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.*