CARLTON FIELDS

Final CCPA Regulations Submitted, but Compliance Burden Could Increase

June 18, 2020

The California Consumer Privacy Act (CCPA) took effect on January 1, 2020, and brought with it a panoply of new legal obligations for many companies doing business with California residents. Enforcement for violations going back to January 1, 2020, the look-back period, is slated to begin July 1, 2020, but the California attorney general's office has only recently, on June 1, 2020, submitted final proposed regulations to California's Office of Administrative Law (OAL). The OAL typically has 30 working days to review submissions, but a COVID-19-related executive order gives the OAL an additional 60 calendar days for their review. Even with this order, the attorney general has requested an expedited review, within 30 days. Once approved, the regulations will be filed with the secretary of state and become enforceable. Practically speaking, enforcement actions will likely begin in September 2020, although as noted above, those actions can reach back to January 1. The good news for companies is that the final regulations have not been altered since the attorney general requested comment on them back in March 2020. The curveball is that a pending ballot initiative, the California Privacy Rights Act of 2020 (CPRA), often referred to as "CCPA 2.0," may add even more compliance obligations for companies already struggling to meet their CCPA obligations. If it passes, the CPRA would become operative on January 1, 2023, and make a number of significant changes to the CCPA's current requirements. First, the CPRA would create a new category of data, "sensitive personal information," with additional consumer rights, including a new consumer right to correct personal information, and consumer rights regarding a business's activities involving automated decision-making. The CPRA would also require data minimization and notice regarding the length of time for which personal information is kept. In addition, the CPRA would expand liability for data breaches involving email addresses and passwords or a security question. Some companies, such as those performing high-risk processing, would be required to undergo annual cybersecurity audits and submit regular risk assessments. The CPRA would create an entirely new enforcement agency, the California Privacy Protection Agency, the purpose of which would be the protection of

California consumer privacy rights. The agency would have subpoena and audit powers, and the ability to levy fines of up to $2,500 per violation of the CPRA or up to $7,500 per intentional violations or violations involving minors. The California State Assembly held a hearing to discuss the CPRA on June 12, 2020, and officials are now verifying the initiative's signatures. Roughly 900,000 signatures were reportedly submitted, well in excess of the requisite number of signatures necessary for ballot inclusion. Californians for Consumer Privacy has filed a court order seeking signature verification be concluded by June 25, 2020, the deadline for ballot inclusion. Companies that have delayed their CCPA compliance efforts should use the summer to immediately address any shortcomings before investigations and enforcement actions begin this fall, with an eye on the CPRA's progress. Those action items should include:

- Review and update your privacy policy and CCPA disclosures.
- Review and update your subject access request workflows.
- Evaluate your vendor and other contracts to ensure compliance with the CCPA.

Authored By

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology

accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.