WILSON SONSINI

2026 Year in Preview: AI Regulatory Developments for Companies to Watch Out For

CONTRIBUTORS

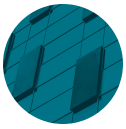

Maneesha Mithal


Jodi Daniel


Doo Lee


Laura De Boel


Demian Ahn


Lidia Niecko-Najjum

ALERTS

January 13, 2026

In 2026, businesses will face an increasingly complex regulatory environment for Artificial Intelligence (AI). With new state laws and various federal action on the horizon, here's our top 10 list of what businesses should watch out for in the AI regulatory space in 2026:

1. **For companies operating in the European Union, be prepared for new EU AI Act requirements to become effective**. In 2025, the first wave of AI Act requirements relating to new general purpose AI models (GPAI) released in the EU and prohibited uses of AI became applicable. By August 2, 2026, companies will need to comply with specific transparency requirements and rules for certain types of high-risk AI systems (HRAI).

   To help companies navigate the new AI Act requirements, the European Commission (EC) is expected to publish guidance in 2026, including on the practical application of many AI Act requirements and the AI Act's interplay with EU data protection law. The EC is also developing a new Code of Practice for marking and labeling AI-generated content, to support compliance with some of the AI Act's transparency obligations. A first draft was published on December 17, 2025, and it is expected to be finalized by June 2026.

   At national level, many EU countries are still appointing the regulators that will be tasked with overseeing and enforcing the AI Act requirements in each country. More laws implementing the AI Act in EU countries are expected to be passed in 2026, and companies should monitor country-specific nuances (e.g., Italy's AI law, which entered into force on October 10, 2025, is closely aligned with the AI Act but contains some Italy-specific provisions such as additional protections for minors under 14).

   As implementation progresses, there are parallel talks of amending legislation relevant to AI in 2026. In November 2025, the EC published a set of legislative proposals which would make important changes to the legal framework for providing and deploying AI in the EU, such as extending the date of applicability of the rules on HRAI from August 2, 2026, to December 2027 at the latest. EU lawmakers will negotiate the amendments in 2026, and further changes will likely be made before they are passed. For more information on the EC's proposals, see previous alert here.
2. **For companies developing or deploying AI for consequential decisions (e.g., financial or lending services, education and employment opportunities, healthcare, housing, essential government services, or legal services), be prepared for new U.S. state laws regulating high-risk AI use.** For example, under new regulations issued under the California Consumer Privacy Act, businesses that use "automated decision-making technology" or ADMT to make "significant decisions" about consumers must 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. Businesses must comply with these requirements beginning January 1, 2027. In addition to California, the Colorado AI Act,

Hattie Watson

Joseph (Tony) Misher

currently slated to come into effect on June 30, 2026, will place substantial new responsibilities on AI developers and deployers, including requirements to undertake reasonable care to avoid algorithmic discrimination, to develop a risk management policy and program, to implement notices, and to conduct impact assessments, among other requirements. According to media reports, the law is expected to be the subject of debate during the legislative session this year and may change before it goes into effect in 2026.

3. **Prepare for increased state AG oversight.** State attorneys general (AGs) and regulators stepped up scrutiny and enforcement actions related to AI issues last year, and we expect that trend to continue in 2026. For example, in May 2025, the Pennsylvania Attorney General announced a settlement with a property management company over allegations that the company's use of an AI platform to assist in its operations contributed to delays in maintenance repairs and rentals of unsafe housing in violation of state laws. In July 2025, the Massachusetts Attorney General announced a $2.5 million settlement with a student loan company to resolve allegations that the company's lending practices, including its use of AI models, violated various consumer protection and fair lending laws by unfairly placing historically marginalized student borrowers at risk of being denied loans or receiving unfavorable loan terms.
4. **Protect against AI-related cyberattacks.** AI-related risks—and AI-related cyberattacks—will dominate cybersecurity headlines throughout 2026. Threat actors will leverage generative AI to orchestrate cyberattacks at previously impossible speeds; employees will use unsanctioned AI tools and cause inadvertent leaks; and AI integrations will open new attack vectors for exploitation. Regulators, customers, and auditors will increasingly expect provable security controls across the AI lifecycle (data sourcing and ingestion, training/tuning, deployment, monitoring, and incident response)—and the absence of AI-specific cybersecurity regulations will not prevent regulators from scrutinizing AI-related security under existing frameworks. The U.S. Securities and Exchange Commission's (SEC) Division of Examinations, for example, has identified cybersecurity and operational resiliency, including AI driven threats to data integrity and third-party vendor risk, as a focus area for examinations in FY2026. Similarly, the SEC's Investor Advisory Committee recently recommended enhanced disclosures concerning how boards oversee AI governance as part of managing material cybersecurity risks.

   The cyber insurance market is undergoing an AI-related transformation, with many carriers increasingly conditioning coverage on the adoption of AI-specific security controls. Insurers have begun introducing "AI Security Riders" that require documented evidence of adversarial red-teaming, model-level risk assessments, and specialized safeguards as prerequisites for underwriting. We expect this trend to continue in 2026, and it will become increasingly common for insurance carriers to require alignment with recognized AI risk management frameworks as a baseline for "reasonable security."
5. **For frontier AI developers, undertake compliance efforts under new frameworks.** In late 2025, two major U.S. states—California and New York—enacted sweeping state laws regulating frontier AI models. In California, Governor Gavin Newsom signed S.B. 53 (the Transparency in Frontier AI Act) into law, and in New York, Governor Kathy Hochul signed S.B. S6953B (the Responsible AI Safety and Education Act, or RAISE Act) into law. Both statutes require large frontier AI developers to create and publish an AI safety and security framework, report certain safety incidents, and provide transparency disclosures related to frontier AI model's risk assessment and use, among other requirements. Most provisions of California's S.B. 53 became effective starting January 1, 2026. New York state lawmakers are expected to approve the modified version of New York's RAISE Act that Governor Hochul signed in December in early 2026.
6. **Comply with new AI training data transparency requirements.** Under California AB 2013, developers of generative AI systems (subject to narrow exceptions) are now required to publicly disclose information about their AI system's training data, including detailed summaries of datasets used for training generative AI systems. See our previous alert here. Covered developers are required to disclose information such as the number of data points within the datasets, whether the datasets include protected intellectual property or personal information, and whether the datasets were purchased or licensed, among other requirements.[1]
7. **Consider risks associated with AI chatbots, particularly those that may be used by minors.** In 2025, federal and state regulators from both blue and red states began scrutinizing AI-powered "companion chatbots." For example, in September 2025, the Federal Trade Commission launched an inquiry into AI chatbots acting as companions. In November 2025, the North Carolina AG Jeff Jackson (Democrat) and Utah AG Derek Brown (Republican) announced the formation of a new bipartisan task force that will work to "identify emerging issues related to AI and develop safeguards that AI developers should follow to protect the public" to prevent harm to users, especially children, as AI technology develops. Most recently, on December 9, 2025, the National Association of Attorneys General sent a letter on behalf of 42 state AGs to multiple AI companies expressing concern about "sycophantic and delusional" AI outputs. The letter urges the AI companies "to adopt additional safeguards to protect children" and warns that "[f]ailing to adequately implement additional safeguards may

violate our respective laws." Further, in 2025, Utah, Nevada, New York, Maine, Illinois, and California enacted new laws regulating AI-enabled chatbots.

8. **Monitor evolving federal and state policies on AI and health.** The U.S. Department of Health and Human Services (HHS) is looking to advance the use of AI innovation in healthcare. At the end of 2025, HHS published a request for information (RFI) on accelerating adoption and use of AI in clinical care. See our previous alert here. The RFI addressed regulation (including confidentiality, governance, liability, evaluation and testing, and interoperability), reimbursement, and research and development. In 2026, HHS is expected to take action based on this RFI feedback. The FDA has already published guidance in 2026 that will reduce regulatory oversight for some AI-enabled technology. HHS has also published new models to test the use of AI in healthcare, including through an outcome-aligned payment program under Medicare (ACCESS Model) and FDA enforcement discretion for pre-approved digital health tools (TEMPO Pilot). See our client alert here. In 2026, we will see HHS announce participants in the ACCESS Model and the development of a Tools Directory. We anticipate that HHS will continue to take deregulatory efforts and guidance that provides more flexibility to promote the use of AI-enabled technology. We also see the federal government continue to push for greater access to health data to support the development and use of AI in healthcare, including through enforcement of information blocking regulations. At the state level, we see a different picture. In 2025, many states passed new legislative requirements related to health AI. These include laws that regulate the use of AI in mental health, create safeguards for AI companions to address self-harm, require transparency for patient communications and for use of AI by clinicians, and require transparency and opt-out for automated decision-making technologies. See our previous alert here. In 2026, the pace of these state AI laws will likely be impacted by the recent AI Executive Order.
9. **Expect the Trump Administration and U.S. states to clash on AI regulations.** As discussed in our previous client alert, the Trump Administration issued an Executive Order (EO) on December 11, 2025, that seeks to establish "a minimally burdensome national standard" on AI (AI EO). Among other directives, the AI EO instructs the U.S. Department of Justice to sue states over unconstitutional AI regulations and for the U.S. Secretary of Commerce to publish an evaluation of "burdensome" state AI laws within 90 days for referral to the Administration. According to public statements by Trump Administration officials, including White House Special Advisor for AI and Crypto David Sacks who is assigned to play a critical role in the AI EO's implementation, laws in California, New York, Colorado, and Illinois are in the crosshairs. However, because the AI EO cannot automatically void state laws or make them unenforceable, AI laws in these states remain in full force unless and until they are amended, repealed, or struck down through appropriate legal or administrative processes.
10. **Be on the lookout for congressional action on AI.** The AI EO also instructs executive branch officials to draft a legislative recommendation for a uniform federal regulatory framework for AI that would preempt state laws, provided that the legislative recommendation not propose to preempt otherwise lawful state AI laws relating to child safety protections, AI compute and data center infrastructure, state government procurement and use of AI, and "other topics as shall be determined." On December 19, 2025, U.S. Senator Marsha Blackburn unveiled "The Republic Unifying Meritocratic Performance Advancing Machine Intelligence by Eliminating Regulatory Interstate Chaos Across American Industry" (or TRUMP AMERICA AI Act) that would "codify President Trump's executive order to create one rulebook for [AI] that protects children, creators, conservatives, and communities." Expect more congressional proposals on AI to follow in 2026.

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 announcements. For more information, please contact Maneesha Mithal, Jodi Daniel, Demian Ahn, Laura De Boel, Lidia Niecko-Najjum, Doo Lee, Hattie Watson, Joseph (Tony) Misher, or any member of Wilson Sonsini's Artificial Intelligence and Machine Learning, Data, Privacy, and Cybersecurity, and Digital Health practices.

---

[1] On December 29, 2025, xAI filed a legal challenge, arguing that the AB 2013 violates the U.S. Constitution's Takings Clause by forcing developers to relinquish (or at least greatly diminish) the value of their trade secrets without compensation and that the law forces compelled speech. The bill's requirements remain in effect as the litigation is ongoing.