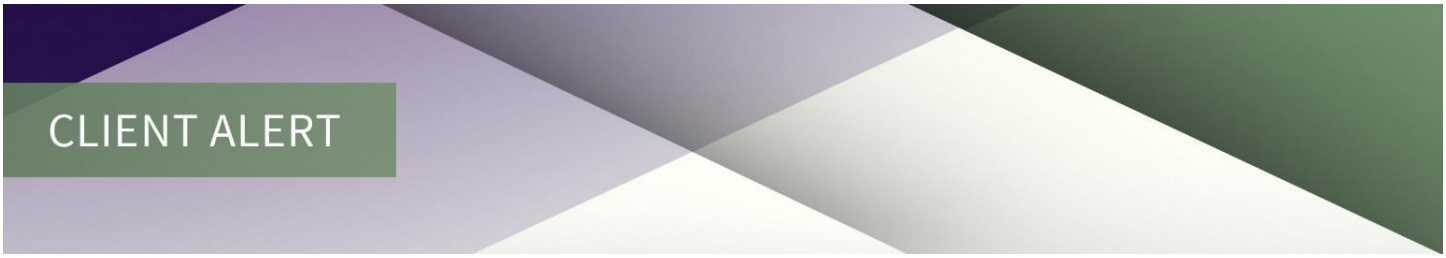

CPRA Passes: What's Next for Privacy Compliance?

November 11, 2020

AUTHORS

Daniel K. Alvarez | Simona Agnolucci | Benedict Y. Hur | Nicholas Chanin

Last Tuesday, voters in California approved the California Privacy Rights and Enforcement Act of 2020 ("CPRA").[1] The CPRA was drafted and brought to the ballot by the advocacy group behind the original California Consumer Privacy Act ("CCPA") with the goal of "strengthening" the CCPA by addressing a number of perceived weaknesses and shortcomings. In this Client Alert, we highlight some of the major changes the CPRA makes to the CCPA, and identify some key questions for companies as they begin their compliance efforts.

Major Changes Introduced By The CPRA

After 18 months of working to come into compliance with CCPA, and just a few weeks after the California Attorney General issued revised draft CCPA rules, companies are faced with a number of significant changes to the CCPA enacted in the CPRA. These include: (1) restrictions and obligations on "sharing" personal information; (2) new limitations and obligations for service providers; (3) provisions related to "sensitive personal information"; (4) a new consumer right to "correct," and clarification to existing rights; and (5) a new privacy agency charged with implementation and enforcement of the statute.

- *New Restrictions and Obligations Related to "Sharing" Personal Information.* One of the most notable changes the CPRA introduces is a new category of regulated transfers of personal information — sharing — focused on disclosures made for "cross-context behavioral advertising" (another new term) regardless of any exchange of

[1] California Privacy Rights and Enforcement Act, *available* here.

money or other valuable consideration. Under the CPRA, "sharing" personal information is treated similarly to "selling" under the CCPA, with many of the same attendant obligations.

- *New Limitations and Obligations for Service Providers.* The CPRA imposes new limitations, requirements, and obligations on service providers in an effort to more clearly define the line between transfers of personal information to service providers and "selling" or "sharing" information. These include (i) a prohibition on combining the personal information received from/on behalf of the business with personal information received from/on behalf of another business; (ii) a new obligation that service providers assist businesses with consumer data requests; and (iii) a requirement that, where service providers engage any other person to assist in processing personal information, those service providers notify the business of such an engagement and conduct such engagement pursuant to a contract with the same limitations/requirements as the business-service provider engagement.

- *"Sensitive Personal Information."* The CPRA introduces to the CCPA the concept of "sensitive personal information" and imposes more stringent obligations and requirements on its collection, use, sale, and sharing than those imposed on non-sensitive personal information. "Sensitive personal information" includes categories of information familiar from both state data breach laws in the United States (e.g., social security number, driver's license number, etc.) and from the General Data Protection Regulation in the European Union (e.g., the consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership, or information about the consumer's sex life or sexual orientation). In their privacy policies, notice at collection, and other public-facing documents, businesses must identify which categories of sensitive personal information are collected, used, and disclosed, and must explicitly identify those categories as "sensitive." Businesses also must provide a button consumers can click to "limit use/disclosure of sensitive information," similar to the "do not sell my information" button. Consumers have a right to limit the use and disclosure of their sensitive personal information.

- *Consumer Data Rights.* The CPRA adds a new consumer right to the coterie already established by the CCPA, and clarifies businesses' obligations under existing consumer rights. In particular, the CPRA introduces a new "right to correct" under which businesses must use "commercially reasonable" efforts to fulfill verifiable requests to correct consumer data. Likewise, the right to access now requires businesses to provide a more granular breakdown of the personal information they use, collect, share, or sell (including categories of sensitive personal information collected).

- *A New Agency for Implementation and Enforcement.* The CPRA also creates an entirely new agency, the California Privacy Protection Agency (the "Agency"), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA/CPRA. The operating costs of the Agency and any other related costs incurred by the state will be offset by the proceeds of any fines collected by the Agency and deposited into a "Consumer Privacy Fund." The Agency will be governed by a five-member board appointed by the Governor (two

members, including the Chair), the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly (one member each).

Next Steps

The amendments enacted in the CPRA come into effect on January 1, 2023, so businesses will have more than two years to identify and execute any changes that need to be made to their data collection, use, security, or sharing activities. During that time, we expect that companies will need to focus on five key areas:

- *Monitoring for New Regulations and Guidance.* The CPRA tasks the Attorney General ("AG") with promulgating a series of initial regulations and undertaking initial enforcement actions, but this role ultimately will be transitioned to the Agency. For example, the CPRA directs the AG to conduct a rulemaking proceeding to determine the scope of "business purpose," particularly with respect to those purposes for which a service provider can process personal information. These rulemakings will be important inputs to any compliance efforts.

- *Reassess Data Sharing Arrangements.* The introduction of a new category of data disclosure arrangements – "sharing" – means that companies likely will need to reassess their data sharing/data collection arrangements to identify any that may qualify as "sharing."

- *Service Provider Contracts.* The CPRA imposes new requirements for contractual language/provisions that need to be included in any service provider contracts. Companies likely will need to review their current template agreements and existing contracts to determine the extent to which changes need to be made to ensure compliance with the CPRA's new requirements.

- *Security Policies and Procedures.* The CPRA imposes an affirmative obligation on companies to establish and maintain reasonable and appropriate security policies and procedures. Companies will need to consider steps – including potentially working with third parties to conduct vulnerability and risk assessments – to ensure their existing policies and practices are sufficiently robust.

- *Employee/B2B Information.* After legislation earlier this fall extended the CCPA's carve-outs for personal information collection in the employee and business-to-business (B2B) context to January 1, 2022, the CPRA extends the carve-out further – to January 1, 2023. While that is a helpful extension, it likely means companies will include this data and all the activities they undertake with that data as part of the compliance efforts that they will undertake for CPRA purposes.

Conclusion

As it did with the CCPA, California has once again pushed to the front of the American privacy conversation with the passage of the CPRA. Companies that feel as if they have just finished establishing their CCPA compliance programs may see the two-year ramp-up period as a good reason to take a break before turning to the CPRA, but the list of potential steps they may need to take to achieve compliance could be significant, so any break may need to be a brief one.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Simona Agnolucci
415 858 7447
sagnolucci@willkie.com

Benedict Y. Hur
415 858 7401
bhur@willkie.com

Nicholas Chanin
202 303 1164
nchanin@willkie.com