PUBLICATION

How California's New(er) Privacy Legislation Will Affect U.S. Businesses

Authors: Matthew George White, Alexander Frank Koskey, III
November 09, 2020

While most of us have been understandably focused on the presidential election, the State of California has passed significant new privacy legislation that may have a substantive impact on your business. Specifically, Californians voted to pass Proposition 24, the California Privacy Rights Act of 2020 (CPRA). The CPRA will replace the California Consumer Privacy Act (CCPA) beginning January 1, 2023. While many may be quick to label this as "CCPA 2.0," the CPRA has a much broader set of rights and obligations than the CCPA, which may create new compliance hurdles for covered businesses. This alert will summarize several of the provisions of the CPRA that all covered businesses need to consider.

Timing

The CPRA takes effect on January 1, 2023. However, it will have a "look back" period to January 2022, meaning that personal information collected by businesses starting January 1, 2022 will be subject to the CPRA's requirements. Until that time, the CCPA remains in force. We have previously provided guidance on key considerations for complying with the CCPA, and now that enforcement of the CCPA has begun, companies must ensure they remain compliant.

Key Provisions

The CPRA appears to be moving California's privacy regulations even closer to the requirements of the European Union's General Data Privacy Regulation (GDPR). The CCPA was already the most significant privacy legislation in the United States, and with the passage of the CPRA, the requirements companies will face are now further heightened. Some of the CPRA's key provisions include:

- Creating the California Privacy Protection Agency (CPPA), the first privacy-specific regulator in the United States. The CPPA will be in charge of enforcing the CPRA and, once created, will assume enforcement of the CCPA from the California Attorney General's Office. In addition to its enforcement abilities, the CPPA will be charged with conducting rulemaking to clarify a number of key areas of the CPRA's requirements.

- Revising the definition of a "Covered Business." The CPRA modifies the definition of covered businesses to include all businesses that share personal data, without regard to whether they receive monetary compensation.

- Classifying "Sensitive Personal Information." The CPRA establishes this specialized category of personal information and grants consumers additional rights with respect to the use of this information. Sensitive Personal Information is defined to include: Social Security numbers, driver's license numbers, passport numbers, financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information about sex life or sexual orientation.

- Expanding liability for data breaches. The CPRA expands the private right of action under the CCPA to include data breaches that result in the compromise of an email address and password or other

information that would permit access to the consumer's account.

- Increasing protections for minor's data. The CPRA triples fines for violations of the CCPA's opt-in rights relating to the sale of data for consumers under the age of 16.

- The CPRA expands upon the CCPA's "Right to Opt-Out" to include both the sharing and sale of personal information. If your business determined that it did not need to provide an opt-out to California consumers under the CCPA, your processes will likely need to be evaluated again for the CPRA.

In addition to these provisions, the CPRA contains additional requirements with respect to the sharing of information, adds additional consumer rights (such as the creation of a new right of correction and expansion of the right to deletion), limits the CCPA's 30-day opportunity to cure provisions, expands the CCPA's anti-retaliation provisions, and includes new personal data retention requirements. Notably, the CPRA also extends the current CCPA exemption for personnel/applicant data until January 1, 2023.

Takeaway

With the CPRA, California has taken the nation's toughest privacy law – the CCPA – and expanded it to make it more comparable to Europe's GDPR. Companies need to review their current CCPA compliance plans and prepare to revamp those plans to address the numerous additional requirements imposed by the CPRA. This will involve, among other things, revision of privacy notices, retention schedules, privacy practices and disclosures. The consequences for failing to do so are only heightened by the creation of the CPPA, whose charge will be to focus on protecting the privacy of California consumers by enforcing the CPRA.

If you have any questions regarding the CPRA, any of California's other privacy regulations, or any other aspect of your data protection and privacy practices, please contact the authors Matt White, CIPP/US, CIPP/E, CIPM or Alex Koskey, CIPP/US, CIPP/E, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.