HINSHAW

2026 AI Compliance: Upcoming Laws Every Organization Needs to Know

Trump's AI Executive Order, State AI Laws, Chatbot Disclosure Laws, and More

Privacy, Cyber & AI Decoded Alert | 6 min read
Aug 5, 2026

By: Cathy Mulrow-Peattie, *Elyssa Eisenberg

This edition of Hinshaw's *Privacy, Cyber, and AI Decoded* highlights several 2026-enacted AI laws as well as Executive Orders that organizations should consider in their compliance planning.

As we enjoy the last few weeks of summer by pulling out those straw hats and hitting the beach, the pool, or the lake, remember that maintaining AI and data compliance—similar to organizing a summer trip—requires planning and a strategic approach.

A Federal Change in Direction? Trump AI Executive Order: *Promoting Advanced AI Innovation and Security*

Signed: *June 2, 2026*

On June 2, President Trump signed an executive order establishing two new federal AI oversight mechanisms. The order does not impose direct compliance obligations on businesses but formalizes the government's role in the AI development cycle in ways that may affect companies relying on frontier models.

Key Provisions

- **Voluntary 30-day Pre-release Review:**
  - Developers of "covered frontier models" (a threshold to be set through a classified benchmarking process) may provide the federal government access to new models for up to 30 days before releasing them to trusted partners.

- **AI Cybersecurity Clearinghouse:**
  - The US Department of Treasury, the National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) must establish a clearinghouse to coordinate AI-assisted vulnerability scanning, validate findings, and manage patch distribution across critical infrastructure.
  - On July 14, the White House launched "Gold Eagle," the clearinghouse platform intended to help companies identify, share, and address software vulnerabilities using advanced AI models.
- **"Trusted Partners" Early Access:**
  - Developers are encouraged to collaborate with the government to identify partners who receive frontier model access ahead of general release.
- **Criminal Enforcement Priority:**
  - The US Attorney General (AG) is directed to prioritize enforcement of existing federal criminal statutes (Computer Fraud Abuse Act (CFAA), wire fraud, identity fraud) against anyone using AI to illegally access or damage computer systems or deploying AI agents to unlawfully access data for criminal purposes, in particular as it relates to cybercrimes.

Why it Matters

Although the order does not impose direct compliance obligations on most businesses, it signals a more hands-on approach to AI regulation, particularly regarding threats to national security and cybersecurity.

This executive order follows the Trump Administration's export control concerns regarding Mythos and Fable 5, which are concerned about putting powerful AI in the hands of threat actors, including nation-state actors. A testing approach was developed to protect the critical infrastructure.

The Nutmeg State and Connecticut Artificial Intelligence Responsibility and Transparency Act

Effective Dates: *October 1, 2026; October 1, 2027; July 1, 2027*

On May 27, Connecticut Governor Ned Lamont signed SB 5, also known as the Connecticut Artificial Intelligence Responsibility and Transparency Act (the Act), into law.

The Act takes a targeted approach to AI regulation, with key business-facing requirements for automated employment-related decision technologies (AEDT), subscription-based AI services, and generative AI transparency. The Act also directs the state to develop a plan for an AI regulatory sandbox program.

Key Provisions

- **AI in Employment Decisions:**
  - Beginning **October 1, 2027,** employers using AEDT must disclose when applicants or employees are interacting with such technologies and provide written notice before making an employment-related decision (such as hiring, promoting, disciplining, or discharging) using the tool.
  - The "plain language" notice must include the technology used, the technology's purpose, the nature of the decision, the name of the tool used, the categories and sources of personal data analyzed, how the data will be processed and assessed, and employer contact information.
  - The Act also provides that use of an AEDT is not a defense to discrimination claims, although evidence of anti-bias testing may be considered.
- **Subscription-based AI Services:**
  - Subscription-based providers offering AI technologies to Connecticut consumers must provide written notice of key subscription terms before entering into or renewing a subscription or collecting fees.
  - The disclosure must include material limitations on the AI technology and whether the provider may limit, reduce, or eliminate access to AI functionality. Consumers must affirmatively accept the disclosed terms before fees may be charged.
- **AI Regulatory Sandbox:**
  - The Act directs the Connecticut Commissioner of Economic and Community Development to develop a plan for an AI regulatory sandbox program that would allow approved applicants to temporarily test innovative AI products or services under reduced regulatory requirements.
  - This regulatory sandbox is similar to the ones enacted in Texas, Utah, and Delaware.

Enforcement

The Act is enforced exclusively by the attorney general under the state's unfair or deceptive trade practices statute. There is no private right of action.

Certain employment-technology violations occurring before **December 31, 2027,** are subject to a 60-day cure period.

Why it Matters

- Employers using AI in hiring, promotion, discipline, discharge, or other employment decisions should prepare for Connecticut's notice requirements before **October 1, 2027.**
- Companies offering AI tools through subscription models should review onboarding, renewal, and fee-collection processes to ensure required disclosures and affirmative acceptance mechanisms are in place.
- Companies using innovative AI solutions should take advantage of regulatory sandboxes to get prerelease regulatory insights.

The Centennial State's Changing Laws: Colorado's AI Act Revisions

***Effective Date**: January 1, 2027*

On May 14, Colorado Governor Jared Polis signed SB 26-189, revising the 2024 Colorado AI Act. The revised law, the Colorado Automated Decision-Making Technology Act (CADMA), replaces the original governance-heavy framework for "high-risk" AI systems with a narrower, disclosure-focused approach.

Scope

The Act applies to consequential decisions relating to employment, housing, lending, insurance, healthcare, education, and government benefits, where a covered ADMT materially influences the decision.

Key Provisions

- **Covered ADMT:**
  - The law applies to technology that processes personal data and uses computation to generate outputs, including predictions, recommendations, classifications, rankings, or scores, that are used to make, guide, or assist decisions concerning individuals. There is no exclusion for a human in the loop.
  - The tool becomes a "covered ADMT" when it materially influences a consequential decision.
- **Developer and Deployer Obligations:**
  - Developers must provide deployers with documentation describing the ADMT's intended uses, categories of personal data used in training data, known limitations and risks, and instructions for appropriate use and human review.

- Deployers must provide consumers with a pre-use notice before consumers use a covered ADMT and an additional notice within 30 days after an adverse outcome, which provides a plain-language explanation of the decision, the ADMT's role, and available consumer rights.
- Post-adverse outcome decisions are being further explored through the rulemaking process.

Enforcement

The Act is enforced exclusively by Colorado's Attorney General, with violations treated as deceptive trade practices. There is no private right of action. The Colorado Attorney General is required to issue post-adverse disclosure requirement rulemakings on or before January 1, 2027.

There is a 60-day cure period unless the violation was done knowingly or repeatedly. The right to cure sunsets **January 1, 2030.**

Why it Matters

Companies using or developing ADMTs doing business in Colorado in employment, insurance, lending, healthcare, housing, education, or government-benefit decisions should start the risk assessment process to understand whether those tools qualify as covered ADMTs.

Illinois Artificial Intelligence Safety Measures Act (Frontier Model Safety Law)

On July 6, following New York and California, Illinois became the third state to enact a frontier AI safety law, the Artificial Intelligence Safety Measures Act. (the AI Act).

This law imposes transparency, catastrophic-risk management, safety frameworks, and incident-reporting obligations on covered developers, with additional requirements applying to "large frontier developers."

The AI Act requires covered developers to assess and address potential catastrophic risks posed by frontier models and establish processes for responding to critical safety incidents.

Who is Covered?

- "**Frontier Model**" means a foundation model that was trained using a quantity of computing power greater than 10^26 integer or floating-point operations.
- "**Large Frontier Developer**" means a frontier developer that, together with its affiliates, collectively had annual gross revenues in excess of $500,000,000 in the preceding calendar year.

- Unlike California's SB 53 and New York's Responsible AI Safety and Education (RAISE) Act, Illinois is the first state to require large frontier developers to retain an independent third party to conduct annual audits of compliance with the AI Act's frontier AI framework requirements.
- **Beginning January 1, 2028,** large frontier developers also must implement, publish, and annually review a frontier AI framework describing how they identify, assess, and mitigate "catastrophic risks," including risks involving chemical, biological, radiological, or nuclear weapons, certain autonomous cyberattacks or criminal conduct, and loss of model control.

- **The AI Act takes effect January 1, 2027**, but the frontier AI framework, publication, and third-party audit obligations for large frontier developers do not begin until January 1, 2028, or 90 days after a developer first qualifies as a large frontier developer, whichever is later.
  - A separate governmental disclosure-statement filing requirement for large frontier developers operating a frontier model in Illinois takes effect earlier, on **January 1, 2027.**

Enforcement

The Illinois Attorney General's Office has exclusive authority to enforce the AI Act and bring civil penalty actions.

Frontier developers must report critical safety incidents within 72 hours of learning facts establishing a reasonable belief an incident occurred, or within 24 hours if the incident poses an imminent risk of death or serious physical injury.

Why it Matters

Third-party audit requirements and disclosures will allow deployers more insight into the catastrophic and cybersecurity risks of these large models.

Virginia Independent Verification Organization Framework Study (HB 797 / Chapter 425)

Virginia enacted HB 797, directing the Joint Commission on Technology and Science to study whether the Commonwealth should develop a framework for independent verification organizations that assess AI models or applications against standards designed to prevent personal injury and property damage.

The report, **due November 1,** must evaluate AI-related risks, measurable risk metrics, existing mitigation standards, approaches in other states, and the feasibility of licensing independent verification organizations.

Why it Matters

While the law does not impose current compliance obligations, it signals that Virginia may consider a future AI audit or certification regime, and other states could follow.

New Chatbot Laws

State legislatures have moved aggressively in 2026 to regulate AI-powered chatbots, with nearly 100 chatbot-specific bills introduced across 34 states and at the federal level, creating a rapidly expanding patchwork of compliance obligations for companies that develop or deploy conversational AI.

State Laws

Laws have already been enacted in the following states, with effective dates ranging from laws already in force to provisions taking effect as late as July 2027:

- California (SB 243)
- Colorado (HB 1263)
- Connecticut (SB 5)
- Georgia (SB 540)
- Idaho (SB 1297)
- Iowa (SF 2417)
- Maine (LD 1727)
- Nebraska (LB 525)
- New York (S 3008C)
- Oregon (SB 1546)
- Rhode Island (SB 2195)
- Tennessee (SB 1700)
- Washington (HB 2225)

Scope

While these laws share a common core of requiring AI disclosure, minor protections, and safety protocols, the definitions and compliance requirements diverge significantly across jurisdictions.

Key Compliance Requirements Include:

i. operators are required to disclose, at set intervals, that users are interacting with AI rather than a human;
ii. safety protocols preventing minors in particular from engaging in certain harmful or conversations;
iii. age verification; and
iv. prohibitions on the chatbot stating or implying that it is a licensed mental health professional.

Many of the laws have exemptions for routine business tools, including customer service bots, internal research tools, and narrow single-purpose utilities.

Why it Matters

Companies that use or develop these chatbots should understand the requirements of these laws in the states where they operate and establish a high-level compliance approach.

**We extend a huge thanks to our Hinshaw summer Legal Intern Elyssa Eisenberg for her contributions to this alert. Elyssa is not admitted to practice law.*

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Related Capabilities

Data Privacy, AI & Cybersecurity

Regulatory & Compliance

Website Data Privacy

Related Insights

Hot Topics in Data Privacy: Staying Cool and Compliant This Summer