

Introduction

The absence of federal regulation has created a vacuum into which states have stepped at a remarkable rate. With hundreds of bills proposed at the state level in 2025 and 2026, here are the trends and developments you need to know to prepare for this evolving landscape.

What You Need to Know: Privacy

- States are increasingly focused on “data brokers,” and expanding what that means.
- Privacy laws are also expanding in other ways, covering more entities and defining more data as “sensitive.”
- States are further restricting what companies can do with sensitive personal information, including outright banning “sales.”
- The kid and teen privacy landscape continues to fragment, creating significant compliance challenges.
- And new comprehensive privacy laws continue to iterate on existing frameworks, with a few standouts in the latest group of states.



Five key trends are driving the latest legislative developments on privacy:

1. Data Broker regulations are increasing and expanding in scope.

States are building on the data broker framework initially pioneered in California by creating expansive definitions and new categories of covered entities. Connecticut and New Jersey both recently enacted new laws that apply broadly and add meaningful differences when compared to other states. Connecticut’s new provisions take effect on October 1, 2026, with a new data broker registration requirement starting on January 1, 2027. A “data broker” is defined as any business that sells or licenses “brokered personal data” to another person. There are exceptions, such as exclusions applying only to businesses that collect information about consumers that are or were “in a contractual relationship with the business,” an investor, a donor, or in another “similar” relationship with the business. Connecticut’s law also establishes an accessible deletion mechanism program similar to California’s Delete Request and Opt-out Platform (DROP) mechanism. California’s DROP launched on January 1, 2026, and while data brokers operating there must begin processing deletion requests by August 1, 2026, Connecticut residents will have to wait until July 1, 2028, to submit similar requests.

Unlike Connecticut, New Jersey's new data broker law took effect immediately upon enactment. After an overwhelmingly negative reaction across industries, New Jersey's Division of Consumer Affairs (DCA) advised that covered entities will not need to register or pay fees until registration begins, currently scheduled for spring 2027. The statute also directs the DCA to adopt rules and regulations for implementation, and the regulator has indicated that it expects to issue guidance to help entities understand and comply with the new requirements. Even so, the law introduces unusually high fees and severe penalties, while also creating a new category of covered entity – "data collectors" – specifically defined to bring in-scope businesses that collect information directly from consumers and then sell or license it to a data broker. Both data brokers and data collectors must register, which means both consumer-facing businesses and data suppliers will face annual fees well above those under other state data broker registries. Keep an eye on developments in New Jersey, as the reaction from industry indicates there could be a significant push for amendments.

2. States are expanding the application of and definitions in comprehensive privacy laws. In addition to expanding "data broker" definitions, other states have been amending their comprehensive privacy laws to expand other definitions and thresholds for coverage. Connecticut and New Jersey both led the way again, applying their restrictions on sensitive data to any business – even those that do not otherwise meet applicable thresholds. Similarly, Montana enacted changes for handling minors' data that apply to any entity in Montana.

States are also revising their definitions of "sensitive" data. Connecticut amended its definition of sensitive data to include the following new elements: mental or physical disabilities or treatments; status as transgender or nonbinary; status as a victim of a crime; information derived from biometric data; information from an individual the controller has actual knowledge, or willfully disregards, is a child; neural data; a consumer's financial account number, financial account login information, or credit card or debit card number in combination with a required access code or password; or government-issued identifiers, like Social Security numbers.

In Maryland, the legislature revised the state's definition of sensitive data to focus on "sensitive attributes," and expressly includes data inferred to indicate race, religion, health, or sex life. Given Maryland's strict ban on the sale of sensitive data, this could make certain inference-based advertising segments "sensitive data," and is one of the most highly restrictive ads-related amendments to watch in 2026.

3. States are significantly restricting how businesses can process sensitive personal information.

State legislatures have enacted laws and amendments that severely curtail the sale of sensitive personal data generally, and geolocation data specifically. New Jersey and Maryland recently banned the sale of all sensitive data and, as noted above, New Jersey applies this restriction regardless of the number of consumers whose data the entity processes or controls. The legislature in Delaware enacted amendments with a similar prohibition. Oregon, Virginia, and Connecticut further prohibit the

sale of precise geolocation data, while Oregon and New Hampshire prohibit the sale of kids' data. Oregon's restriction applies to individuals under 16 years of age, while New Hampshire's applies to children under 13. In each case, consent is no exception to the prohibition and the ban is absolute. Companies will need to revisit their data flows to address these bans, particularly where consumer consent was a key part of existing business practices.

4. Child and teen privacy remains a focus across jurisdictions. Federal and state lawmakers are expected to continue their ongoing, focused efforts to require that businesses do more to keep children and teens safe online. Even with bipartisan support in Congress, however, none of the various federal proposals have crossed over the finish line to enactment. In the meantime, states have passed dozens of laws aimed at boosting online privacy and safety protections for children in ways that merge privacy, security, AI governance and online safety concerns.

More than a dozen states have now passed age-appropriate design codes and laws limiting children's access to social media. Requirements under these laws echo federal proposals, including default privacy settings for minors. Others go further, enacting social media "bans" for children under 14. Industry groups like NetChoice have filed challenges on First Amendment grounds, with some initial success, but appellate courts are now revisiting preliminary rulings and lifting injunctions. For example, the Texas App Store Accountability Act is now in effect after a series of court rulings lifted a prior injunction. App store operators and developers now must deal with an obligation to request age signals and block minors in Texas from downloading apps in the absence of parental consent. Certain portions of California's Age Appropriate Design Code Act – including an age estimation requirement – are now in effect after court rulings earlier this year. State attorneys general remain very engaged in this space and have indicated enforcement of these laws will begin as soon as possible.

Other states are moving forward with implementing regulations. In July 2026, New York Attorney General Letitia James released final rules on how social media companies must restrict "addictive features" on their platforms to comply with the SAFE for Kids Act. The Act requires age assurance and strict parental consent requirements for minors using social media, and the regulations take effect on January 25, 2027.

As states continue to legislate and update requirements for these age groups, companies face significant operational challenges in developing and implementing compliance models against an increasingly complex and fragmented landscape.

5. New state comprehensive privacy laws come with new nuances. Last year gave companies a bit of breathing room, as no states passed comprehensive privacy laws in 2025. By contrast, this year, Alabama, Louisiana, Oklahoma, and Vermont have already added to the sprawling state privacy law landscape regulating how companies handle consumers'

personal information. Each state law shares a few core principles with existing frameworks, which reinforces a sense that states are converging around certain key consumer rights, disclosure requirements, and protections for sensitive personal data.

Even so, each state also added its own nuances. For example, Oklahoma's law is considered more business- and ad-friendly but includes pseudonymous data in its definition of "personal data," so that hashed identifiers tied to a match key remain regulated. Vermont applies some of the lowest numeric thresholds in any state (selling data on just 3,000 Vermonters puts a business in-scope). Vermont further prohibits both targeted advertising and sale of personal data of a consumer known to be between 13 and 17 years old – with no consent override. Vermont also enacted a requirement previously found only in Connecticut's amended privacy law, adding that privacy notices must disclose whether personal data is collected, used, or sold to train large language models. Interestingly, Alabama excluded analytics and controller-only marketing disclosures from its definition of "sale," so measurement and agency data flows that count as sales elsewhere are carved out here. Finally, Louisiana requires controllers that sell sensitive data include specific language in their privacy notices ("NOTICE: We may sell your sensitive personal data"), with an equivalent notice for biometric data sellers.

Congress has shown some renewed interest in a uniform federal privacy framework, with legislation introduced earlier this year, but various proposals have met with significant backlash and failed to generate much traction. In the meantime, expect to see more nuanced frameworks and developments like these at the state level.

What You Need to Know: AI

- The only federal law that squarely addresses AI focuses on "deepfakes" and nonconsensual intimate imagery.
- States are under federal pressure to limit AI regulation but continue to pass laws on transparency and safety.
- Initial momentum for comprehensive state AI regulation has mostly fizzled in favor of a more targeted, piecemeal approach.

1. The federal TAKE IT DOWN Act focuses on specific "deepfake" harms. The U.S. currently has just one major federal law focused on artificial intelligence – the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (or the TAKE IT DOWN Act) – in effect as of May 2026. The Act criminalizes nonconsensual publication of intimate images, requiring that platforms remove covered content with 48 hours of notification. Criminal penalties can be imposed for unlawful distribution. While there has been some limited congressional action since related to addressing "catastrophic" risks, no other legislation has passed. Executive orders have signaled a federal preference for a more centralized and minimally burdensome AI framework, while promoting voluntary reviews of advanced models in light of hacking and security concerns. In response to a recent executive order, the Federal Trade Commission issued a proposed

policy statement on the potential legal implications of state laws that require changes to “truthful outputs” from AI models. For now, though, states continue to fill the regulatory void.

2. Common regulatory trends are emerging in state legislation. The volume of artificial intelligence bills proposed at the state level has been significant, and almost every state has at least one law in this area. While the laws differ significantly from state-to-state, four common trends have emerged.

Transparency and disclosure. Many state laws aim to prevent consumer deception by requiring disclosures and even periodic reminders that individuals are interacting with AI. Laws regulating “companion” chatbots have proliferated, with more specific requirements for minor users and mental health guardrails where the chat interaction leverages AI and provides adaptive, human-like responses to inputs across multiple interactions. Certain exceptions may apply for chat features used for operational purposes, customer support, and solely internal purposes.

Automated decision-making technologies and algorithmic pricing. Privacy and AI continue to merge as states enact laws requiring that businesses offer consumers notice of certain automated decisions that produce a legal or other significant effect on the individual or the ability to opt out of processing of personal information for “profiling.” Additional state laws make it clear that anti-discrimination laws apply to use of AI in ways that unlawfully discriminate on the basis of protected characteristics. Algorithmic decision-making and pricing are also under scrutiny at the state level, with certain laws prescribing disclosures or prohibiting use of tools that use personal information to set prices. While these laws do not address advertising or ad targeting directly, they still impact the advertising ecosystem and data flows.

Deepfakes and digital replicas. Nearly every state now has a deepfake law, and intimate imagery statutes similar to the TAKE IT DOWN Act are nearly universal. Other states have outlawed certain AI-generated deepfakes in the context of elections, and criminalized deepfake use to commit fraud or other crimes. A different set of enacted laws specifically addresses the creation and use of digital replicas using AI with specific contractual requirements. New York requires a specific label for fully synthetic performers, while digital replica statutes in New York and California establish consent and contract formalities for use of AI on real performers.

Frontier models. States have started enacting laws that specifically apply to rapidly evolving, large-scale, and complex “frontier” models, with a focus on safety standards, audits, pre-release review, governance frameworks, and whistleblower protections.

Most states have focused on specific legislative fixes covering one or two of the above issues at a time. For example,

California's AI package focuses on transparency, frontier AI, and training data. Similarly, Colorado recently repealed its more comprehensive AI Act and replaced it with a narrower framework focused on disclosure and transparency. Companies have been watching Colorado closely, since its AI Act initially aimed to set broad and significant governance requirements for "high-risk" AI systems. The revised AI Act now focuses exclusively on automated decision-making technologies and requires notice when using AI in certain employment, healthcare, and housing decisions.

Regulators recently proposed draft regulations intended to clarify obligations for developers and deployers, disclosure and reporting requirements, and consumer rights.

By contrast, Connecticut's recently enacted Online Safety Act (SB5) creates an omnibus AI package that aims to cover almost all of these topics and more, including chatbot safety, foundation model risks, AI in employment decisions, synthetic content labeling, and subscription transparency, among other concerns. Portions of Connecticut's new law even reach beyond AI to include youth online safety requirements. Connecticut's law goes into effect October 1, 2026, with key compliance dates varying and most obligations starting in 2027.

Organizations that deploy AI systems should expect more legislative activity in this area and must regularly evaluate existing compliance programs as states continue to act.



Author



Caroline Hudson

Partner
Loeb & Loeb LLP