THOMPSON HINE

Privacy & Cybersecurity Update

April 2023

California and Colorado Finalize Privacy Regulations

In just the first few months of this year we already have seen significant state law developments that raise the privacy compliance stakes, including five new state privacy statutes, and the pace of change continues to accelerate. California and Colorado both have adopted final regulations that implement their respective comprehensive consumer privacy legislation. The new regulations fill in areas left open in the statutes and, in some instances, actually add to the compliance burden. The key issues that impact evolving organizational privacy compliance obligations include:

California

The California Privacy Rights Act (CPRA), which significantly amended the California Consumer Privacy Act (CCPA), went into effect on January 1. Under the CPRA, the California Privacy Protection Agency (CPPA) is tasked with adopting regulations to implement the CPRA. On February 3, after several rounds of rulemaking activity including extensive public comments, the CPPA adopted and approved its first rulemaking package. On March 30 the CPPA announced the California Office of Administrative Law had approved the regulations, which took effect immediately upon publication. The approved CCPA regulations include:

- Restrictions on how businesses can collect, use and disclose personal information internally and externally with service providers, contractors and third parties.
- Updates to requirements for consumer disclosures and communications that provide for device formats, accessibility, disability and language requirements.
- Requirements for designing and implementing methods for how businesses receive and respond to CCPA requests and obtain consumer consent, including restrictions on the use of "dark patterns" that would impair or interfere with the consumer's ability to make a choice.
- Additional instructions for notice at collection requirements; for example, the regulations permit businesses to provide a single notice at collection that contains the required information about their collective information practices.
- Updates to notice of right to opt-out of sale or sharing to include the location of the link to be added to either the header or footer of the website.
- Limits on how service providers, contractors and third parties can use, retain and disclose personal information collected pursuant to a written contract with a business.
- Restrictions on contractual relationships for cross-context behavioral advertising to third parties and prohibitions on service providers and contractors contracting with a business to provide cross-context behavioral advertising.
- Requirements for additional privacy terms that must be included in written contracts with service providers and contractors.
- Instructions for verifying a consumer's identity with respect to data right requests as well as specific rules related to verification of consumers with password-protected accounts and those who do not have or cannot access a password-protected account.
- Additional rules for children, including methods for verifying the identity of the child's parent or guardian.
- Requirements for businesses collecting large amounts of personal information, characterized as a business that, alone or in combination, buys, receives for its

commercial purposes, sells, shares or otherwise makes available for commercial purposes the personal information of 10 million or more consumers in a calendar year.

With its first major rulemaking agenda completed, the CPPA's rulemaking activity continues. Seven days after approving the first set of regulations summarized above, on February 10, the agency issued an invitation for preliminary comments on cybersecurity audits, risk assessments and automated decision-making, issues that are not covered in the recently approved regulations.

Colorado

On March 15 the Colorado Attorney General's Office filed final rules with the Secretary of State implementing the Colorado Privacy Act (CPA) enacted in 2021. The new regulations provide guidance ahead of the CPA's July 1 effective date.

The CPA regulations include provisions specific to data protection assessments and profiling, similar to those now being considered by the CPPA. Major provisions of the CPA regulations include:

- Rules governing automated decision-making, including the duties of controllers and consumers' rights (e.g., transparency, opting out, consent and data protection assessment). The rules define profiling as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."
- Requirements for data protection impact assessments. Under the CPA, companies must conduct a data protection assessment before engaging in processing activities that may increase the risk of harm to consumers. The rules clarify the scope and requirements of such data protection assessments.
- Substantial new guidance for recognition and implementation of universal opt-out mechanisms. For example, the CPA provides technical and other specifications to controllers and platform developers to allow consumers to express their choice to opt out of processing their personal data for either targeted advertising, sale of personal data, or both. The CPA regulations provide flexibility rather than requiring consumers to opt out of data collection on a case-by-case basis. It enables them to use a universal opt-out mechanism to communicate their opt-out choice to multiple businesses using one method.
- Transparency and implementing guidelines on covered entities offering loyalty program benefits that utilize personal data. For example, under the new rules, a controller is not obligated to provide a certain loyalty program to a consumer who exercises data privacy rights (e.g., deletion, opt-out, consent to use of sensitive data) if the program requires personal data that is subject to the opt-out. Among other provisions, the controller must notify the consumer before discontinuing the consumer's membership in the program. In addition, the controller must continue to offer certain loyalty programs that do not require non-personalized data.

Conclusion

California's and Colorado's new privacy regulations provide important guidance to help companies bolster their compliance activities mandated in the 2023 calendar year. Common provisions across these two state privacy laws may ease the challenge of meeting state compliance but the differences will require adaptive approaches and guidance from counsel to ensure businesses are current on their privacy obligations.

FOR MORE INFORMATION

For more information, please contact:

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com