the Agency can issue a cease and desist order as well as impose a fine of up to $2,500 for each violation or up to $7,500 for each intentional violation or for violations involving the personal information of a minor consumer.

In a civil action by the Attorney General, the available penalties are the same. In a civil action, the Act provides that the "court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty."

The Act also makes provision for the dual enforcement authority of the Agency and the Attorney General. For example, the Attorney General can ask the Agency to stay administrative actions or investigations to permit the Attorney General to proceed with its own investigations and/or civil actions. Under the CPRA, the Agency must defer to such requests and "may not limit the authority of the Attorney General" to enforce the Act. Additionally, the Attorney General cannot file a civil action against a person for the same violation that has been the subject of an administrative penalty, and the Act also provides that "[a] business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation."

Retroactivity

As discussed in our previous installments, the CPRA's substantive requirements are effective Jan. 1, 2023, and enforcement of its provisions may begin at that time. However, CPRA includes a "lookback" provision which makes its provisions applicable to information collected on or after Jan. 1, 2022. There is good news for businesses that are already compliant with the CCPA and a warning for those still waiting to get into compliance.

Agency Funding and Enforcement Impact

The Agency will begin work with an annual budget of $10 million, which is nearly twice what the AG's office budgeted for enforcement of the CCPA. As a result, the Agency will have more dedicated employees to pursue more businesses for alleged violations and is expected to employ 34 staff members and attorneys to carry out its mission. These resources are in addition to those already deployed by the Attorney General's office.

Additionally, the Act provides for the creation of a Consumer Privacy Fund that will provide most funding for the Agency moving forward. The Consumer Privacy Fund will be funded by recoveries under the CPRA in enforcement actions. The majority of fines deposited into the Consumer Privacy Fund will be used to offset costs incurred by the Attorney General and the courts for enforcement actions, invested for the benefit of California taxpayers, to support the Agency, and the remainder will be used for grants to promote education and non-profit initiatives to increase visibility and awareness about privacy related issues. Therefore, the Agency is incentivized to vigorously enforce provisions of the CPRA. It is unclear whether the Agency or Attorney General expect recoveries to exceed the annual budget. Regardless, businesses should assume that regulators will be looking to offset the expense to California taxpayers with recoveries under the Act and be prepared for enforcement to begin after July 2023.

Private right of action

Like the CCPA, no private right of action exists under the CPRA for alleged violations of the Act. However, the CPRA expands upon the private claim that already existed under the CCPA for data breaches – i.e., where a consumer's "nonencrypted and nonredacted personal information… is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

The CPRA's private right of action provision incorporates the definition of "personal information" used by the CCPA, which means "[a]n individual's first name or first initial and the individual's last name in combination with" a number of data elements identified in the Act, "when either the name or the data elements are not encrypted or redacted." These data elements include Social Security number, driver's license, passport, or other unique government identification number, account number or credit or debit card number in combination with any required password or code to access the account, medical, health or genetic data, or unique biometric data. However, the CPRA also expands on the CCPA's definition of personal information by including an "email address in combination with a password or security question and answer that would permit access to the account" in the list of personal information whose breach gives rise to a cause of action. We expect that this expansion of the definition of personal information will result in increased consumer litigation following data breaches.

Consumers who prove entitlement to recovery may recover damages between $100 and $750 per consumer per incident, or actual damages, whichever is greater, and may obtain injunctive or declaratory relief. The Act provides that in assessing the amount of statutory damages, the court shall consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Before instituting a private action, CPRA requires consumers to provide a business with a 30-day written notice of the alleged violation. If the business cures the violation and provides the consumer with an "express written statement" to that effect, the consumer cannot sue. However, this notice requirement and cure period is only applicable if the consumer is seeking statutory damages, not if the consumer is only seeking actual pecuniary damages. Additionally, the Act makes clear that "[t]he implementation and maintenance of reasonable security procedures and practices… following a breach does not constitute a cure with respect to that breach." And, businesses may also be subject to litigation if they fail to abide by any "express written statement" provided to a consumer.

The civil action provision of CPRA is effective Jan. 1, 2023.

Impact of pending rulemaking

Under the CPRA, the Agency assumes responsibility for rulemaking activity from the Attorney General. Moving forward, the Agency will then have sole responsibility for promulgating, revising, and implementing regulations interpreting both the CCPA and CPRA.

Much like the rulemaking process under the CCPA, the CPRA requires that the Board:

- Begin the informal rulemaking process;
- Receive public comments on proposed rules/regulations;
- Modify the regulations and rulemaking package to account for public comment;
- Prepare the final rulemaking package;
- Send the rulemaking package to the Office of Administrative Law for review and approval;
- The Secretary of State must adopt the regulations.

Unlike the rulemaking process under the CCPA, however, the Agency must comply with California's Bagley-Keene Open Meeting Act, which requires the board to conduct its meetings and make all decisions in public. Transparency comes at the expense of efficiency. As a result, and as the Agency has already suggested, it is unlikely that the Agency will have final regulations approved by the July 1, 2022 deadline.

Subcommittees are permitted to meet in private so long as only two board members are present and they only work to advise the Board. The Agency consists of three subcommittees that will advise the Board in the following areas:

- Regulations: Provide guidance on planning and priorities for the rulemaking process.
- Public Awareness and Guidance: Ensure consumer visibility and guidance for consumers and business with respect to CPRA requirements.
- Administration: Manage administrative issues involved in the creation of the Agency (e.g. staffing and internal policy).

The CPRA includes a mandate for the development of new or additional regulations in 22 specifically enumerated areas. In contrast, the CCPA only included seven mandates which resulted in 23 pages of CCPA regulations. Under the CPRA, the Agency is directed to develop new rulemaking regarding issues such as establishing definitions under the CPRA, ensuring consistency with federal and state privacy laws, developing rules related to consumer exercise of privacy rights, setting civil penalties, harmonizing the CPRA with other laws and regulations, and clarifying the scope of Agency's authority. We anticipate that regulations promulgated by the Agency will be significantly more voluminous than those promulgated by the Attorney General under the CCPA.

The Agency has already begun initial informal rulemaking, with the public comment period held from Sept. 21, 2021 through Nov. 8, 2021. Preliminary public comments are available on the Agency's website, here. The initial rulemaking process sheds some light on the regulatory

priorities with respect to the following topics:

• Definitions: how terms and concepts should be defined, including but not limited to the definitions of personal information, sensitive personal information, de-identified information, geolocation, and dark patterns.

• Identification of significant privacy and security risk: identifying processes and practices that pose significant privacy and security risks (and which processes and practices will require annual security auditing and risk assessment reporting under the CPRA).

• Automated Decision-making: what information is necessary for businesses to share about automated decision-making processes employed by the business.

• Agency Audits: the scope of Agency's authority to audit a businesses' compliance with CPRA and applicable privacy laws and regulations.

• Consumer Rights: defining the rights added under the CPRA, such as the right to correct, right to opt out of sharing, and the right to limit the use of sensitive personal information.

• Consumer Requests: understanding the challenges businesses may encounter when responding to consumer requests for data collected by the business for time periods longer than the CCPA's requirement for access to data for the preceding 12-months.

As of the writing of this series, the Agency has not commenced formal rulemaking. The Agency's final deadline to promulgate regulations is currently July 1, 2022, which will allow companies time to comply before the CPRA goes into effect on Jan. 1, 2023. However, the Agency has already indicated that final regulations likely will not be ready until the fourth quarter of 2022. Enforcement of the CPRA will begin July 1, 2023, but the Agency may need to exercise discretion to allow sufficient time for businesses to interpret and respond to the final regulations.

Litigation and Enforcement: Comparison of Key Provisions

While the CCPA forms the foundation of California's privacy protection framework, the CPRA continues to evolve that framework and significantly amends the CCPA to strengthen consumer privacy protections and regulate the technology industry. Some of the notable similarities and differences between the CCPA and CPRA are highlighted in the table, below, to illustrate the evolution of California's privacy law enforcement efforts.

Conclusion

Throughout this Series we have discussed the many changes between the CCPA and CPRA to provide covered businesses with tools to evaluate compliance and plan for a different privacy landscape beginning January 2023. It is important for businesses to take note of these changes and plan accordingly because compliance with the CPRA currently required by the look-back period.

On July 1, 2023, the Agency will begin enforcement activities and we anticipate an immediate increase in regulatory oversight. Plaintiffs' attorneys are equally eager to bring litigation under the expanded private right of action. Companies should consider the following actions to mitigate regulatory and litigation risk:

• Conduct a CPRA compliance gap analysis to understand what efforts are still required to bring the company in line with the CPRA.

• Ensure that company management and the board are aligned to support CPRA compliance objectives and that key stakeholders are accountable for meeting compliance deadlines.

• Create a "crown jewels" inventory of data collected from consumers. Ensure that the "crown jewels" (e.g., financial information, personally identifiable information and all categories of "sensitive personal information") are carefully mapped and the company understands data flows of consumer information.

• Prepare for annual risk assessments by ensuring that cyber security measures are effective, and that data is adequately protected.

• Make sure that the company is engaging in data minimization practices and that data retention requirements are closely followed and documented.

• Audit and revise internal policies, procedures and practices to align with CPRA requirements.

• Conduct an audit of third-party agreements to ensure compliance and alignment with the CPRA. Make sure that any agreements with data processors are in writing, set forth the instructions for processing data, and describe the types of data shared. Also ensure that contracts prohibit vendors from sharing, using, or aggregating personal information outside the business purpose for the relationship.

• Maintain a list of third-party vendors and partners with whom consumer information is shared, including what information is shared and for what purpose. Also ensure that third-parties are aware of the company's data retention policy and agree to a cadence for data destruction that aligns with the CPRA's data minimization and retention requirements.

• Update publicly facing privacy policies on the company website.

• Ensure the company website contains information about how a consumer can exercise his/her privacy rights and confirm that the business has a documented and effective process to honor those requests

---

Josh Davey, Ron Raether, Jim Koenig *and* **Kamran Salour** *are partners and* **Daniel Waltz** *and* **Sadia Mirza** *are associates at Troutman Pepper Hamilton Sanders LLP.*

CONTACTS

Ronald Raether
Partner
ron.raether@
troutman.com
949.622.2722

Jim Koenig
Partner
jim.koenig@
troutman.com
212.704.6363

Joshua Davey
Partner
joshua.davey@
troutman.com
704.916.1503

Kim Phan
Partner
kim.phan@
troutman.com
202.274.2992

Kamran Salour
Partner
kamran.salour@
troutman.com
949.622.2441

Sadia Mirza
Associate
sadia.mirza@
troutman.com
949.622.2786

Graham Dean
Associate
graham.dean@
troutman.com
919.835.4142

Grady Howe
Associate
grady.howe@
troutman.com
949.622.2445

Mary Kate Kamka
Associate
marykate.kamka@
troutman.com
415.477.5751

Robyn Lin
Associate
robyn.lin@
troutman.com
949.622.2447

Gerar Mazarakis
Associate
gerar.mazarakis@
troutman.com
202.220.1454

Lissette Payne
Associate
lissette.payne@
troutman.com
704.916.1514

Whitney Shephard
Attorney
whitney.shephard@
troutman.com
617.443.3709

Edgar Vargas
Attorney
edgar.vargas@
troutman.com
949.622.2473

Daniel Waltz
Associate
daniel.waltz@
troutman.com
312.759.5948