

Looking Down the Road: Data Privacy Priorities in 2024

February 16, 2024 – *The TMCA*

by Alexandra Holbus and Deb Howitt



Related People

- Alexandra Holbus

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

2023 brought a surge of data privacy developments, with a large expansion of state comprehensive privacy laws, litigation of new claims based on older laws (e.g. wiretapping and VPPA cases), increased scrutiny on data brokers, and more. Because 2024 is shaping up to be equally complex for those who manage data privacy in their organizations, we have compiled a summary of the US data privacy topics to watch in the coming year.

More State Privacy Laws

January was already a busy month for state privacy legislation, with new comprehensive privacy laws passed in both New Jersey and New Hampshire. The New Jersey law goes into effect January 15, 2025 and applies to businesses that control or process the

personal data of 100,000 or more New Jersey consumers or the personal data of 25,000 or more New Jersey consumers and derive revenue from the sale of the personal data. Notably, the New Jersey law's definition of sensitive information differs from existing state laws, and includes financial information, transgender or non-binary status, and a broad definition of biometric data. Sensitive information can only be processed after obtaining express consent from the consumer. New Jersey's law also does not include as many exemptions as previous laws: data processed by nonprofits, personal data subject to the Family Educational Rights and Privacy Act (FERPA), and data processed by institutions of higher education are all subject to the law.

New Hampshire's privacy law takes effect January 1, 2025 and affects entities that do business in the state that target residents if they control the personal data of at least 35,000 residents, with some exceptions, or control at least 10,000 residents while deriving more than a quarter of their gross revenue from the sale of personal data. New Hampshire continues the trend of including a broad definition of sensitive data and follows in Delaware's footsteps by prohibiting the processing of data without prior parental consent for targeted advertising if the controller has actual knowledge that the consumer is thirteen to sixteen years old. Both New Hampshire and New Jersey specify the definition of consent as the same type of express, unambiguous, and unbundled agreement that has been seen in several other state privacy laws.

Several other comprehensive state privacy laws will take effect or have deadlines this year, including Oregon and Texas's comprehensive laws becoming effective on July 1st, and Montana's comprehensive law on October 1st. On January 1st in California, data brokers were required to be registered with the new California Privacy Protection Agency (CPPA) and starting July 1st data brokers must collect and report information in their privacy policies regarding the types of CCPA requests the brokers have received. In addition, as of March 29, 2024, there is no longer a cure period for enforcement of the CPRA regulations, and companies must ensure they have a data request process in place for HR data, as well as other unique requirements under the California law. The CPPA also released draft regulations for updated cybersecurity audits, which would apply to businesses that receive 50% or more of their gross annual revenue from selling or sharing personal data, as well as businesses that meet a few other yet to be defined thresholds.

Looking to Colorado, on July 1st, controllers under the Colorado Privacy Act must recognize approved universal opt-out mechanisms, provide an explanation of how requests using these mechanisms will be processed, and controllers must get consent to process any sensitive data they collected without valid consent prior to July 1, 2023. Finally, in Connecticut, on December 31, 2024 the right to the sixty day cure period ends.

Numerous bills have been proposed to amend many existing state privacy laws and to create new laws, including bills proposing to strengthen protections for children's data, biometric data, requirements relating to AI, and more. The volume of these bills is too great to discuss in this short article, but we are watching these bills closely and will provide further updates if/when these bills become law.

My Health My Data Act

2024 will also bring significant obligations from new consumer health data laws, most notably Washington's My Health My Data Act (MHMDA) which goes into effect on March 31, 2024. MHMDA covers a broad range of entities: it applies to any business, including non-profits, that conduct business in Washington and collect, process, share, or sell consumer health data, which is broadly defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." Opt-in consent is needed for the sale of such data.

Although Washington does not yet have a comprehensive data privacy law, MHMDA provides similar consumer rights and controller/processor duties as other existing state laws. However, the Attorney General's updated guidelines state that entities should have a separate and distinct privacy policy (with unique requirements) for consumer health data, accessible via a separate link. Because MHMDA offers a private right of action (in addition to enforcement by the state's Attorney General), we anticipate significant litigation as soon as this law becomes effective.

Nevada and Connecticut quickly passed laws similar to the MHMDA. Nevada's goes into effect the same date as MHMDA, and Connecticut's is an amendment to its comprehensive data privacy law, which took effect on July 1, 2023, and more states are expected to follow.

Federal Agency Developments

In addition to advancements at the state level, federal agencies are also expected to continue to change the data privacy landscape in 2024. At the end of last year, the Federal Trade Commission announced a Notice of Proposed Rulemaking to update the Children's Online Privacy Protection Rule (COPPA). The proposed changes would drastically change how companies can control and process the data of minors, potentially requiring parental opt-in consent for targeted advertising and third party disclosures, diminishing companies' ability to nudge kids to return to their services, limiting retention of minor's data, formalizing guidance in the ed tech sector, and strengthening data security requirements. The FTC has also indicated its willingness to continue robust enforcement actions in the data privacy space, as illustrated by its enforcement actions in early January against InMarket Media and Outlogic LLC regarding their sales of precise location data, and specifically for failing to disclose how they used location data and retaining the data longer than reasonably necessary.

Authorities are also emphasizing the need to regulate artificial intelligence as it relates to privacy in 2024. The FTC broadcasted their AI-powered voice cloning challenge in January and the Federal Communications Commission also opened a Notice of Inquiry to investigate AI generated robocalls.

The FTC may also finalize its Health Breach Notification Rule this year and the Consumer Financial Protection Bureau is expected to complete a proposed Personal

Financial Data Rights Rule by late 2024 which would compel banks to make transaction data available to consumers and track their data requests.

Conclusion

Overall, 2024 is looking to be another busy year in the data privacy world. For more information or help navigating the realm of data privacy, please contact Dorsey's data privacy and cybersecurity team.