Shumaker

FEBRUARY 13, 2026 | PUBLICATION

The Patchwork of Data Privacy Laws: Recent Developments and Implications

The data privacy landscape in the United States continues to evolve at a rapid pace, but state-to-state changes are seldom uniform. For businesses operating across multiple jurisdictions, the challenge of maintaining compliance is increasingly complex and requires ongoing monitoring of regulatory developments. A few recent developments worth monitoring include Maryland's new comprehensive privacy law, Rhode Island's distinctive approach to applicability, Connecticut's Artificial Intelligence (AI) disclosure amendment, California's treatment of youth data as sensitive personal information, and updates to the federal Children's Online Privacy Protection Act (COPPA) framework.

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis
Andrew R. DeWeese

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Maryland's Comprehensive Data Privacy Law

Maryland's Online Data Privacy Act (MODPA), signed into law on May 9, 2024, represents one of the most stringent state privacy regimes enacted to date. The law became effective on October 1, 2025, though it does not apply to personal data processing activities that occurred before April 1, 2026. This approximately 18-month implementation timeline, which will soon close at the time of this article's publication, has now largely elapsed, making compliance a pressing priority as organizations should anticipate enforcement efforts to begin imminently.

MODPA applies to businesses conducting business in Maryland or offering goods or services to Maryland residents that either control or process the personal data of at least 35,000 Maryland consumers, or control or process data of at least 10,000 consumers while deriving more than 20 percent of gross revenue from data

sales. Unlike many other state privacy laws, MODPA does not include a revenue-based threshold for applicability, which broadens its reach.

MODPA also contains a few unique privacy hallmarks.

- It has a data minimization mandate that requires data controllers to limit collection to what is "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer."
- MODPA outright bans the sale of sensitive data, regardless of consumer consent.
- The law prohibits targeted advertising and data sales involving consumers the data controller knows or should know are under 18 years of age.

Rhode Island's Data Transparency and Privacy Protection Act (RIDTPPA)

RIDTPPA, enacted on June 28, 2024, took effect on January 1, 2026. Its approach to determining which entities fall within its scope contains distinctive features.

Like other states, RIDTPPA establishes threshold-based applicability for its comprehensive consumer rights provisions: businesses must have controlled or processed data of at least 35,000 Rhode Island residents, or processed data of at least 10,000 residents while deriving more than 20 percent of gross revenue from data sales. Notably, RIDTPPA lacks a revenue-only threshold. Like MODPA, a data controller can become subject to RIDTPPA if it controls the data of enough state residents, lowering the bar for regulatory coverage compared to other state regimes.

RIDTPPA also has stringent privacy notice requirements. Businesses that do not meet RIDTPPA's consumer data thresholds are still required to meet certain disclosure obligations if they operate "[a]ny commercial website . . . in Rhode Island or with customers in Rhode Island." This broad approach requires any business with a Rhode Island presence—even just one customer—to comply with RIDTPPA's disclosure requirements.

Another key feature of RIDTPPA is its lack of cure period. Unlike other states that give businesses a chance to fix violations before enforcement action begins, RIDTPPA allows the Rhode Island Attorney General to enforce immediately. In other words, noncompliance is immediately punishable.

Connecticut's AI Disclosure Requirement

On June 25, 2025, Connecticut enacted Senate Bill 1295. This new Bill amended the Connecticut Data Privacy Act (CTDPA) to include state-mandated disclosure requirements regarding the use of personal data to train large language models (LLMs). Effective July 1, 2026, data controllers subject to the CTDPA must update their privacy notices to include clear, conspicuous statements disclosing whether personal data is used, collected, or sold to train LLMs (including widely known models such as ChatGPT, Gemini, DeepSeek, and Grok, among others).

The new CTDPA amendments are notably broad. As written, the amendment applies to *any* use of personal data to train LLMs. Adding ambiguity, the law does not expressly define "large language models," leaving businesses to determine whether related AI systems—such as smaller models or fine-tuned versions—fall within scope. Until the law is interpreted and applied, organizations should consider taking a conservative approach in determining which systems, LLMs, and software fall within its purview.

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) Treatment of Youth Data as

Sensitive Personal Information

California continues to be a major player in the data privacy landscape, with its most recent regulatory developments redefining the treatment of youth data. California's regulations now define sensitive personal information to include "personal information of consumers that the business has actual knowledge are less than 16 years of age."

This new classification carries operational implications. Under the CPRA, consumers have the right to limit a business's use and disclosure of their sensitive personal information to purposes necessary for providing requested goods or services. By classifying minors' data as sensitive, businesses must now treat such data with the heightened protections that the law requires, including honoring consumer requests to limit use of sensitive personal information to purposes necessary for providing requested goods or services.

CCPA already required business to obtain affirmative authorization before selling the personal information of consumers under 16 years of age. For children under 13, consent must come from a parent or legal guardian. For consumers age 13 to 15, the consumer may consent themselves. Regardless, though, any information about consumers under 16 now qualifies as "sensitive information" in California.

COPPA Updates at the Federal Level

On January 16, 2025, the Federal Trade Commission finalized significant amendments to the COPPA Rule—the first major overhaul since 2013. The amendments took effect on June 23, 2025, with a compliance deadline of April 22, 2026 (about two months away at the time of this article's publication), which is now imminent.

One key amendment requires the operators of child-directed websites to obtain verifiable parental consent before the website owner may disclose a child's personal information to third parties. This is particularly noteworthy for advertisers targeting audiences under 18 years old, as it imposes additional friction on data sharing for marketing purposes.

For businesses operating nationally, understanding the interplay between COPPA and state-level children's privacy requirements is critical. COPPA establishes a federal floor for children under 13, while state laws often extend protections to teenagers or impose additional substantive requirements.

Age Verification and Age Assurance: Emerging State Requirements

Beyond comprehensive privacy laws, a significant and rapidly expanding trend concerns state laws requiring age verification or age assurance measures. Currently, 21 states have enacted laws with age assurance provisions, primarily targeting access to pornographic or other content deemed "harmful to minors." These laws typically require commercial entities to verify that individuals seeking to access restricted material are 18 years of age or older.

To a lesser extent, age assurance provisions also appear in legislation seeking to prevent minors from creating or maintaining social media accounts without parental consent. States including Texas, Utah, Louisiana, and others have enacted such requirements, though many face ongoing constitutional challenges on First Amendment and privacy grounds.

Additionally, several states, including California, Utah, and Texas, have recently enacted laws requiring app developers, app store providers, and device operating system providers to implement age verification at the device or platform level. For example, California's Digital Age Assurance Act (AB 1043), signed in October 2025, requires operating system providers to prompt users to indicate their age during device setup. These

laws represent a significant expansion of age verification beyond individual websites to foundational technology infrastructure.

Businesses operating nationally should monitor this patchwork of age verification laws closely, as noncompliance may result in substantial penalties and restricted access to key markets.

If you have questions about how these evolving state and federal privacy requirements may impact your organization or would like assistance assessing your current compliance posture, updating privacy notices, and documenting AI/data governance practices, please contact Jade Davis, Andrew DeWeese, or another member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker