Published on *The National Law Review* https://natlawreview.com

How Will the "New" New California Privacy Law Affect Your Business?

Article By:

Theodore F. Claypoole

We had started getting (sort of) comfortable with the CCPA—California's omnibus privacy legislation—when the state decided to change the law again. The CCPA just began to be enforced in July of 2020 when a mere 4 months later the state passes Proposition 24, a stricter, more all-encompassing privacy law aimed at protecting the same consumers (and a few more) from most of the same activities of the most of the same businesses.

The new law, known as the California Privacy Rights Act ("CPRA") becomes fully effective January 1, 2023, with "right to know" requests applicable from January 1, 2022, so your company has time to prepare, but prepare it must. The CPRA starts with the obligations imposed on your business by CCPA and adds to them, so you will need to be more restrictive in treatment of the consumer data you collect and provide more options to California consumers.

This article does not address all of the changes to current law made by the CPRA. Instead, this article addresses some of the provisions that will add operational costs to companies and force regulated businesses to change the way they are currently operating under CCPA.

For example, enforcement and audit of the new rights will add administrative cost and work responsibilities to business. The CPRA famously expands enforcement powers, creates and funds a new regulatory bureaucracy with audit rights over business, increases fines, and eliminates rights for companies to cure mistakes. Also, certain companies with significant consumer data must perform independent annual cybersecurity audits and regularly submit to the state risk assessments concerning the processing of information, "including whether the processing involves sensitive personal information, and 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 such processing, with the goal of restricting or prohibiting such 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." So such businesses will be responsible for undertaking assessments on a complicated balancing formula that California will further define in the future.

One of the most significant changes is the core definition of California consumer, which right now is broad, but relates to people one might casually think of as "consumers" – you know, people who

consume your company's products and services. Starting in 2023, "consumers" will also be applied to your California employees and people who are involved in your company's trade and business contacts. Prior to enforcement, there may be additional legislative rules passed to clarify how businesses will apply a law meant for addressing customer information to the different types and uses of information collected for employees, but we don't know this for certain.

The heart of the CPRA is the set of limitations for businesses on collection of data, some of which relate to earlier restrictions, but taken together will create an entirely new paradigm for businesses trying to be compliant. The CPRA limits collection of a consumer's data to the minimum amount of information necessary, which must only be used for the stated purpose the information was given to a business, and stored for only as long as the business has stated publically it would retain the data. In other words, no collecting data from customers and then deciding how to use it productively in the future. If the CCPA was primarily about restricting sales and transfers of consumer data, then the CPRA can be seen as primarily about restricting how and why data is collected and used. So this will force limitations on how companies collect, keep and use their own data about their own transactions, as long as those transactions also involve California consumers.

To that end, the CPRA gives consumers rights to object about analytics being used on their data. The law allows consumers to stop "automated decision-making" and to force a business to provide "meaningful information" about the logic involved in any such automated decision-making algorithms. In addition, consumers can opt out of cross-context behavioral advertising, which may affect how many businesses use Google Analytics or similar programs tracking customers and prospects online. Further, the CPRA restricts precision geolocation programs, not allowing companies to track people within a radius of 1850 feet. This intentionally makes geo-fencing and location-based apps difficult to use, as companies can't choose to send information to people standing right outside the storefront.

Under CPRA, a company that passes consumer data on to someone else will be held responsible to inform the recipient company to delete the information if the consumer requests it. Right now the collecting company is simply responsible for deleting the data that it is holding when requested to do so by the person described by the data, but it will soon be the legally liable to notify others of deletion requests, and the company holding transferred data will be responsible for deleting it upon request of its source. No indication of the verification required for such intracompany requests.

The new California law is also one of the first U.S. regulations to address the collection and use of a category of data it calls "sensitive personal information." Under this provision, a consumer can force businesses to stop using data about the consumer that describes race, religion, sexual orientation, genetics, biometrics, precise geolocation, union membership or the contents of the consumer's communications (unless the business is the intended recipient of the communication). The biometrics portion of this requirement, especially as applied to the new category of "consumer" that are actually employees, could n affect physical security systems in California workplaces, as employees opt out of needing to prove their identities to perform sensitive jobs or to access restricted spaces. The CPRA allows for limited use of biometric security, but the company using it would need to justify that use of the system is reasonably necessary and proportionate for these purposes.

While changes to the California law include additional provisions that will affect business, these are the provisions I believe will have the largest operational effects on companies trying to comply. This blog will cover some of these provisions in more detail in coming months, but all companies with customers or employees in California need to be examining their current data practices in light of the new restrictions and obligations. When California decides to grant new rights to its residents, someone always needs to pay for those rights, and this time it will be the companies who serve

them.

National Law Review, Volume XI, Number 61