Professional Perspective

Steps for Proactive CPRA Compliance

Erin Illman, Junaid Odubeko, and Steve Snyder,
Bradley Arant Boult Cummings

Bloomberg Law

Steps for Proactive CPRA Compliance

Contributed by Erin Illman, Junaid Odubeko, and Steve Snyder, Bradley Arant Boult Cummings

California voters signaled that privacy is a top priority by overwhelmingly approving Proposition 24 on Nov. 3, 2020—the California Privacy Rights Act (CPRA). The CPRA amends and significantly strengthens the recently enacted California Consumer Privacy Act and moves California's privacy laws toward those of the EU General Data Protection Regulation (GDPR).

CPRA aims to place consumers "on a more equal footing when negotiating with businesses in order to protect their rights" by adding unprecedented consumer rights to those already afforded under CCPA. CPRA also specifically targets business practices that involve internet advertising, collection and use of sensitive personal information or children's data, and automated decision- making technologies.

The CPRA becomes operative on Jan. 1, 2023, however, like CCPA, it has a "look-back" provision that applies to information collected on or after Jan. 1, 2022. That means that although enforcement cannot begin before Jan. 1, 2023, companies should be substantially in compliance with the law by Jan. 1, 2022—a little more than one year away. While that may seem a long way out, many companies who have effectuated GDPR or CCPA programs will attest that one or even two years to implement these laws is often insufficient.

With the clock ticking, our team has put together six things that companies can start doing now to get a head start on ensuring CPRA compliance.

Assess if Your Business Meets New Thresholds

There is good news for some businesses. CPRA doubles the CCPA's threshold number of consumers or households, while deleting the reference to devices, from 50,000 to 100,000, resulting in reduced applicability to small and midsize businesses. Importantly, the new threshold requirement also deletes the reference to "receives for the business's commercial purposes" and only applies to personal information bought, sold, or shared.

This means that even if your business receives personal information of California residents, if your business does not buy, sell, or share personal information of 100,000 consumers or households—and assuming the other two thresholds do not apply—then businesses who may have previously met the threshold for CCPA may now be exempt from CPRA.

The definition of "business" has also been clarified to exclude commonly branded and controlled businesses that do not share California consumer's personal information with each other. As a result, if a "business" does not share California consumer's personal information with other commonly branded and controlled entities, then those entities are not defined as within the scope of "business" for the purpose of the statute. This could be a significant development for businesses that met the CCPA thresholds based only their association with other entities within a corporate structure.

Determine if Your Business Collects Sensitive Personal Information

The CPRA introduces "sensitive personal information" as a new regulated dataset in California. The category is subject to new disclosure and purpose limitation requirements, and consumers will have new rights designed to limit businesses' use of their sensitive PI. This includes providing a new link on the business's webpage, "Limit the Use of My Sensitive Personal Information," that would enable the consumer to limit the use or disclosure of that information to a limited subset of purposes described under the statute.

"Sensitive personal information" is defined to include personal information, as that term is defined under California's data breach statute, such as 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.

Additionally, "sensitive personal information" includes a consumer's precise geolocation, a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; 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. The protections afforded "sensitive personal information" also extend to the processing of biometric information for the purpose of uniquely

identifying a consumer; personal information collected and analyzed concerning a consumer's health; or personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Companies that collect any of this sensitive personal information should start to inventory the types collected, how that information is used, who that information is shared with—and whether that sharing is legally allowed under the statute without consumer consent—to formulate a comprehensive strategy on how the business will collect, use, share, retain, and protect sensitive personal information in compliance with CPRA.

Amend Service Provider Agreements and Update Templates

The CPRA requires that agreements between businesses and service providers, contractors or third-party providers must specify that the personal information is sold or disclosed by the business only for limited and specific purposes. The CPRA grants businesses the right to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business's obligations under CPRA.

The CPRA also grants businesses the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. In addition, the CPRA obligates the third party, service provider, or contractor to comply with applicable CPRA obligations and provide the same level of privacy protection as required by the CPRA.

Accordingly, even if organizations updated their vendor agreements to ensure their vendors were service providers pursuant to CCPA they will likely have to update them all again to include the following specific provisions, beyond the prior CCPA requirement that the service provider cannot retain, use or disclose the personal information other than for the specific purpose of the contract, that must appear in the contract:

- Service provider cannot sell or share the personal information
- Service provider cannot maintain, use, or disclose information "outside of a direct business relationship" with the business
- Service provider cannot combine the data with personal information received on behalf or another entity, with some exceptions

Further, if the service provider wants to use a subprocessor to process personal information on behalf of the business it must notify the business of that engagement, which must bind the subprocessor to the same restrictions as outlined above.

Update Your Data Retention Policy

The CPRA will require a business to inform consumers of the length of time the business intends to retain each category of personal information and sensitive personal information or the criteria used to determine that period. The CPRA would prohibit businesses from retaining such information for longer than reasonably necessary for the disclosed purpose of collection.

These requirements will move a data retention policy from a "should have" best practice to a "must have" policy subject to enforcement. Given the lack explicit statutory requirements around data retention and the historical tendencies of businesses to keep as much data as possible even without a purpose, this measure may require privacy professionals to educate their internal stakeholders as to the concept of a strict purpose limitation tied to retention. Once CRPA is enforceable, businesses will have a new risk of non-compliance when keeping data too long. Importantly the data cannot be kept for just any "business purpose," only those purposes disclosed when the data was collected.

Analyze How New Privacy Rights Will Affect Your Business

The CPRA would grant consumers an expansive set of new rights beyond those contained in the CCPA. Included in these new rights are the following:

Right to Correction. The provisions of the CPRA allow consumers to request any correction of their personal information held by a business if that information is inaccurate.

Right to Opt Out of Automated Decision-Making Technology. The CPRA authorizes regulations allowing consumers to opt out of the use of automated decision-making technology, including "profiling," in connection with decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Right to Access Information About Automated Decision-Making. The CPRA authorizes regulations allowing consumers to make access requests seeking meaningful information about the logic involved in the decision-making processes and a description of the likely outcome based on that process.

Right to Restrict Sensitive PI. Under the CPRA, consumers may limit the use and disclosure of sensitive personal information for certain "secondary" purposes, including prohibiting businesses from disclosing sensitive personal information to third parties.

Determine if Your Business is a 'High-Risk Data Processor'

The CPRA provides for the issuance of regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security. The law will require these businesses 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. In performing these audits, the factors businesses should consider in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

The CPRA also requires businesses to submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal 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.

In addition to the six steps listed above, companies should also assess their risk and understand how CPRA will be enforced. The CPRA creates the California Privacy Protection Agency, a five-member board charged with investigating possible violations under the law and enforcing the provisions of the law. The new agency will begin enforcing the law on July 1, 2023.

Until then, the CCPA will "remain in full force and effect and shall be enforceable until the same provisions of [the CPRA] become operative and enforceable." The new agency, the California Privacy Protection Agency, will assume rulemaking responsibilities from the California Attorney General.

The requirements of the CPRA are extensive, and, although the implementation date may be over two years away, it will be important for companies to begin reviewing their existing privacy compliance programs to incorporate new obligations to ensure compliance with the new law. The CPRA can only be amended if the amendment furthers the intent and purpose of the law. Consequently, barring federal legislation, this new privacy regime is here to stay.