Davis Polk

The AI regulatory and enforcement landscape: Key developments and trends

Presented by

Ben Rossen (Associate General Counsel, Policy & Regulation, OpenAI)

Jamie Haldin (Partner, Davis Polk)

David Feinstein (Counsel, Davis Polk)

May 2026

Davis Polk & Wardwell LLP

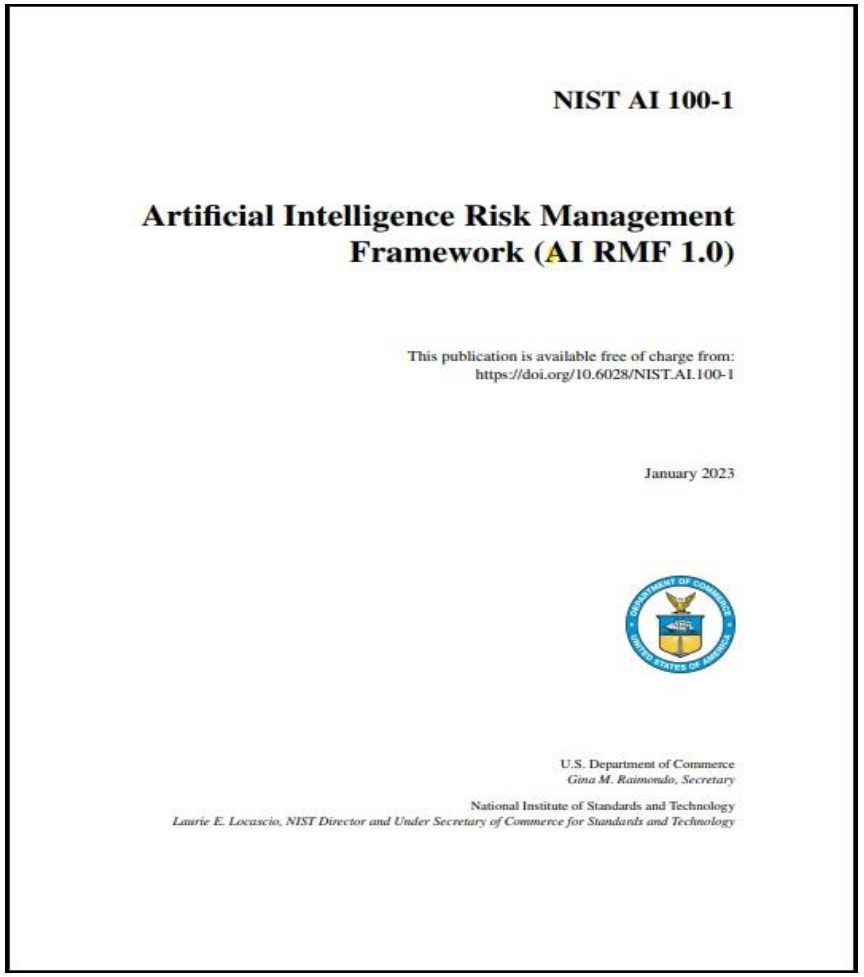
Agenda

Terminology

01

Terminology

AI system



NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AI.100-1

January 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

"An engineered or machine-based system that can, for a given set of human-defined objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments."

– Definition of "AI system" under NIST AI RMF (NIST AI 100-1)

– Adapted from OECD Recommendation on AI: 2019 (ISO/IEC 22989:2022)

Terminology

AI types/models

- Modern AI systems often learn from data or iterative feedback, rather relying solely on hard-coded rules.
  - **Prediction / Classification / Recommendation** ➡ **Predictive AI**
    - E.g., facial recognition, image classification, risk scoring
  - **Content Creation** ➡ **Generative AI (Gen AI)**
    - E.g., text, image, multimodal, video
- **Foundation models** can power a wide range of applications, often through APIs or embedded model access.
- A foundation model can power **many different applications**, generally through APIs. For example:
  - OpenAI models like the GPT-5 series power first-party products like ChatGPT and Codex.
  - Third-party developers can also integrate model provider APIs into their own software and services to power their own AI features and products (e.g., Harvey, Legora, CoCounsel / Westlaw AI).
- **Frontier models** are the most advanced and capable models, often defined by the amount of computing power used to train, modify, or fine-tune the model.
  - For example, California law defines frontier models as those trained with “a quantity of computing power greater than 10^26 integer or floating-point operations (‘FLOP’).”

Terminology

Developers/deployers

AI ecosystem

- **Developer**: An individual / entity that **develops or intentionally and substantially modifies** a "high-risk" AI system.
  - CO AI Act, Sec. 6-1-1701(1)(7)
- **Provider**: An individual / entity that develops an AI system or general purpose AI model and places it on the market or into service under its own name or trademark, whether for payment or free of charge.
  - EU AI Act, Ch. I Art. III

Deployer

- An individual / entity doing business in Colorado that deploys a high-risk AI system.
  - CO AI Act, Sec. 6-1-1701(1)(6)
- An individual / entity using an AI system under its authority, except where the AI system is used in the course of a personal nonprofessional activity.
  - EU AI Act, Ch. I Art. III

Terminology

AI stack

Chips and Cloud Infrastructure

AI Chips / Accelerators | Cloud Services | Data Centers | Power & Cooling

– *Examples:* Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud, CoreWeave, NVIDIA, AMD

Data and Model Layer

Training Data | Foundation Models | API Access

– *Examples:* OpenAI, Anthropic Claude, Google DeepMind, Meta, xAI, Cohere, Mistral, ElevenLabs, Black Forest Labs

Application and Deployment

Consumer Apps | Developer / Productivity Tools | Enterprise Software

– *Examples:* OpenAI ChatGPT & Codex, Anthropic Claude & Claude Code, Google Gemini, xAI Grok, Meta AI, Microsoft Copilot, Cursor, Harvey, Adobe Firefly, Salesforce Agentforce

Note: The layers are not mutually exclusive: many actors operate at multiple levels of the stack.

AI regulatory landscape

02

Trump Executive Order No. 14179

January 2025

45 47

PRESIDENTIAL ACTIONS

REMOVING BARRIERS TO AMERICAN LEADERSHIP IN ARTIFICIAL INTELLIGENCE

The White House | January 23, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The United States has long been at the forefront of artificial intelligence (AI) innovation, driven by the strength of our free markets, world-class research institutions, and entrepreneurial spirit. To maintain this leadership, we must develop AI systems that are free from ideological bias or engineered social agendas. With the right Government policies, we can solidify our position as the global leader in AI and secure a brighter future for all Americans.

This order revokes certain existing AI policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in artificial intelligence.

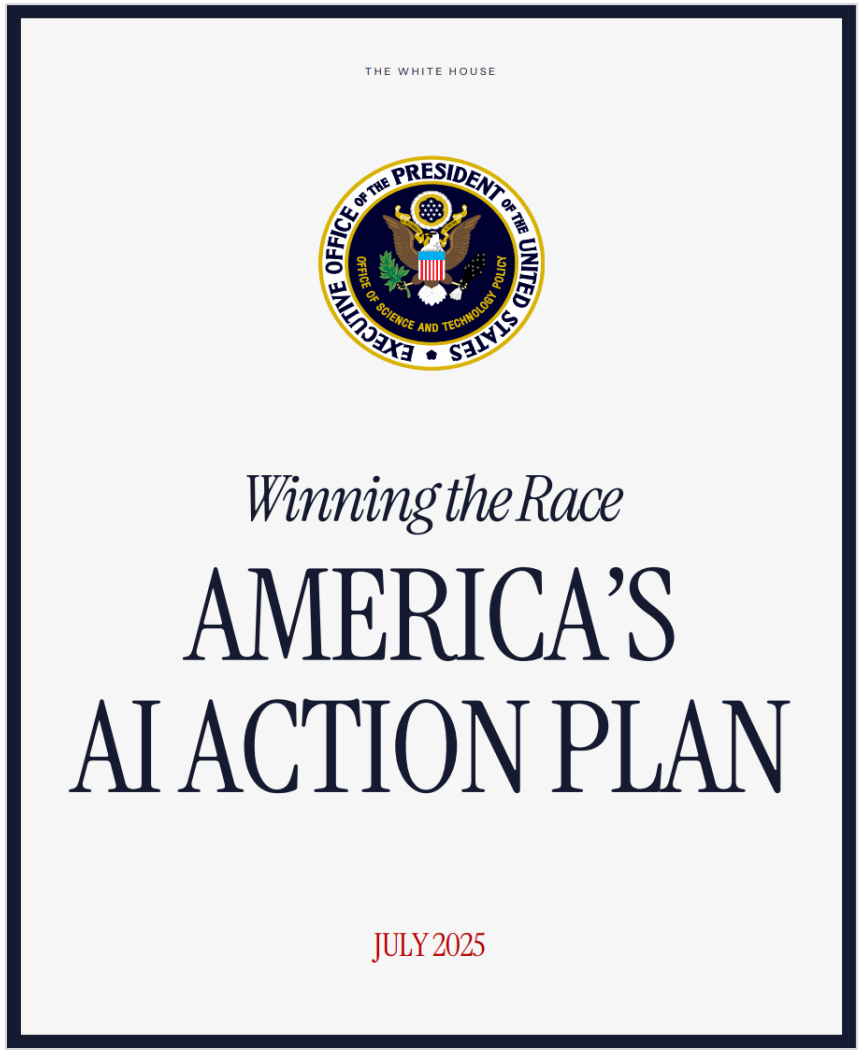
Sec. 2. Policy. It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security.

Key provisions

- Establishes U.S. policy to "**sustain and enhance America's global AI dominance" to promote human flourishing, economic competitiveness, and national security.**
- Directs development of **AI Action Plan** within 180 days.
- Directs federal agencies to suspend, revise or rescind policies and directives implemented under Biden-era EO 14110 "that act as barriers to American AI innovation."

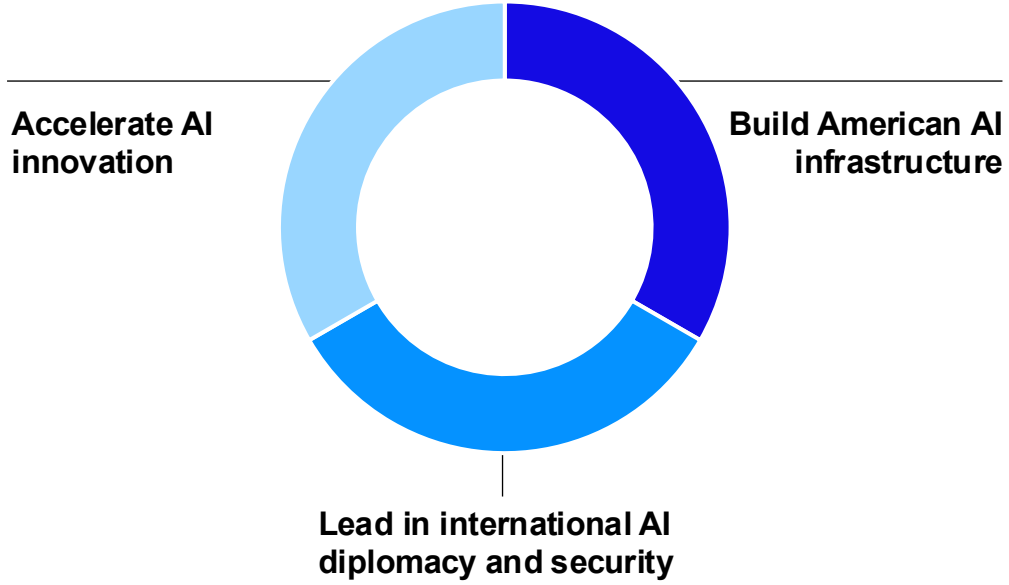
AI Action Plan

July 2025



"As our global competitors race to exploit these [transformative] technologies, **it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance.** To secure our future, we must harness the full power of American innovation."

– Pres. Donald J. Trump, America's AI Action Plan



AI Action Plan

Three Pillars

Accelerate AI Innovation

Foster innovation with whole-of-government policy recommendations including:

- **Reduction of regulations** that hinder AI development
- **Treatment of federal datasets** as national strategic AI assets
- **Enhance access** to computing power
- **Funding** of AI-related science, R&D, and supply chain
- **Promote** public-private sector collaboration

Build American AI Infrastructure

- **Accelerate development** of the infrastructure needed to sustain the American AI industry, including chip factories, data centers, and energy infrastructure
- **Training** the domestic workforce
- **Bolster the defensibility** of AI-infused critical infrastructure
  - Secure-by-design AI
  - Federal AI-specific incident response practices and frameworks

Lead in International AI Diplomacy and Security

- **Export American** AI-related technology
  - Chips and servers
  - Data center storage
  - Cloud services and networking
  - AI models
  - Security systems
- **Strengthen export controls** for advanced technology
- **Mitigate influence** of other nations in international AI governance bodies

Trump Executive Order No. 14365

December 2025

PRESIDENTIAL ACTIONS

ENSURING A NATIONAL POLICY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

Executive Orders | December 11, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. United States leadership in Artificial Intelligence (AI) will promote United States national and economic security and dominance across many domains. Pursuant to Executive Order 14179 of January 23, 2025 (Removing Barriers to American Leadership in Artificial Intelligence), I revoked my predecessor's attempt to paralyze this industry and directed my Administration to remove barriers to United States AI leadership. My Administration has already done tremendous work to advance that objective, including by updating existing Federal regulatory frameworks to remove barriers to and encourage adoption of AI applications across sectors. These efforts have already delivered tremendous benefits to the American people and led to trillions of dollars of investments across the country. But we remain in the earliest days of this technological revolution and are in a race with adversaries for supremacy within it.

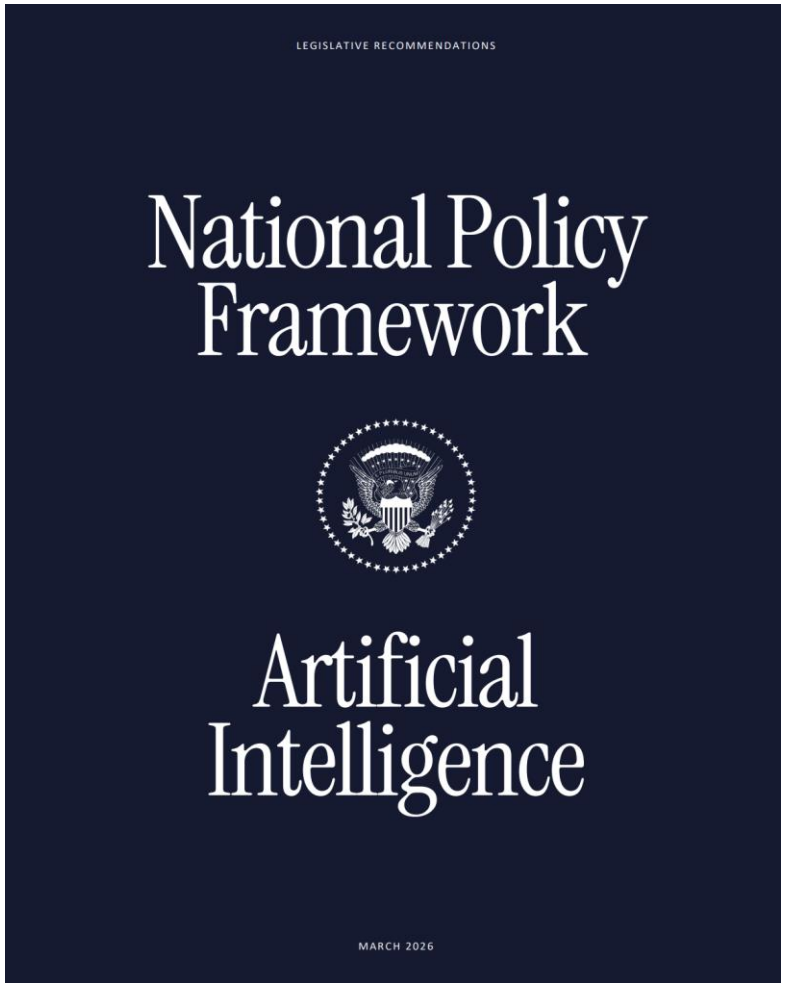
To win, United States AI companies must be free to innovate without cumbersome regulation. But excessive State regulation thwarts this imperative. First, State-by-State regulation by definition creates a patchwork of 50 different regulatory regimes that makes compliance more challenging, particularly for start-ups. Second, State laws are increasingly responsible for requiring entities to embed ideological bias within models. For example, a new Colorado law banning "algorithmic discrimination" may even force AI models to produce false results in order to avoid a "differential treatment or impact" on protected groups. Third, State laws sometimes impermissibly regulate beyond State borders, impinging on interstate commerce.

Key provisions

- Directs federal agencies to evaluate and challenge "onerous and excessive" state AI regulations:
  - DOJ to establish AI Litigation Task Force
  - Commerce to evaluate existing state AI laws
  - FTC to issue policy statement on UDAP and AI
  - FCC to initiate proceeding on possible federal reporting and disclosure standard
  - Agencies to assess whether discretionary federal funding may be conditioned on state AI-law posture.
- Legislative recommendations to preserve some state authority, including on:
  - Child safety
  - State government procurement and use of AI
  - Laws reducing barriers to AI compute and data infrastructure
- Directs development of a uniform federal AI policy framework.

National Policy Framework for Artificial Intelligence

March 2026



Key recommendations

- Federal preemption: Preempt state laws creating "undue burdens," describing AI as "inherently interstate"
- Child safety: parental controls, age verification methods, no preemption of state laws
- Community effects: electricity cost control, streamlined federal permitting, enforcement against scams and frauds
- IP: IP licensing frameworks for use of copyrighted content, limitations on use of digital likeness
- Censorship and free speech: prevent government "coercion" of providers
- Accelerating access and deployment: regulatory sandboxes, federal datasets for industry

Looking ahead: Focus on deepfakes and minors

Take It Down Act (TIDA)

- Enacted May 2025
- Targets nonconsensual intimate imagery, including AI-generated "digital forgeries"
- Requires covered platforms to maintain notice-and-removal process for covered content
- Platform compliance deadline: May 19, 2026
- FTC enforces platform notice-and-removal obligations

CHATBOT Act / GUARD ACT

- The CHATBOT Act (Senate Commerce Committee) is aimed at giving parents tools to manage minors' chatbot use and places limits on targeted advertising and manipulative design
- The GUARD Act (Senate Judiciary Committee) targets AI companion chatbots for minors, requires disclosures that users are interacting with AI rather than a human, and would impose criminal penalties for companies whose chatbots engage in sexually explicit conduct with minors or solicit minors to commit self-harm or violence

Looking ahead: Focus on frontier models

Frontier models with powerful cyber capabilities, such as Anthropic's Claude Mythos, may be prompting renewed federal attention to pre-release evaluation and national-security testing

- **Potential government review of AI models:** The administration is reportedly contemplating an executive order that would bring together tech executives and government officials to examine potential oversight procedures, including a review process for new AI models. No binding pre-release program has been announced.

- **CAISI pre-deployment evaluations:** This would be a step beyond the work the Center or AI Standards and Innovation ("CAISI") has done on pre-deployment evaluations and targeted research on AI models developed by frontier labs.
  - CAISI has continued its work under the Trump administration, securing agreements in May 2026 with Microsoft, xAI, and Google DeepMind to allow the government to vet their models for national security risks ahead of release—building on its existing collaborations with OpenAI and Anthropic.

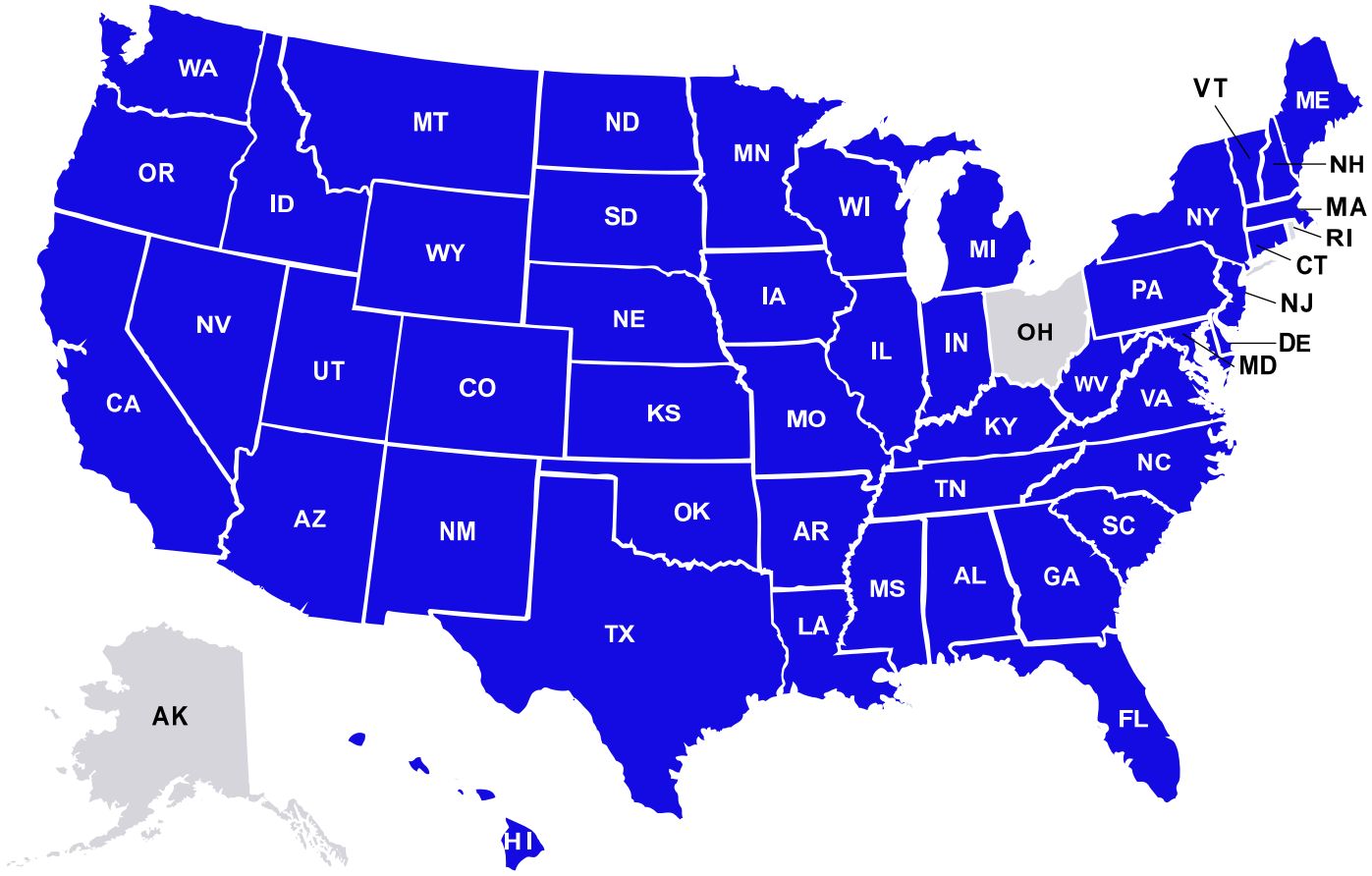
Colorado AI Act

Enacted in 2024, the Colorado AI Act is the leading state example of regulating "high-risk" AI systems used to make, or substantially assist in making, consequential decisions

- **Core focus:** Preventing algorithmic discrimination in consequential decisions involving areas such as employment, housing, lending, education, health care, insurance, and essential government services.
- **Who it regulates:** Both those who develop and deploy high-risk AI systems.
- **Key obligations**: Imposes a reasonable care standard; risk management programs; impact assessments; consumer notice, correction, adverse decision disclosures and appeal / human review rights.
- **Current status:** The law's effective date was delayed to June 30, 2026; enforcement is currently paused by a court stay while litigation proceeds and Colorado lawmakers consider revisions.

State AI regulatory landscape

Proliferation of targeted laws



At least one targeted AI law in effect

Comprehensive legislation

GenAI	**Consumer protection**
Chatbots	**Sector-specific**
Frontier models	**Algorithmic pricing**

Algorithmic discrimination

GenAI transparency, chatbots, etc.

States are increasingly targeting user-facing AI systems, particularly where users may believe they are interacting with a human or where minors users may be involved

- **Core focus:** Consumer disclosures, mental health chatbot safeguards, companion chatbot safety protocols, and protections for minors.
- **Examples:**
  - **UTAH AIPA:** GenAI disclosures in consumer and regulated-occupation interactions (effective May 2024).
  - **Utah HB 452:** Mental-health chatbot privacy, advertising, disclosure, and safety-policy rules (effective May 2025).
  - **California SB 243:** Companion chatbot disclosures, self-harm safety protocols, and minor-focused safeguards (effective Jan. 1, 2026; annual reporting obligations begin July 2027).
  - **New York AI Companion Models law:** AI companion safeguards, periodic AI interaction notices, and self-harm / crisis-intervention protocols (effective Nov. 2025).
- **Who they regulate:** Operators, suppliers, or providers of consumer-facing AI and chatbot services (depending on the statute).

Frontier models

California and New York have enacted model-layer AI laws focused on transparency, safety frameworks, and incident reporting for frontier models

- **Core focus:** Managing risks from high-capability foundation models, including critical safety incidents and catastrophic risk scenarios.
  - **California SB 52** requires large frontier developers to publish frontier AI frameworks; creates critical safety incident reporting and whistleblower protections, with enforcement by the California AG.
  - **New York RAISE Act** requires frontier model frameworks and critical safety incident reporting; additional transparency notices; establishes an AI model developer transparency and reporting oversight office.
- **Who they regulate:** These laws target frontier model developers, not ordinary application developers or downstream users.
- **Current status:**
  - *California SB 53:* signed in Sept. 2025; took effect Jan. 1, 2026
  - *New York RAISE Act:* signed in Dec. 2025, amended in March 2026; takes effect on Jan. 1, 2027.

AI-generated media and digital replicas

States are regulating AI-generated media and impersonation risks through consent, disclosure, and civil liability frameworks

- **Core focus:** Regulating digital replicas, requiring synthetic-performer and political-ad disclosures, and creating remedies for nonconsensual sexually explicit imagery.
  - **California examples:** AB 2602 and AB 1836 address digital replicas / likeness rights; AB 621 expands civil remedies for nonconsensual deepfake sexually explicit imagery; AB 2355 requires AI political-ad disclosures.
  - **New York examples:** S.8420-A/A.8887-B requires disclosure for AI-generated synthetic performers in advertisements; S.8391/A.8882 requires consent for certain postmortem commercial uses of name, image, or likeness.
- **Who they regulate:** Performers / contracting parties, advertisers, producers or creators of covered ads, and persons creating or facilitating covered synthetic content.

EU AI Act

Status

May 2024: EU AI Act enacted

- The EU AI Act was the first major broadly applicable AI-targeted statute.
- It uses a risk-based structure: prohibiting "unacceptable risks," and imposing compliance and documentation obligations on providers, importers, distributors and deployers of high-risk and limited risk AI systems.

April-August 2025: Missed deadlines

- The EC missed key deadlines for implementing required guidance, including:
  - Technical compliance standards (April 2025)
  - The General Purpose AI Code of Practice (May 2025)
  - Incident reporting guidance (August 2025)

November 2025: Digital Omnibus

- The EC proposes a Digital Omnibus package containing major amendments to the AI Act.
- Proposed changes include pushing effective dates into 2027-28, measures to reduce burdens on small- and mid-size entities, and adding a new ban on systems capable of generating intimate deepfakes.

Summer 2026: Formal vote

- The European Parliament and Council adopted the Digital Omnibus on AI in March 2026, and will begin negotiating a consolidated text, which may come as early as April or May.
- European stakeholders are racing to finalize and ratify a proposal in advance of the existing law's August 2, 2026 effective date for key compliance obligations.

AI enforcement landscape

03

AI enforcement landscape

FTC

Federal Trade Commission

April 2025: Workado

FTC order prohibiting Workado, LLC from advertising the accuracy of its AI detection products unless "it maintains competent and reliable evidence showing those products are as accurate as claimed[.]"

August 2025: Air AI

Settlement including permanent marketing ban for misrepresentations about its agentic "conversational AI" product (marketed as "Odin"), including that it could autonomously take action across 5,000+ apps.

August 2025: Click Profit

Settlement including permanent industry ban for an "AI-powered" e-commerce business that misrepresented potential to generate automated profits and misled consumers about brand partnerships.

September 2025: AI Chatbots

FTC issued 6(b) orders to seven companies for information about how they monitor and measure their AI chatbots' potential negative impacts on children.

AI enforcement landscape

FTC (cont.)

Rytr revisited

- In September 2024, announced enforcement actions against five companies, including Rytr, as part of Operation AI Comply
- Current FTC Chair Andrew Ferguson issued a dissenting statement at time of original order:
  - *"Treating as categorically illegal a generative AI tool merely because of the possibility that someone might use it for fraud is inconsistent with our precedents and common sense. And it threatens to turn honest innovators into lawbreakers and risks strangling a potentially revolutionary technology in its cradle."*

"[T]he specific facts set forth in the Complaint do not support a finding that Rytr violated Section 5 of the FTC Act. Since Rytr's AI-enabled services did not violate Section 5 of the FTC Act, the Order fails to provide any benefit to consumers and the public and accordingly unduly burdens AI innovation, in contravention of EO 14179 and America's AI Action Plan."

– FTC Order Reopening and Setting Aside Order (December 2025)

AI enforcement landscape

SEC

Securities and Exchange Commission

February 2025

- Announced that Cyber and Emerging Technologies Unit **(CETU)** will replace the Crypto Assets and Cyber Unit.
- Focus to include **fraud committed using emerging technologies, such as AI**
- CETU "*will root out those seeking to misuse innovation to harm investors and diminish confidence in new technologies[.]*"

April 2025

- Charged Albert Saniger (Nate Inc.) for allegedly misleading statements to investors regarding company's AI capabilities.
- Charged Ramil Palafox (PGI Global founder) for alleged fraud scheme regarding the development of an AI-powered crypto trading platform

February 2026

- Chairman Atkins discusses AI regulatory sandbox for SEC-regulated entities in Senate Banking Committee hearing:
  - *"I've been talking about an innovation exemption, to begin at the SEC, to allow entrepreneurs in a sandbox-like environment that's […] cabined, time-limited, transparent, flexible, and then focused on investor protection[.]"*

AI enforcement landscape

DOJ

Department of Justice

September 2024*

- USAO SDNY charged Michael Smith with wire fraud, wire fraud conspiracy, and money laundering conspiracy.
- Alleged scheme involved "stream[ing] songs created with artificial intelligence billions of times in order to steal royalties."
- Smith allegedly streamed his songs 600,000+ times/day via bot accounts.
- Smith pleaded guilty in March 2026.

April 2025

- USAO SDNY charged Albert Saniger for securities fraud and wire fraud.
- Alleged scheme involved making false and misleading claims to investors about company's use of proprietary AI.
- Defendant's company—Nate—marketed "single click" checkouts via AI but, in fact, used hundreds of contractors in the Philippines to manually complete purchases.

February 2026

- EDVA sentenced Ramil Palafox (PGI Global) to 20 years in prison following conviction for wire fraud and money laundering for AI-powered crypto trading platform scheme that defrauded over 90,000 investors worldwide.

April 2026

- USAO EDNY charged founder of iLearningEngines, Inc. with defrauding investors through claims about AI-driven business automation solutions.

AI enforcement landscape

DOJ (cont.)

Department of Justice

February 2025

- Chinese national indicted for downloading Google trade secrets on behalf of the PRC, including about chips, software and network interfaces.

August 2025

- Two Chinese nationals indicted for exporting AI chips without the required license or authorization

November 2025

- Two U.S. citizens and two Chinese nationals indicted for illegally exporting NVIDIA chips

December 2025

- "Operation Gatekeeper": Disrupts trafficking network in AI technology; two guilty pleas and seizure of $50 million of NVIDIA chips

March 2026

- USAO SDNY charged three with conspiring to divert significant quantities of servers with advanced AI capabilities to China in violation of U.S. export controls laws.
- Alleged to have fabricated documents, staged bogus equipment to pass audit inventories, and used a pass-through company to conceal their misconduct and true clientele list.

AI enforcement landscape

State AGs

State Attorneys General

AI advisories

- California, Connecticut, Massachusetts, New Jersey and Oregon have issued **AI advisories**
  - Emphasize applicability of existing state laws, such as consumer protection, anti-discrimination, employment, and data privacy laws.
  - Reinforce that companies are responsible for actions and decisions made by AI.

Increased coordination

- August 2025: 44 State AGs issue letter to 13 developers regarding AI chatbot harms for youth users.
- December 2025: 42 State AGs issue letter to AI industry leaders about legal risks regarding delusional chatbot outputs.
- January 2026: 35 State AGs issue letter to xAI regarding deepfake imagery.

AI enforcement landscape

State AGs (cont.)

State Attorneys General

Texas AG

August 2025: Announced investigation into AI chatbot platforms

California AG

January 2026: Announced formal investigation into xAI regarding deepfake imagery

Massachusetts AG

July 2025: Announced settlement with student loan company—Earnest Operations—over allegations of disparate harm to borrowers

Kentucky AG

January 2026: Announced suit against Character.AI alleging violations of state consumer protection laws over misrepresentations about safety and product design that resulted in deployment of "an inherently dangerous product to children"

Questions?