# California Strikes Back ... for Data Privacy!

The California Privacy Rights Act (CPRA) will largely take effect on Jan. 1, 2023, adding a handful of rights for California consumers and new obligations for businesses, which will be enforceable by the California Privacy Protection Agency, a new state privacy regulatory agency created by the CPRA.

By **Scott M. Smedresman and Morgan Jones** | January 22, 2021

Well, California is at it again. Less than one year after the California Consumer Privacy Act (CCPA) took effect, the people of California voted to approve Proposition 24 (aka the California Privacy Rights Act, the CPRA) on Election Day 2020. The CPRA will largely take effect on Jan. 1, 2023, adding a handful of rights for California consumers and new obligations for businesses, which will be enforceable by the California Privacy Protection Agency, a new state privacy regulatory agency created by the CPRA.

## Concepts

The CPRA has added several new concepts and definitions, some of which are borrowed from the EU's General Data Protection Regulation (GDPR):

- Data minimization, which dictates that only data that is necessary and proportionate to the purpose be collected and processed;

- Purpose limitation, where without notice and additional permissions, data is not used beyond the original purpose(s) for which the consumer provided it, or a reasonably expected purpose stemming from the original purpose; and

- Storage limitation, requiring the data not be held longer than reasonably necessary. Businesses should start analyzing what information they are collecting, whether it is "necessary," how it is used, and what the "necessary" retention period is, given the purpose of processing and any legal obligations they may have.

This amendment also creates a new category of personal information called sensitive personal information (SPI), which is comprised of government-issued numbers (e.g., Social Security number, driver's license number, passport number); account login information with password or security question(s) and answer(s); racial/ethnic information; religious affiliation' the contents of a consumer's email, text messages, or postal mail (if the business isn't a party to the communication); and health, biometric, and genetic data. This information was already covered by the broad definition of "personal information" in the CCPA, but has now been made an explicit category with certain additional notification obligations (e.g., point of collection, privacy policy) and rights.

## Rights

The CPRA doesn't just introduce GDPR-based concepts into California privacy law, it adds consumer rights that closely align with rights under the GDPR. The following rights were added by the CPRA:

- the right to correct personal information;

- the right to opt out of sharing of information for online behavioral advertising;

- the right to restrict the use and disclosure of SPI, which bolsters the concepts of data minimization and purpose limitation above; and

- the right to be free from automated decision making, which comes with certain rights to information regarding such decision making.

Automated decision making is the process of making a decision by automated means without any human involvement, and can affect the rights of consumers. This type of processing can be based on profiles, which are used to analyze and predict consumer traits (e.g., whether someone would be approved for a loan).

Some consumer rights have been updated by the CPRA. The right to deletion, for instance, is now an obligation that must flow down to third parties, service providers, and contractors (a new category of party) that received the personal information from the business responding to the request for deletion, though this is still subject to a few exceptions. Through the CPRA, the right to access personal information held by a business has been expanded to allow for the consumer to request more than the previous 12 months of personal information collected, shared, or sold by a business (if any—no retention obligation is imposed). This expanded right shall not apply to data collected, shared, or sold prior to Jan. 1, 2022. Finally, the right of data portability was revised slightly to address the formatting of the data sent to consumers so that it is easier for them to transfer to another business.

## Obligations

Businesses will face more obligations because of the CPRA, and this will affect a different grouping of entities because the definition of "business" has been revised. The previous threshold criteria of having the personal information of 50,000 or more California consumers, households, or devices has been revised to 100,000 or more California consumers or households in order to exclude more small businesses from having to comply with the CPRA.

The CPRA also amended the third threshold criteria indicating that a business can also be an entity which derives 50% or more of its annual revenue from selling consumers' personal information to now also include "sharing" of data. This is important because cross-context behavioral advertising (CCBA), which was introduced by the CPRA, counts as sharing personal information, leading to many ad-tech and mar-tech companies being considered businesses and subject them to the consumer's new right to opt out of sharing of personal information. (CCBA is the gathering of data on consumers across multiple platforms, sites, etc. to deliver targeted advertising to consumers.)

In certain instances, businesses will have to obtain the consent of consumers before acting, which is a newly defined standard. Similar to the GDPR, the CPRA now defines consent as "any freely given, specific, informed and unambiguous indication of the consumer's wishes." Such consent would have to be obtained in relation to the use of SPI, to use personal information or SPI for new purposes, and for opt-in scenarios, such as for minors to consent to sales and sharing of their information and when attempting to get consumers to opt back in to the sale of their information after opting out previously.

Previously left as an option, businesses will now have to enter into written contracts with service providers and contractors to ensure that the consumer personal information is adequately protected and that businesses can enforce the flow-down obligations, such as deletion pursuant to a consumer's request. Because of this, businesses will have to begin drafting and negotiating contracts with service providers.

In addition to the "Do Not Sell My Information" link required by the CCPA, the CPRA will require businesses to add "Do Not Share My Information" and "Limit Use of My Sensitive Personal Information" links to conform with the newly created consumer rights.

Data security and privacy laws are constantly changing, but the McCarter team is here to help your business navigate these new requirements.

**Scott M. Smedresman** *is a partner and* **Morgan Jones** *is an associate at McCarter & English. They can be reached at ssmedresman@mccarter.com and mjones@mccarter.com, respectively.*