WILSON SONSINI

Recent AI Regulatory Developments in the United States

CONTRIBUTORS


Maneesha Mithal


Demian Ahn


Hale Melnick


Michelle Ullman

ALERTS

May 7, 2026

While the EU Artificial Intelligence (AI) Act has set forth a relatively uniform framework for AI regulation in the EU, U.S. AI regulation has so far primarily consisted of a patchwork of state laws—which continue to evolve at a rapid pace. Despite the Trump administration calling for Congress to pass AI legislation that would preempt overly burdensome state laws in its National Policy Framework for Artificial Intelligence, many states appear to be actively moving ahead with new legislation. Here are the top areas the states are targeting, followed by some key takeaways:

1. **Companion Chatbots.** Several states have passed laws that regulate the operation of "companion chatbots," which generally refer to AI systems with a natural language interface that provide human-like responses to user inputs and simulate human conversation and interaction. Many of these laws require operators of companion chatbots to provide a clear and conspicuous disclosure to the user that they are interacting with a chatbot, not a human. *See, e.g.*, CA SB 243. New York's companion chatbot law requires these disclosures to be made at the beginning of a user's interaction with a companion chatbot and at least every three hours during continued interaction. Washington state's companion chatbot law, which includes similar requirements, will go into effect in January 2027. WA HB 2225 § 3(2)(a)-(b); NY SB S3008C Art. 47, § 1702. Other states have imposed harm mitigation and reporting obligations for particularly vulnerable users, such as minors and individuals expressing ideations of self-harm or suicide. Notably, California's chatbot law will require companion chatbot operators to annually report to the state's Office of Suicide Prevention their protocols to detect, remove, and respond to instances of suicidal ideation by users beginning on July 1, 2027. CA SB 243 § 22603(a)(2)-(3). Chatbot laws have also recently been introduced at the federal level. (See the Children's Health, Advancement, Trust, Boundaries, and Oversight in Technology Act (CHATBOT Act) and the Guidelines for User Age-Verification and Responsible Dialogue Act (GUARD Act).)
2. **Surveillance Pricing.** States are also beginning to regulate surveillance pricing, which generally refers to the practice of collecting consumers' personal information and charging different prices to a consumer or group of consumers for identical goods or services.

   On April 28, 2026, Maryland became the first state to **prohibit** certain differential pricing practices. Effective October 1, 2026, HB 0895 will prohibit food retailers and third-party delivery services from (1) using protected class data to offer or price goods in a way that denies consumers equal access to benefits or services; and (2) engaging in dynamic pricing, defined generally as the discriminatory practice of offering or setting a personalized price for a good or service that is specific to a consumer based on the consumer's personal data. The law exempts certain practices such as loyalty programs, subscription-based contracts, and pricing differences based on costs, supply, or demand.

   While the Maryland law prohibits dynamic pricing in certain sectors, New York's Algorithmic Pricing Disclosure Act requires entities to provide a "clear and conspicuous disclosure" that alerts

consumers that their personal data is being used for the purpose of setting a personalized price. In July 2025, the National Retail Federation (NRF) sued to block the law, arguing that it violates the First Amendment rights of businesses by compelling them to use specific language in their consumer-facing messaging. The lawsuit was dismissed with prejudice in October 2025. The court determined that the law's disclosure requirement triggers a more permissive standard of scrutiny because the pricing law "mandates the disclosure of 'purely factual and uncontroversial' commercial speech."[1] The NRF appealed the decision, but the law remains in effect pending appeal.

3. **Nonconsensual Publication of Intimate Images and AI-Generated "Deepfakes."** The federal Take it Down Act (TiDA) will go into effect on May 19, 2026. Among other things, TiDA will make it illegal to "knowingly publish" or threaten to publish intimate images without a person's consent—including AI-generated "deepfakes." The law will also require covered platforms (defined as public websites and online services that primarily provide a forum for user-generated content) to remove non-consensual intimate depictions within 48 hours of receiving notice from a victim. Covered platforms must also take steps to remove duplicative content.

   Federal law and many state laws concerning obscenity and child sexual abuse material (CSAM) have historically applied to AI-generated images. However, in recent months several states have also expanded the scope of their existing criminal laws to more explicitly include the creation and distribution of certain AI-generated images. For example, California now classifies artificially generated or digitally altered child sexual assault material (CSAM) as child pornography. CA AB 1831 and CA SB 1381. Similarly, CA SB 926 criminalizes the creation and distribution of computer-generated sexually explicit content.
4. **Regulation of High-Risk Use Cases.** The Colorado state legislature enacted the Colorado Artificial Intelligence Act (CAIA) in May of 2024, which would have applied to developers and deployers of "high risk AI systems," defined as AI systems that make, or are a substantial factor in making, a "consequential decision." Although the fate of the CAIA is uncertain as a result of ongoing litigation, new regulations under the California Consumer Privacy Act (CCPA) were approved to include a similar framework. Under the new CCPA regulations, businesses that use "automated decision-making technology" (ADMT) to make "significant decisions" about consumers will be required, among other things, to provide consumers with a pre-use notice, the ability to opt out of the use of ADMT, and access to information about the business's ADMT use. As we noted in a previous client alert, the regulations would cover companies that use AI to "substantially replace" human decision making surrounding "significant decisions." "Significant decisions" are those that result in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services. These regulations went into effect on January 1, 2026, but businesses must come into compliance with the new ADMT requirements by January 1, 2027.
5. **Generative AI Transparency.** Some state AI laws have focused on transparency of training data and watermarking. For example, CA AB 2013—which came into effect on January 1, 2026—requires developers of generative AI systems or services to post documentation on their websites regarding the data they used to train their generative AI systems or services. CA SB 942—which came into effect on January 1, 2026—requires covered providers to include a latent disclosure in AI-generated images, videos, and audio content created by the covered provider's generative AI system regarding the provenance of the content.

   At the federal level, the Protecting Consumers From Deceptive AI Act was introduced on April 23, 2026. This bill would direct the National Institute of Standards and Technology (NIST) to develop guidelines for watermarking, digital fingerprinting, and provenance metadata for AI-generated audio and visual content. It would also require NIST to support labeling standards for AI-modified content on platforms and develop frameworks for identifying AI-generated text.
6. **Frontier Model Regulation.** As discussed in a prior client alert, California and New York have enacted sweeping state laws regulating frontier AI models. Frontier AI models are generally defined as the most advanced general-purpose models that can enable advanced reasoning, generation of images, text, and audio, and the functioning of agentic workflows. Most provisions of California's Transparency in Frontier AI Act (or CA SB 53) became effective on January 1, 2026. Both statutes require large frontier AI model developers to, among other requirements, create and publish an AI safety and security framework, report certain safety incidents, and provide transparency disclosures related to frontier AI models' risk assessment and use.

   In March 2026, New York amended the RAISE Act to more closely mirror CA SB 53, which could potentially ease some multistate compliance challenges for large frontier AI model developers. First, the amendment narrows the scope of frontier developers classified as "large frontier developers" that are subject to certain additional requirements. Specifically, the amendment replaces the previous compute-based definition of a "large frontier developer" with a revenue-based threshold that is the same as the one under CA SB 53 (i.e., developers that exceed $500

million in annual gross revenue in the preceding calendar year). Second, the amendment significantly reduces civil penalties that the New York Attorney General may impose from $10 million to $1 million for a first violation, and from $30 million to $3 million for subsequent violations. This change more closely mirrors the penalties under CA SB 53—which are capped at $1 million per violation. Finally, enforcement of the RAISE Act is now delayed until January 2027. This amendment gives frontier AI model developers more time to assess and comply with their revised obligations under the RAISE Act.

Takeaways: How should companies develop and implement a compliance framework around these regulations?

- **Determine which laws apply:** Although compliance with the emerging patchwork of numerous state laws may seem daunting, some apply to developers, while others apply to deployers; some apply only in specific sectors; and some apply only for specific use cases. In addition, many of them include exceptions.
- **Monitor enforcement and civil litigation trends**: Regulators and civil litigants may proceed with enforcement actions and lawsuits even in the absence of new laws, leveraging existing consumer protection statutes and other theories of liability.
- **Develop an AI governance framework:** This may include developing an internal governance structure for approval of new products/systems; creating diligence questions for third party vendors; and creating guardrails around AI use. Provide workforce members with guidance on use of off-the-shelf AI tools, such as how to turn off training data.
- **Maintain and update incident response plans**: This includes updating and adapting cybersecurity incident response plans for the AI context, in addition to developing incident response plans for other types of AI-related safety and security incidents.
- **Develop compliant external disclosures:** This may range from disclosures that AI is being used to training data transparency requirements for model developers.

Wilson Sonsini works with clients developing, deploying, and using AI across the regulatory spectrum, and we are actively monitoring state and federal AI laws and regulations as well as litigation and enforcement trends. For more information, please contact Maneesha Mithal, Demian Ahn, Hale Melnick, Michelle Ullman, or any member of Wilson Sonsini's Artificial Intelligence and Machine Learning and Data, Privacy, and Cybersecurity practices.

---

[1] https://assets.law360news.com/2397000/2397728/https-ecf-nysd-uscourts-gov-doc1-127138350514.pdf.