CALIFORNIANS VOTE FOR ADDITIONAL DATA PRIVACY PROTECTIONS IN THE CPRA

Authors: Amy Worley, Matt Meinel, Amy Lewis

Most Americans have been laser-focused on the 2020 presidential election. However, other election results are in. In California, voters approved a referendum on consumer privacy called the *California Privacy Rights Act ("CPRA")*, which dramatically alters the privacy compliance landscape in the US and creates the country's first stand-alone privacy regulator.

Privacy advocate Alastair Mactaggart sponsored the CPRA in reaction to what he believed was the California legislature's overly business-friendly privacy law, the California Consumer Privacy Act ("CCPA"). The CCPA went into effect on January 1, 2020, with enforcement by the California attorney general (AG) beginning on July 1, 2020. Companies have been working to implement the CCPA and its dynamic and changeable regulations, but implementation has been complicated by both the impact of COVID-19 and revisions to the implementing regulations.

The CPRA will add complexity to an already complex legal situation. The nuances of how the CPRA and CCPA will work together remain to be seen and will be developed by the newly created California Privacy Protection Agency and the California AG in the coming months.

Key Dates

Most of the CPRA's substantive provisions will not go into effect until January 2023. The employee data compliance moratorium is extended until January 1, 2023 (i.e., personal information collected by a business in the employment context would not be covered until 2023).

Enforcement

Effective immediately, a new data protection agency, the California Privacy Protection Agency (the "Agency"), has been created.

- The Agency will share enforcement with the California AG.

- The Agency will take over rulemaking authority from the AG in July 2021.

- The Agency has an independent budget, which the California legislature is required to increase when necessary.

- The Agency will collect fines for violations, and those fines will fund further CPRA enforcement by the Agency, the AG, and the courts.

Businesses will no longer have thirty days to cure general violations of the law. The thirty-days-to-cure period remains only as a means of preventing statutory damages as a part of a private right of action for security violations.

Data Breach and Private Right of Action

As with the CCPA, the CPRA limits the private right of action to security breaches. However, the CPRA specifies that remedial measures following a security breach would not preclude a consumer lawsuit, which was an open question under the CCPA. Email and password combinations, commonly acquired by phishing attacks, are considered a data breach.

Consumer Rights

Consumers have additional rights with respect to their personal information, including the rights to:

- Correct inaccurate information

- Opt out of sharing in cross-context behavioral advertising

- Limit the use of sensitive personal information: government-issued identifiers, account log-in credentials, financial account information, precise geolocation, contents of certain types of messages, genetic data, racial or ethnic origin, religious beliefs, biometrics, health data, and data concerning sex life or sexual orientation

- Limit sharing of personal information between businesses in certain contexts

Digital Advertising and Profiling

The CPRA attempts to clarify the rules for "sharing" (i.e., not just "selling") personal information for behavioral advertising and digital profiling. These provisions are complex and will likely be the subject of significant rulemaking. It remains to be seen how they will be read in tandem with the CCPA rule allowing consumers to opt-out of "sales" of their personal information.

Business Obligations

A business's collection, use, retention, and sharing of a consumer's personal information must be reasonably necessary and proportionate to achieve the purposes for which it was collected and should not be further processed in any manner inconsistent with that purpose. A business must disclose, at the collection point, the intended retention period and the categories of personal information collected; and must delete the data when the retention period expires.

Businesses that process large amounts of personal information will be required to conduct risk assessments, similar to a provision in the European General Data Protection Regulation ("GDPR") that requires Data Protection Impact Assessments before high-risk personal data can be processed.

Contracting Obligations

The CPRA places new contractual obligations on service providers, contractors, and third parties. This change is similar to GDPR obligations, which should allow businesses to streamline their privacy compliance efforts and create templates that align with both the CPRA and the GDPR. In addition to the defined terms "Third Party" and "Service Provider," which already exist under the CCPA, the CPRA adds a definition for "Contractors."

Contracts must meet three specific requirements: (1) specify restrictions on onward transfers and allowable uses of the data; (2) allow for compliance monitoring; and (3) extend CPRA obligations to third parties.

Privacy by Design

The CPRA also requires something privacy professionals call "Privacy by Design" (PbD). PbD is a process by which companies assess the impact on consumers of activities that involve the collection, use, and sharing of significant amounts of their personal information. If PbD assessments identify any outsized risks to consumers, companies must implement and document controls to remediate those risks.

For PbD, the hard part is not performing the assessments and documenting the controls; it is instead providing the tools to enable employees to identify processes that require analysis and to instill a culture that respects consumer privacy in a way that is still somewhat nonintuitive in the United States.

How Much Effort Will Compliance Require?

Covered businesses that have robust GDPR programs will have much less work to do to comply with the CPRA than businesses that do not. Most of that work will be focused on operationalizing consumer opt-out choices around behavioral advertising, sharing, and profiling.

Covered businesses that do not have GDPR programs will have much more work to do to get ready for the CPRA. Businesses that have not already done so will need to map their business processes that involve personal data and analyze the proportionality of the data collection, document opt-out/opt-in consents for those processes where necessary, enter into data use and sharing agreements, and operationalize retention periods. Those retention periods will need to be enforced, requiring companies to do something many are loath to do: delete large amounts of data.

A Sign of Things to Come

The CPRA will add complexity to an already complex legal situation. The success of the CPRA ballot measure, combined with a growing number of states that are proposing new privacy legislation, will increase pressure on Congress to pass a federal law to streamline the country's approach to privacy. Whether Congress will be able to form a sufficient consensus to do so remains uncertain.

About BRG

Berkeley Research Group (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and strategy and operations. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next.

Visit thinkbrg.com/contact.html to learn more.

BRG

THINKBRG.COM