BLANKROME

Cybersecurity & Data Privacy

NOVEMBER 10, 2020 • NO. 16

California Voters Scrap CCPA For Even More Stringent California Privacy Rights Act

In 2018, California lawmakers passed what was—until just recently—the most groundbreaking piece of privacy legislation in the United States—the California Consumer Privacy Act of 2018 ("CCPA"). Although the CCPA has only been in effect since the start of 2020, California again revised the state's game-changing privacy law even further after Golden State residents voted in favor of adopting the California Privacy Rights Act of 2020 ("CPRA")—commonly referred to as "CCPA 2.0." The CPRA significantly expands California consumers' privacy rights beyond those contained in the CCPA, and fundamentally alters businesses' privacy compliance obligations under California's current privacy law in a number of ways.

KEY ASPECTS OF THE CPRA

The following are some of the most significant aspects of the CPRA:

- **New Category of "Sensitive Personal Information":** The CPRA creates a new category of "sensitive personal information" that includes government-issued identifiers; account credentials; financial information; geolocation; race or ethnic origin; religious beliefs; contents of mail, e-mails, or text messages; and biometric information, among others. Under the CPRA, entities must comply with stricter obligations regarding the processing of sensitive data and allow consumers to limit the use and disclosure of their sensitive data.

- **Expansion of Right to Opt-Out:** The CPRA gives consumers the right to opt-out and stop companies from not only selling, but also "sharing," their personal data, with sharing being defined as the transfer of personal information for cross-context behavioral advertising.

- **Creation of New Privacy Regulatory Agency:** The CPRA establishes the California Privacy Protection Agency ("CPPA"), which is afforded complete administrative power and the authority to implement and enforce the CPRA, taking the place of the state attorney general's office in enforcing the law.

- **Proportionality Requirement:** The CPRA requires businesses' data processing activities to be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible within the context in which the personal information was collected, and prohibits companies from further processing data in a manner that is incompatible with those purposes.

- **Data Retention Limitations:** The CPRA prohibits businesses from retaining personal information for longer than is necessary to achieve the purposes disclosed in the entity's privacy notice.

- **Broadened Data Breach Liability:** The CPRA broadens the scope of the CCPA's private right of action for breaches involving non-redacted, non-encrypted personal information to also include the unauthorized disclosure or access of e-mail addresses and passwords/security questions that would allow third parties to access consumers' accounts.

- **Profiling:** The CPRA adopts the concept of profiling and requires businesses' responses to consumer access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process as it relates to the consumer.

- **Service Providers:** The CPRA broadens service provider obligations, including additional requirements mandating explicit contractual terms in service provider agreements and an explicit prohibition on combining personal information obtained as a service provider with personal information obtained from other sources.

- **Annual Security Obligations:** The CPRA requires businesses whose processing of personal information presents a significant risk to consumers to conduct annual cybersecurity audits and submit risk assessments to the CPPA.

- **Extension of Business-to-Business and Employee Data Exemptions**: The CCPA's business-to-business and employee data exemptions, which are set to expire on January 1, 2021, are extended until January 1, 2023.

TAKEAWAYS & COMPLIANCE TIPS

The CPRA will incorporate the CCPA and the law's new substantive obligations will take effect on January 1, 2023, with new regulations expected to be introduced by July 1, 2022. With the exception of consumer access requests, the CPRA will apply only to personal information collected on or after January 1, 2022.

Until January 1, 2023, covered businesses are required to remain compliant with the CCPA and any corresponding regulations. Further, at this time the California attorney general's office continues to seek additional modifications to the current CCPA regulations, including a number of modifications to the law's "final" regulations that were proposed in October. Thus, businesses should closely monitor regulatory developments and tweak their privacy compliance programs to address any new wrinkles that may arise with respect to the CCPA.

While no immediate action steps have to be taken at this time, companies that fall under the scope of the CCPA are well-advised to review the text of the CPRA to gain a better understanding of the law.

At the same time, businesses should also begin evaluating their CPRA obligations to ascertain how CCPA 2.0 will impact their data processing activities and the scope of enhancements that may need to be made to their privacy compliance programs, as the CPRA offers enhanced consumer rights and a myriad of modifications to businesses' existing privacy obligations under the current CCPA.

Blank Rome will continue to closely monitor the progress of both the CCPA and the CPRA and will provide regular updates on any developments that may impact clients' privacy compliance obligations. For additional information on the CPRA, assistance in enhancing and updating privacy compliance programs, or to discuss other cybersecurity or privacy issues in more detail, please contact any of the following Blank Rome Cybersecurity & Data Privacy attorneys:

Ana Tagvoryan, Los Angeles Office
Partner and Co-Chair, Class Action Litigation
424.239.3465 | atagvoryan@blankrome.com

Jennifer J. Daniels, New York Office
Partner and Chair, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy
513.362.8711 | doberly@blankrome.com

For more information on Blank Rome's cybersecurity and data privacy capabilities, please see our Cybersecurity & Data Privacy and Privacy Class Action Defense homepages.