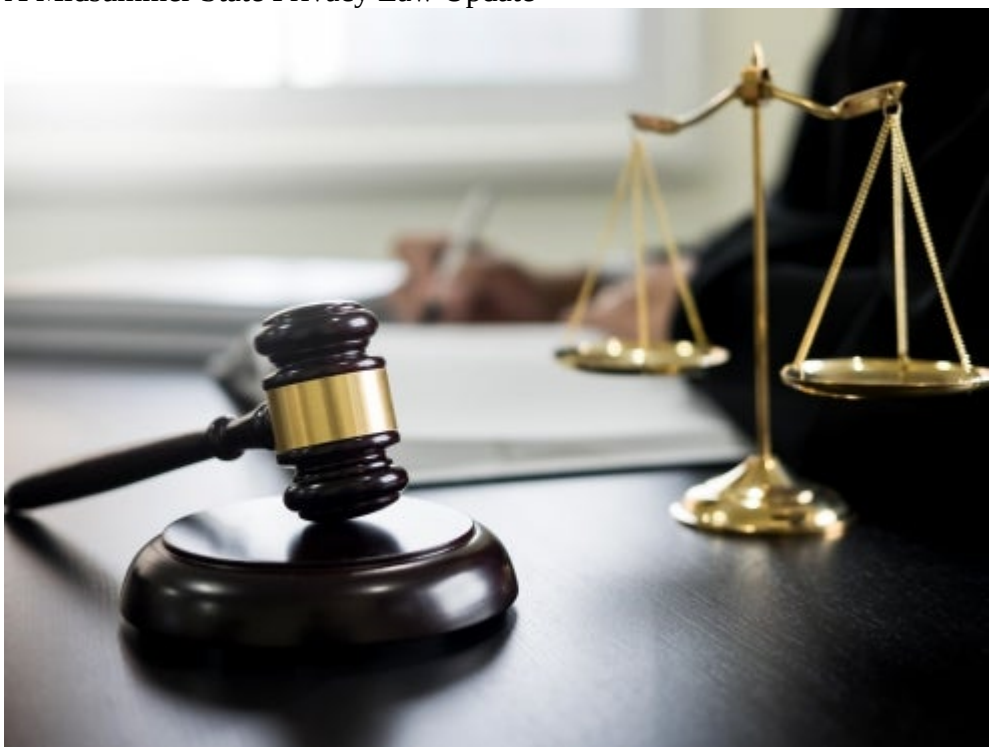
Blogs
July 09, 2024
A Midsummer State Privacy Law Update



APRA Cancellation, Rhode Island's Privacy Act, and CPPA's International Cooperation

In an active summer on the privacy front, we share a few recent updates:

Cancellation of APRA House Markup

On the morning of June 27, 2024, as congressional staffers and audience members prepared to hear the latest updates on the American Privacy Rights Act (APRA), the House Committee on Energy and Commerce announced that it was canceling its meeting to mark up and vote on the latest draft of the APRA. The next steps are unclear.

Rhode Island Data Privacy Law Diverges from the Pack

Marking the latest addition to state comprehensive consumer privacy laws, on June 28, 2024, Rhode Island Governor Daniel McKee transmitted the Data Transparency and Privacy Protection Act (the Act) (SB2500 & HB7787) to be passed without his signature. The Act enters into effect on January 1, 2026.

Whom Does the Act Apply to?

Notably, the Act applies to a broader swath of entities than most other state privacy laws. Similar to other privacy laws, the Act applies to "for-profit entities that conduct business in [Rhode Island] or for-profit entities that produce products or services that are targeted to residents of the state and that during the preceding calendar year did any of the following:

1. Controlled or processed the personal data of not less than thirty-five thousand (35,000) customers, excluding personal data controlled or processed solely for the purpose of completing a payment

transaction.
2. Controlled or processed the personal data of not less than ten thousand (10,000) customers and derived more than twenty percent (20%) of their gross revenue from the sale of personal data."

Critically, though, the Act includes a number of required privacy policy disclosures that would apply to "[a]ny commercial website or internet service provider conducting business in Rhode Island or with customers in Rhode Island or otherwise subject to Rhode Island jurisdiction"—regardless of the size of the entity or the quantity of data processing conducted by the entity.

The Act's Focus on Targeted Advertising

The Act requires any commercial website or internet service provider that conducts business in Rhode Island or with customers in Rhode Island to post a notice that identifies "all third parties to whom the controller has sold or ***may*** sell customers' personally identifiable information" (emphasis added). In addition to a new requirement in privacy disclosures to name the entities that a controller currently sells data to, Rhode Island ups the state privacy law ante by requiring controllers to identify all third parties that the controller may, at some undefined point in the future, be able to sell customers' personally identifiable information to. Interestingly, and in contrast with the rest of the Act, this provision applies to "personally identifiable information," which, unlike "personal data" and "sensitive data," is not defined anywhere in the Act. These ambiguities raise questions about how entities can comply with the Act as well as how the Act will be enforced.

The Act generally aligns with the basic provisions of other state privacy laws; however, it does not include some of the more novel provisions that have become commonplace in recent laws. For instance, the Act does not contain any requirements for entities to adhere to data minimization practices, does not provide any further protections for individuals between the ages of 13 and 17, and does not include a temporary cure period following the effective date. Additionally, unlike some recently proposed legislation, such as Vermont's privacy bill, which was ultimately vetoed by the governor, the Act does not contain a private right of action, and enforcement is left entirely to the discretion of the attorney general. Furthermore, the Act does not require the recognition of universal opt-out mechanisms.

Because of the lack of a cure provision and because of the novel privacy policy disclosure requirements, entities should take this opportunity to review their privacy practices to ensure they meet state privacy law requirements by the effective date.

CPPA Announces Cooperation with CNIL

On Tuesday, June 25, in Paris, the California Privacy Protection Agency (CPPA) signed a "declaration of cooperation" with the French Commission Nationale de l'Informatique et des Libertés (CNIL), allowing both authorities to "collaborate on their efforts to safeguard personal information and advance privacy." According to the CPPA's press update, "[t]his declaration establishes a general framework of cooperation to facilitate joint internal research and education related to new technologies and data protection issues, share best practices, and convene periodic meetings."

This is the latest entry into cross-border collaborative arrangements by the CPPA (the CPPA previously joined other international initiatives, including the Asia Pacific Privacy Authorities and the Global Privacy Assembly), indicating the CPPA's intention to coordinate with other privacy regulators around the globe. This follows on the heels of recent remarks from CPPA Board members that the CPPA wishes to obtain an adequacy decision under the General Data Protection Regulation (GDPR). These developments suggest the CPPA's desire to become a player on the global stage.

Authors

Explore more in

Privacy & Security State Consumer Privacy Laws