NOW + NEXT

DATA PRIVACY & CYBERSECURITY ALERT | NIXON PEABODY LLP

SEPTEMBER 2, 2020

The California Privacy Rights Act — Is this really happening?

What to expect if the CPRA ballot initiative becomes law

By Jason Gonzalez

In 2018, there was a dramatic change in California privacy law: the passage of the California Consumer Privacy Act (CCPA). The law, which took effect on January 1, 2020, brought about a wholesale change to many businesses' privacy practices, including dramatically increased notice, disclosure, and consent obligations relating to how businesses handled personal data. Complicating matters further was the fact that the regulations interpreting the CCPA were not finalized until August 14, 2020, nearly eight months after the statute's effective date. Many businesses, therefore, understandably struggled when implementing the statute's novel provisions, as the legal landscape seemed to be shifting under their feet.

But now that the CCPA's regulations are final, all that uncertainty is over. Right? Unfortunately, maybe not.

This coming November 2020, voters will be asked to decide whether the "California Privacy Rights Act (CPRA)" ballot initiative should become law. This ballot initiative effectively would amend the CCPA to impose additional privacy-related requirements on California businesses, and also make other substantive changes to the CCPA. While difficult to predict, it appears at this point that the initiative has a good chance of passing.

If the CPRA passes, what does this mean for businesses? Here are a few key points:

A compliance runway

- The CPRA would not come into effect until January 1, 2023. Actual government enforcement of the CPRA's provisions would not begin until July 1, 2023.

Additional consumer substantive rights

- The law imposes heightened protections for "sensitive personal information," which includes social security, driver's license, passport, and financial account numbers, and other highly private information. Consumers will have the right to limit businesses' ability to collect, use, and share this information.

- Consumers will have the right to request that businesses correct inaccurate information about the consumer.
- Consumers can limit a business's ability to collect and use geolocation data that has a level of precision within 1,850 feet.
- Businesses must inform consumers of their data retention policies, and are not allowed to keep data longer than is "reasonably necessary."
- Consumers have the ability to prohibit businesses from sharing data with others for the purposes of cross-context behavioral advertising.

Strengthened enforcement

- The CPRA creates a "California Privacy Protection Agency" tasked with enforcement and promulgation of regulations.
- The CCPA's 30-day "cure" period is eliminated for government enforcement actions, replaced with a provision allowing the government the discretion to abstain from enforcement actions depending on the circumstances.
- The penalties for mishandling children's information are tripled from $2,500 per incident to $7,500, dramatically increasing the consequences of violating the statute.
- The scope of potential data breach claims is increased by the CPRA's clarification that leaks of email accounts combined with a password or security question information can support a cause of action for statutory damages.

Audits and risk assessments

- While the CPRA itself does not impose a requirement that a business conduct data privacy audits and risk assessments, it does task the attorney general with issuing regulations that create such a requirement for businesses whose processing "presents a significant risk to consumers' privacy or security."

What hasn't changed? As an amendment to the CCPA, the CPRA initiative leaves many of the current statutory provisions untouched. Generally speaking, the overall statutory scheme requiring that consumers are accurately notified of their rights pursuant to a privacy policy; that data collection, sharing, and usage is generally limited to that which is disclosed to the consumer; differing obligations for "businesses" and "service providers" (although the CPRA imposes some additional contractual requirements); and that businesses promptly respond to consumer requests, all remains essentially same. The CPRA similarly continues the CCPA's exemptions for certain types of data, including employment-related data, up until January 2023.

The good news here is that businesses' efforts to date to comply with the CCPA will serve them well in the future, should the CPRA become law. The same compliance infrastructure to track data flows, refine privacy practices and policies, establish business-to-business (B2B) security and privacy obligations through contracts, and promptly respond to consumer requests that work for the CCPA can be made to work with the CPRA. And overall, once all the dust settles, businesses' knowledge and handling of their customers' private data likely will be more nimble and sophisticated than it was before. Despite the short-term burdens this may entail, the long-term benefits may be worth it.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Jason Gonzalez, 213-629-6019, jgonzalez@nixonpeabody.com
- Jenny Holmes, 585-263-1494, jholmes@nixonpeabody.com
- Troy Lieberman, 617-345-1281, tlieberman@nixonpeabody.com