Articles + Publications | July 21, 2023

CPRA Shuffle: Two Steps Forward, One Step Back: Court Temporarily Halts CPRA Regulation Enforcement as CPRA Enforcements Begins

WRITTEN BY

Sadia Mirza | Ronald I. Raether Jr. | Kim Phan | James Koenig | Joel M. Lutz | Laura Hamady | Robyn W. Lin

CPRA Regulations Delayed. On June 29, 2023, two days before enforcement of the California Consumer Privacy Act (CCPA) was to begin, a Sacramento Superior Court issued a temporary injunction, enjoining enforcement of newly promulgated regulations under the California Privacy Rights Act (CPRA), which amended the CCPA earlier this year. The new regulations were promulgated and purportedly went into effect on March 29, 2023. Specifically, the court enjoined enforcement of these final CPRA regulations, which will be stayed for a period of 12 months from the date that individual regulation becomes final. The court declined to mandate any specific date to finalize the remaining regulations.

CPRA Regulations Addressing 12 of 15 Areas Effective March 29, 2024; Final Three Areas Not Effective for Over a Year. While the CPRA stated that "the timeline for adopting final regulations required by the [CPRA] shall be July 1, 2022," the agency did not issue final regulations until March 29, 2023 (Cal. Civ. Code § 1798.185(d)). Yet, the CPRA establishes a minimum of one year between promulgation of final regulations and regulation enforcement. Moreover, the final regulations issued on March 29, 2023 only pertained to 14 of the 22 areas outlined in the CPRA (such as updating definitions, establishing rules to govern opt-outs, and further defining and adding to business purposes)[1]. These 14 will become effective March 29, 2024. The agency is currently conducting preliminary rulemaking on the remaining three areas (*i.e.,* cybersecurity audits, risk assessments, and automated decision-making), and these final regulations will not become effective until 12 months following publication.

CPRA Enforcements Still Starting on July 1, 2023 (But Not on Regulations Requirements). In its decision, the court cited language from the CPRA that enforcement of the regulations would not begin until July 1, 2023. Therefore, the court agreed "the very inclusion of these dates indicates the voters intended there to be a gap between the passing of final regulations and enforcement of these regulations."

Immediately Beginning CPRA Good Faith Compliance. While the court's decision offers a temporary respite from any last-minute compliance efforts, companies should continue to strive for compliance with the regulations since the agency's decision to pursue an investigation into CPRA violations will be based on "all facts it determines to be relevant, including … good-faith efforts to comply with those requirements." For CPRA/CCPA compliance resources and best practices, see our two webinars on the topic, How to Navigate the Rush of New State Privacy Laws and Navigating the Critical Differences Between the CCPA and CPRA; and our five-part California Privacy Rights Act Series, published in the *California Daily Journal*.

As always, Troutman Pepper's Privacy + Cyber Practice stands ready to assist with U.S. state/federal and global privacy/security compliance, including developing policies and procedures for companies with CCPA/CPRA and other U.S. state comprehensive privacy laws.

Please contact Jim Koenig, Ron Raether, Kim Phan, Sadia Mirza, Joel Lutz, Laura Hamady, Robyn Lin, or any member of our Privacy + Cyber Practice Group with questions.

---

[1] The rulemaking touched on the following topics: (1) defining notified purposes for which a consumer can collect, use, retain, and share consumer personal information, (2) establishing rules, procedures, and any exceptions to notice requirements, (3) establishing rules and procedures to facilitate and govern submission of a consumer's request to opt-out of sale/sharing and requests to limit use and disclosure of sensitive personal information, (4) establishing rules and procedures for facilitating a consumer's right to delete, correct, or obtain personal information, (5) establishing rules on how often and under what circumstances a consumer can request a correction, (6) establishing procedures to extend the 12-month period of disclosure of information, (7) defining requirements and specifications for an opt-out preference signal, (8) establishing regulations governing how business respond to an opt-out signal, (9) establishing rules governing use or disclosure of sensitive personal information, (10) defining and adding to business purposes, (11) identifying business purposes for which service providers may use consumers' personal information pursuant to a written contract, (12) establishing procedures for filing complaints with the CPPA, (13) defining scope and process for the exercise of the CPPA's audit authority, and (14) harmonizing regulations.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber