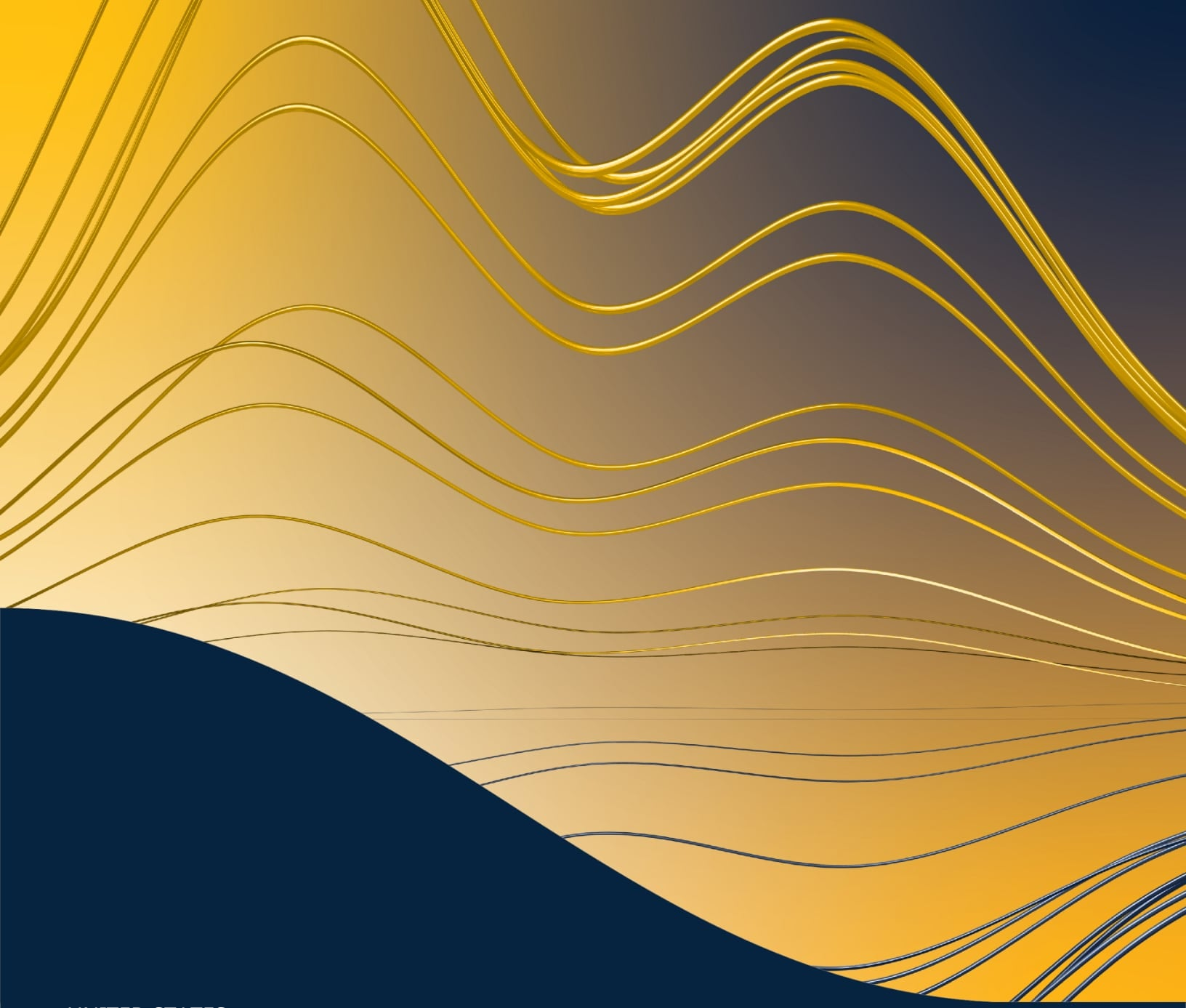


UNITED STATES

AI Laws of the World

DLA PIPER

Introduction

Artificial intelligence (AI) is rapidly transforming the way we work. As AI technology advances, governments are grappling with how to regulate its development to maximise benefits whilst mitigating risks.

Some jurisdictions have implemented AI-specific laws, whilst others are in the process of drafting regulations, and many rely on existing legal frameworks to address AI-related concerns.

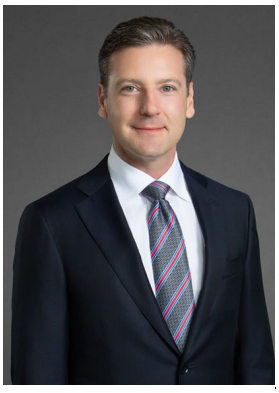
This guide provides an overview of AI laws and proposed regulations across 40+ countries. It highlights key legislative developments, including regulations, proposed bills and guidelines issued by governmental bodies.

As the global landscape of AI regulation evolves at an accelerating pace, our 2025 Q1 snapshot provides an insightful overview of these developments, as well as of the common thematic approaches of lawmakers and AI-focused organisations around the world.

Global key contacts

Gareth Stokes
Partner
Global Co-Chair, AI Practice
gareth.stokes@dlapiper.com
Full bio

Jeanne Dauzier
Partner
Global Co-Chair, AI Practice
jeanne.dauzier@dlapiper.com
Full bio



Danny Tobey
Partner
Global Co-Chair AI and Data Analytics
danny.tobey@us.dlapiper.com
Full bio

United States

LAST MODIFIED 10 MARCH 2026

Law / proposed law

AI laws and Proposed Laws

In the U.S., artificial intelligence (AI) is regulated at both the federal and state levels. While the U.S. lacks a unified federal AI law, the states have been active in modifying existing laws to account for AI and, in some cases, passing targeted AI-specific legislation.

This section outlines the major enacted laws at both federal and state levels, highlighting how states have taken the lead in adapting existing legal frameworks and introducing AI-specific laws in the absence of a comprehensive federal approach.

Federal AI legislation landscape

The federal regulatory landscape for AI remains limited in scope. Although a significant volume of AI-related legislation has been introduced in Congress, only one standalone statute intended to regulate the posting and distribution of AI-generated content has been enacted to date:

- Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act): Although the statute does not regulate AI systems directly, it requires online platforms to delete flagged non-consensual intimate imagery, including AI-generated deepfakes, within 48 hours. The law creates criminal penalties for distributing content and empowers the Federal Trade Commission (FTC) to enforce compliance.

Accordingly, federal policy is more defined by proposals than binding obligations, and most operational guidance continues to come from executive actions and agency-level enforcement.

Potential federal framework

On 11 December 2025, President Trump signed an Executive Order (EO) aimed at creating a national policy framework for AI to ensure American dominance in the field. The EO seeks to replace the existing patchwork of state laws—which the Trump

Administration views as burdensome and detrimental to innovation—with a unified standard.

To achieve this, the EO outlines a two-pronged strategy: challenging existing state AI laws in court and establishing a new federal regulatory framework that would preempt them. A new task force, led by the Attorney General (AG), will be created to raise legal challenges to state laws that are viewed as unconstitutional or otherwise conflicting with federal regulations. Additionally, the EO directs the Secretary of Commerce to evaluate state AI legislation. The proposed federal framework will focus on key areas such as child safety, censorship prevention, and copyright protection, while preempting conflicting state-level regulations.

State-level AI legislation landscape

The lack of comprehensive federal AI legislation has led to a proliferation of state-level laws and regulations, with many more bills working their way through state legislatures in 2026. Some of these laws establish frameworks and requirements that impact both public- and private-sector use of AI technologies.

In 2025, all 50 states, Puerto Rico, the Virgin Islands, and Washington, D.C., introduced AI-related legislation. According to the National Conference of State Legislatures, 38 states adopted or enacted approximately 100 AI-related measures. What materially changes in 2026 is enforceability: several major state AI laws take effect, significantly increasing the need for cross-state governance frameworks, comprehensive inventories, and demonstrable evidence of controls.

These laws and regulations impose transparency and disclosure obligations, prohibit deceptive uses of generative AI, and seek to mitigate algorithmic discrimination in certain domains. The following list includes the principal state laws shaping AI regulation in the U.S. and a few examples of some of the narrower AI-focused laws:

California

- California has enacted significant AI-related legislation, establishing new requirements for transparency, safety, and accountability across various AI applications. California's SB53, the Transparency in Frontier Artificial Intelligence Act (TFAIA), was signed into law on 29 September 2025, and took effect on 1 January 2026. It requires large frontier AI developers to publish transparency reports and annually update a public frontier AI safety framework describing how they assess and mitigate "catastrophic risk," secure unreleased model weights, and respond to critical safety incidents. Further, California's AB2013, Generative Artificial Intelligence: Training Data Transparency Act (TDTA) was signed into law 28 September 2024, and took effect 1 January 2026. The TDTA requires AI developers to publicly post a high-level summary of the datasets used to train generative AI systems or services made available to the public since January 2022, enumerating specific categories of required disclosures.
- During 2025, the California state legislature continued to pass many AI-related bills, most of which took effect on 1 January 2026. Signed into law on 13 October 2025, the California AI Transparency Act (AB853) mandates that developers of generative AI must embed "provenance data" into digital content to verify its authenticity and origin. (This law has staggered effective dates through 1 January 2028.) AB489,

signed into law on 11 October 2025, prohibits the use of AI to falsely imply that advice or services are being provided by a licensed healthcare professional. Further, enacted on 13 October 2025, SB243 imposes specific safety protocols on " companion bots," requiring them to prevent harmful conversations and regularly remind users that they are interacting with an AI. Other new laws, also enacted on 13 October 2025, create liability for services that enable deepfake pornography (AB621) and bar defendants from claiming an AI "autonomously caused the harm" in civil actions (AB316).

Colorado

- Colorado enacted the Consumer Protections for Interactions with AI Act (Colorado AI Act) in May 2024, and it is scheduled to take effect on 30 June 2026. It is recognized as the first comprehensive statute in the U.S. specifically targeting "high-risk" AI systems. The law requires developers and deployers of qualifying AI applications to exercise reasonable care in preventing algorithmic discrimination, mandates clear documentation of AI activities, and holds entities accountable for the outputs of their AI systems. By categorizing certain AI deployments as "high-risk, " the Colorado AI Act imposes heightened responsibilities in critical areas such as employment, healthcare, lending, housing, and government services.

Illinois

- In August 2025, Illinois enacted the Wellness and Oversight for Psychological Resources Act, which imposes significant restrictions on the use of AI in mental healthcare. The law, effective immediately, broadly prohibits any entity without a professional license from offering therapy services, a rule that explicitly includes services delivered via AI, and bars licensed healthcare professionals from delegating therapeutic decisions to AI systems.

Kentucky

- Signed and effective on 24 March 2025, Kentucky's AI Governance Act (SB4) establishes a comprehensive framework for AI use within state government. It calls for adoption of uniform AI policy standards and creates a governance committee to oversee ethical, transparent, and responsible AI use across state agencies. It includes provisions for human oversight, public disclosure, and protection of personal and business information.

Nevada

- On 5 June 2025, Nevada enacted AB406, which makes it a deceptive trade practice to misrepresent the capabilities of AI in mental healthcare. The law prohibits offering AI systems that are programmed to perform services that would constitute the practice of professional mental healthcare if done by a person. Furthermore, providers are barred from marketing or otherwise representing that their AI systems are capable of delivering such care. AB406 took effect on 1 July 2025.

New York

- New York enacted the Responsible AI Safety and Education (RAISE) Act on 19 December 2025, which establishes a comprehensive regulatory framework for

developers of large-scale "frontier" AI models.[1] Effective on 1 January 2027, this law requires large developers to implement and publicly disclose a detailed "safety and security protocol" designed to mitigate the risk of "critical harm," defined as events causing mass injury or over USD 1 billion in damages. It also requires developers to report any "safety incident" that demonstrates an increased risk of such harm to the state attorney general within 72 hours.

- Further, New York enacted a first-of-its-kind law requiring advertisers to disclose the use of AI-generated individuals in commercial advertising on 11 December 2025. The law mandates a conspicuous disclosure when a "synthetic performer"—a digitally created asset made with generative AI to resemble a human who is not an identifiable person—is featured in a visual or audiovisual advertisement. This rule is narrowly targeted at AI-generated actors and does not apply to audio-only ads, deepfakes of real performers, or AI enhancements of real performers. This law takes effect on 9 June 2026.

- Enacted on 11 December 2021, New York City's Local Law 144 regulates the use of " automated employment decision tools" (AEDTs) in hiring and promotion decisions. Effective since 5 July 2023, the law imposes three core obligations on employers: they must conduct an annual independent bias audit to assess whether the tool has a disparate impact on candidates based on race, ethnicity, or sex; they must post a summary of the audit results publicly on their websites; and they must provide notice to candidates that an AEDT is being used and of their right to request an alternative screening process.

Texas

- Texas enacted the Texas Responsible AI Governance Act (TRAIGA) on 22 June 2025, establishing foundational duties for state agencies, developers, and deployers of AI systems operating within Texas. The law went into effect on 1 January 2026, and prohibits state agencies from certain uses of social scoring and biometric data. Developers and deployers face prohibitions on the intentional misuse of AI for certain types of behavioral manipulation, unlawful discrimination, deepfakes, and infringement of constitutional rights. TRAIGA provides protections for organizations that follow recognized frameworks, such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework, as well as a 60-day cure period for violations, and the creation of a regulatory sandbox.

Utah

- Utah employed a relatively comprehensive approach to AI oversight by adopting, and making effective, the AI Policy Act (SB149) on 1 May 2024. This legislation requires professionals in regulated occupations – such as law, medicine, and financial services – to disclose their use of generative AI tools during high-risk interactions, such as when providing sensitive advice or handling personal data. Additionally, consumers must be informed if they explicitly inquire whether they are interacting with AI.

A handful of other U.S. states have considered and rejected broad AI laws. In addition, numerous other states and localities have enacted specific statutes or municipal ordinances that regulate discrete aspects of AI. The following list includes several such examples:

Maine

- Maine enacted "An Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence" (the Maine AI Chatbot Disclosure Act) on 12 June 2025. Effective 23 September 2025, the law establishes targeted disclosure requirements for AI-driven interactions. It generally prohibits businesses (and other persons) from using an AI chatbot – or similar text- or voice-based computer technology – in trade or commerce in a manner that may mislead or deceive a reasonable consumer into believing they are interacting with a human, unless the business provides a clear and conspicuous disclosure that the interaction involves AI.

Maryland

- Maryland enacted HB820 on 20 May 2025, regulating how health insurance plans and related entities may use AI in coverage and treatment decisions made in utilization management and review decisions. Effective 1 October 2025, the law requires covered entities to ensure that the AI tool's determinations are grounded in the enrollee's individual clinical information, do not replace the role of a health care provider, and are applied fairly and equitably without resulting in unfair discrimination.

Pennsylvania

- On 7 July 2025, Pennsylvania enacted Act 35 (formerly SB649) to address the malicious use of AI-generated deepfakes. Effective 5 September 2025, the law establishes criminal penalties for generating (or creating and distributing) a forged digital likeness with intent to defraud or injure, or with knowledge and intent to facilitate fraud or injury by another – including where the actor knows or reasonably should know the audio or visual at issue is forged.

Illinois

- Illinois enacted HB3773 on 9 August 2024, amending the Illinois Human Rights Act to regulate the use of AI in employment decisions, prohibiting discriminatory practices. Effective 1 January 2026, the law requires employers to provide notice to applicants and workers if they use AI for hiring, discipline, discharge, or other workplace-related purposes.

This continued surge in state legislative activity reflects a wide range of approaches and priorities – from establishing task forces to study AI's impact to imposing specific obligations on companies deploying AI systems. This dynamic landscape may underscore the growing value of state-level action in the absence of federal guidance, and organizations are encouraged to closely monitor both enacted laws and pending legislation in the jurisdictions in which they operate.

Regulatory guidance / voluntary codes

Over many years, and especially from 2022 onward, the U.S. federal government issued Presidential Executive Orders, voluntary frameworks and reports, and agency-level enforcement and guidance to set priorities and shape AI governance. States have also issued guidance and voluntary codes of conduct.

Presidential Executive Orders and Official Statements

In addition to the December 2025 Executive Order described above, the Trump Administration has also issued other orders and documents focusing on AI, the most significant of which are described below.

In January 2025, the Trump Administration issued EO 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence," which revoked an executive order from the Biden Administration that had focused in part on civil rights and algorithmic discrimination. The new EO called for the elimination or revision of prior AI-related policies deemed inconsistent with promoting innovation and leadership in the U.S. It emphasized the development of AI systems that are "free from ideological bias or engineered social agendas," and directed agencies to align their policies accordingly within 180 days.

In July 2025, the White House released "America's AI Action Plan" which establishes a strategic framework for achieving U.S. global dominance in AI. The plan identifies over 90 federal policy actions across three pillars: accelerating AI innovation through deregulation and support for open-source models, building American AI infrastructure including energy capacity and semiconductor manufacturing, and leading in international AI diplomacy while securing strategic advantages over adversaries. The plan emphasizes removing regulatory barriers that hinder private sector innovation, empowering American workers to benefit from AI opportunities, and ensuring AI systems reflect American values and free speech principles.

Voluntary AI-related frameworks

In parallel, voluntary frameworks continue to guide ethical and responsible AI development. Most notably:

- AI Bill of Rights (October 2022): Issued by the White House Office of Science and Technology Policy (OSTP) during the Biden Administration, the "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People" is a set of principles aimed at guiding ethical AI use and protecting the public from harmful AI practices. While not enforceable, its core principles have influenced corporate ethics policies and state-level legislation. The Trump Administration has moved away from the principles expressed therein.
- NIST AI Risk Management Framework (AI RMF 1.0) (January 2023): This voluntary and non-binding framework, released by the U.S. Department of Commerce's NIST, is designed to mitigate AI risks. Widely adopted by both private companies and government agencies as a best-practice guide, the Risk Management Framework (RMF) encourages organizations to assess and mitigate risks based on the context and potential impact of the AI system. Notably, the Trump Administration, through the White House's July 2025 AI Action Plan, recommends that NIST revise the AI RMF 1.0 to remove references to certain topics including misinformation, DEI, and climate change.
- NIST Generative AI Profile (July 2024): NIST released this voluntary guide as a supplement to the RMF. It tailors the RMF's core principles – "map," "measure," " manage," and "govern" – to the risks of generative AI, such as misinformation, deepfakes, and IP concerns. It offers over 400 recommended actions across the

generative AI lifecycle and emphasizes stakeholder engagement, transparency, and responsible deployment.

- NIST AI 100-4 (November 2024): In furtherance of the Biden Administration's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, NIST issued the report "Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency" as a technical overview of methods to increase transparency and reduce the risks associated with AI-generated content. It provides foundational guidance for developing future standards and applies its concepts to the AI RMF. It aims to improve trust in digital media by examining technical approaches for content authentication, provenance tracking, synthetic content detection, and the prevention of harmful AI-generated materials.
- NIST Cybersecurity Framework AI Profile (December 2025): Issued as a preliminary draft, NIST's Cyber AI Profile provides guidelines for managing cybersecurity risks associated with AI systems and for leveraging AI to improve cybersecurity capabilities. It applies the core functions of the NIST Cybersecurity Framework (CSF) 2.0 to help organizations strategically adopt AI while addressing emerging cybersecurity risks. It organizes its guidance into three focus areas: securing AI components, using AI for cyber defense, and thwarting AI-enabled attacks.
- NIST Possible Approach for Evaluating AI Standards Development (January 2026): NIST issued the grant contractor report, "A Possible Approach for Evaluating AI Standards Development," as a conceptual paper proposing a framework to measure the effectiveness and impact of AI standards. While the report presents a non-prescriptive approach intended to foster discussion, it introduces a formal " theory of change" model to help stakeholders evaluate how AI standards achieve goals such as promoting innovation and public trust. It outlines a process for identifying the inputs, activities, outputs, and outcomes of standards development and measuring their impact against a "counterfactual," or what would have happened in the absence of the standard.

Federal agency action

Several federal agencies are also leveraging their statutory authorities to address emerging risks, ensure compliance, and hold organizations accountable for the misuse or misrepresentation of AI technologies. Enforcement actions by agencies such as the FTC, Securities and Exchange Commission (SEC), Department of Justice (DOJ), Food and Drug Administration (FDA), and Department of Health & Human Services (HHS) have aimed to help shape responsible AI practices. These actions span a range of issues – from consumer protection and investor transparency to employment discrimination and medical device safety. The following outlines the roles of some of the key federal agencies in AI oversight and highlights their regulatory focus areas.

FTC

The FTC's mission is to protect consumers and promote fair competition. The agency has targeted deceptive practices and misleading claims about AI – often referred to as " AI washing." The agency has now brought numerous enforcement actions against companies that exaggerate the capabilities of their AI systems or falsely market

products as AI-powered to gain consumer trust. The FTC has also focused its enforcement on privacy issues with AI systems and the misuse of generative AI for scams and fake reviews. In addition, the agency has explored antitrust issues relating to algorithmic pricing and the market for cloud computing.

SEC

The SEC's regulatory focus on AI centers around ensuring transparency, managing conflicts of interest, and protecting investors. It requires firms to clearly disclose how AI is used, particularly when it influences investment decisions or client interactions, to police false or misleading AI statements to investors or clients. The SEC addresses organizational claims about AI capabilities that are misleading to investors, and requires compliance with existing securities laws, applying a technology-neutral, risk-based approach to oversight. Like the FTC, the SEC has been bringing enforcement actions relating to "AI washing."

DOJ

The DOJ enforces a broad array of federal criminal and civil laws, intensifying its focus on misconduct related to AI, particularly "AI washing." In April 2025, the DOJ, working in parallel with the SEC, brought securities and wire fraud charges against the former CEO of a technology startup for allegedly defrauding investors of over USD 42 million by falsely claiming his company used advanced AI when its services were actually being performed manually. This enforcement posture underscores the significance of the DOJ 's late 2024 guidance on how companies should manage risks associated with AI and other emerging technologies. In certain cases, when considering punishment for criminal wrongdoing, federal prosecutors would use this guidance in considering the efficacy of a company's relevant compliance program. The agency has also brought law enforcement actions involving AI-related mistakes and misuse, sometimes working with agencies like the SEC. Given that DOJ also enforces civil rights laws, it has signaled in the past that AI systems used in areas like housing, employment, and lending must comply with anti-discrimination statutes.

FDA

The FDA plays a central role in regulating AI in both the medical device and drug development contexts, proactively establishing regulatory infrastructure to ensure compliance and safety. In January 2025, the agency released a draft guidance, " Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products," which introduces a risk-based credibility assessment framework for AI models used in this context. It outlines a seven-step process for assessing AI model credibility, discusses challenges such as data quality and algorithmic bias, and highlights the need for life cycle maintenance of AI models to ensure their continued reliability. The FDA has also adopted a separate risk-based framework for the regulation of Software as a Medical Device (SaMD), focusing on the intended use of the software and the potential impact on patient health, which includes evaluating the software's clinical functionality, reliability, and performance. The FDA strongly encourages sponsors to engage with the agency early in the development process to discuss the use of AI in the context of drug development.

HHS

The HHS, through its Office for Civil Rights (OCR), plays a central role in governing the use of AI and other advanced technologies that implicate protected health information. OCR administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules, and has increasingly framed these authorities to account for evolving technological and cybersecurity risks. In particular, OCR has moved to modernize HIPAA Security Rule requirements to reflect changes in the digital health ecosystem, explicitly citing the growing sophistication of cyber threats, the expanded use of automated and data-intensive systems, and the need for stronger safeguards around electronic protected health information.

Appointed supervisory authority

The U.S. has no centralized federal regulator specifically dedicated to AI. Instead, federal oversight of AI remains distributed across multiple agencies and advisory bodies. For example, the Trump Administration's December 2025 EO pushed a national policy framework and strategies to challenge state AI laws but did not suggest the need for a new regulator to oversee such efforts; it relies instead on existing agencies and officials.

Similarly, most states do not charge a single agency with oversight or responsibility for AI-related matters. A growing number of states have adopted AI-specific statutes that embed regulatory or enforcement authority in existing agencies or frameworks, such as consumer protection, and that sometimes designate specialized oversight bodies in particular market sectors.

For example, Colorado's AG is tasked with regulatory and enforcement responsibilities under the Colorado AI Act, while Utah has designated oversight through its Department of Commerce and an emerging Office of AI Policy. New York's RAISE Act will create a new agency, within a larger, existing one, to implement that law. At the local level, New York City's Local Law 144 assigns enforcement to NYC's Department of Consumer and Worker Protection (DCWP).

In other states, AGs are actively leveraging existing consumer protection, privacy, and anti-discrimination laws to investigate and enforce against AI-related harms. In addition to engaging AGs, several states have empowered consumer protection agencies or other regulatory bodies to oversee AI-related compliance, resulting in a decentralized enforcement landscape where responsibilities vary by jurisdiction.

Definitions

In the U.S., the definition of AI varies across jurisdictions and legal frameworks.

At the federal level, definitions of AI have appeared in several laws, including the National AI Initiative Act, reflected in 15 U.S.C. § 9401, which defines AI as follows:

> *"(3) ARTIFICIAL INTELLIGENCE – The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:*

> *(A) perceive real and virtual environments;*
>
> *(B) abstract such perceptions into models through analysis in an automated manner; and*
>
> *(C) use model inference to formulate options for information or action."*

State laws have also used different definitions of AI. Below are two variants.

Colorado's AI Act does not provide a standalone definition of AI, but rather regulates AI systems as:

> *"Any machine-based system that, for any explicit or implicit objective, infers from the inputs the system received how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments." (C.R.S. § 6-1-1701(2))*

Utah's AI Policy Act carves out Generative AI as:

> *"An artificial system that: (i) is trained on data; (ii) interacts with a person using text, audio, or visual communication; and (iii) generates nonscripted outputs similar to outputs created by a human, with limited or no human oversight." (Utah Code § 13-2-12(1)(a))*

Prohibited activities

As noted, the U.S. has not enacted a comprehensive federal law that explicitly outlines prohibited uses of AI. However, certain AI-related activities are restricted or prohibited under existing laws and proposed legislation. Enforcement actions have been taken under broader legal authorities such as consumer protection, civil rights, and securities laws.

At the federal level, two of the many proposed bills aiming to prohibit specific AI practices are:

- The Preventing Algorithmic Collusion Act (2025), which would ban the use of pricing algorithms – including those powered by AI – to incorporate nonpublic competitor data to facilitate price-fixing
- The Transparency and Responsibility for Artificial Intelligence Networks Act (TRAIN Act) (2025), which would create an administrative subpoena process allowing copyright owners to compel AI developers to disclose copies of, or records sufficient to identify, copyrighted works used to train generative artificial intelligence models

While these bills have not become law, federal agencies have used existing statutes that prohibit deceptive or harmful AI practices. For example:

- The FTC has taken enforcement action against companies for "AI washing" (misleading claims about AI capabilities) and is studying the business practices of companies that offer companion chatbots, focusing on their effect on children
- The SEC has charged firms for misrepresenting the role of AI in investment strategies
- The DOJ has pursued criminal charges in cases involving fraudulent claims about AI functionality

At the state level, some jurisdictions have enacted laws that explicitly prohibit certain AI uses, such as:

- Colorado's AI Act, which prohibits the deployment of high-risk AI systems without reasonable safeguards to prevent algorithmic discrimination
- Utah's AI Policy Act, which prohibits the undisclosed use of generative AI in regulated occupations (*e.g.,* legal, medical), requires clear disclosure when AI is used in consumer interactions, and holds individuals liable for AI-driven misconduct under state consumer protection laws
- New York City's Local Law 144, which prohibits the use of automated employment decision tools without prior bias audits and candidate notification
- California and Illinois, which have passed laws restricting the unauthorized use of AI-generated digital replicas and require transparency in political advertising

Overall, while the U.S. lacks a unified list of federally prohibited AI activities, a growing patchwork of federal enforcement actions and state-level statutes is continuing to define the boundaries of acceptable AI use.

High-risk AI

Unlike in the EU, the risk categorization of AI technologies in the U.S. is not defined by a single, harmonized legislative or regulatory taxonomy. Whether a specific AI technology or use is considered "high-risk" will depend on, and will matter only if, jurisdiction-specific laws or rules include a relevant definition. Currently in the U.S., the Colorado AI Act is the only legislation that adopts a risk stratification system that categorizes certain uses of AI as "high-risk."

The Colorado AI Act defines "high-risk" AI systems as those that make, or significantly contribute to making, a "consequential decision." Under the Act, a consequential decision has a material legal or similarly significant effect on the provision, denial, cost, or terms of:

- Education enrollment or opportunity
- Employment or an employment opportunity
- A financial or lending service
- An essential government service
- Healthcare services
- Housing
- Insurance, or
- Legal services.

The definition excludes AI systems intended to perform a narrow procedural task or detect deviations in decision-making patterns. These systems are not intended to replace or influence a previously completed human assessment without human review.

Controls on generative AI

As the U.S. does not have a comprehensive federal law regulating generative AI, controls on generative AI are emerging through a combination of enforcement actions, state and local legislation, and agency rules or guidance.

At the federal level, several agencies, including the FTC and SEC, have taken enforcement actions against deceptive claims about AI. The FTC will be enforcing the TAKE IT DOWN Act, which covers certain types of deepfakes, and has issued rules about impersonation scams and fake reviews that would cover the use of generative AI tools.

At the state level, several jurisdictions have enacted targeted controls on generative AI. These laws include transparency obligations on AI developers, prohibitions on AI-generated deepfakes, disclosure requirements for consumer-bot interactions, and restrictions on chatbot use for mental health or companionship, among other things. Three examples are:

- California's Generative AI Training Data Transparency Act, which requires disclosure of high-level details about the training data used in generative AI systems

- Colorado's AI Act, which includes provisions requiring developers and deployers of high-risk AI systems, including generative models, to exercise reasonable care to prevent algorithmic discrimination
- Utah's AI Policy Act, which prohibits the undisclosed use of generative AI in regulated occupations and mandates clear disclosure when AI is used in consumer interactions

Enforcement / fines

Federal and state agencies can vary widely in how they enforce AI-related laws – not only because the laws themselves differ, but also due to the distinct enforcement powers that each agency holds.

For example, the DOJ and SEC jointly charged the founder of an AI startup with securities and wire fraud involving false claims about AI capabilities. Each agency sought several forms of relief, with the DOJ seeking a prison sentence and the SEC seeking civil fines.

The FTC's cases involving deceptive marketing of AI tools have resulted in injunctions and sometimes monetary payments.

At the state level, enforcement is similarly fragmented, with available relief dependent on the agencies and laws involved. For example, Colorado and Utah have enacted AI-specific laws that include statutory penalties:

- Colorado's AI Act authorizes the AG to bring actions for violations as unfair or deceptive trade practices, with penalties aligned with the Colorado Consumer Protection Act
- Utah's AI Policy Act imposes fines of up to USD 2,500 per incident and USD 5,000 per violation for undisclosed or unlawful use of generative AI in regulated occupations

User transparency

In the context of AI, transparency may involve different types of disclosures, such as the use of a machine learning tool to make consequential decisions about consumers or the use of a chatbot to interact with consumers. The U.S. does not currently have a federal law that specifically mandates transparency in AI systems. Some laws of general applicability, like broad consumer protection laws, may require disclosures about AI to avoid consumer deception. On the state and local level, however, a patchwork of laws has developed requiring transparency in different situations. For example:

- California's Generative AI: Training Data Transparency Act mandates disclosure of high-level details about the training data used in generative AI systems
- California's TFAIA requires large "frontier" AI developers to publish transparency reports and annually update a public frontier AI safety framework describing how they assess and mitigate "catastrophic risk," secure unreleased model weights, and respond to critical safety incidents

- Colorado's AI Act requires developers and deployers of high-risk AI systems to maintain documentation that demonstrates reasonable care in preventing algorithmic discrimination
- Utah's AI Policy Act mandates verbal or written disclosure when consumers interact with generative AI in regulated service contexts
- New York's RAISE Act requires large developers to implement and publicly disclose a "safety and security protocol" and report any "safety incident" to mitigate risk
- New York City's Local Law 144 requires employers to notify candidates when automated employment decision tools are used, and to publish the results of bias audits

These efforts may reflect a growing consensus that transparency is key to responsible AI deployment, particularly in applications such as employment, healthcare, and consumer services. However, the scope and enforcement of transparency obligations vary significantly across jurisdictions, contributing to a fragmented compliance landscape.

Fairness / unlawful bias

As with transparency, there is no federal law in the U.S. that specifically addresses fairness, bias, or other forms of algorithmic discrimination in AI systems. Under the Biden Administration, federal agencies sought to address these issues by applying existing civil rights, employment, and consumer protection laws to AI use cases. However, this activity has almost entirely ended, and agency-issued guidance on these subjects has in some cases been removed from public websites. Meanwhile, however, several states have enacted or proposed legislation to directly address algorithmic discrimination. For example:

- California's Fair Employment and Housing Act applies to employers' use of "[AI], algorithms, and other automated-decision systems" in employment decisions
- Colorado's AI Act prohibits the deployment of high-risk AI systems without reasonable safeguards to prevent algorithmic discrimination, with enforcement led by the AG
- Illinois has enacted workplace AI legislation that prohibits the use of AI in hiring or employment decisions that could result in discrimination
- New Jersey issued guidance clarifying that the New Jersey Law Against Discrimination (LAD) applies to "algorithmic discrimination" resulting from the use of AI and other decision-making tools, including in employment
- New York City's Local Law 144 requires annual bias audits for automated employment decision tools and mandates candidate notification

These state and local efforts, combined with prior federal activity, may reflect a growing – though not entirely shared – belief that AI systems can perpetuate or amplify existing societal biases, and that legal frameworks are evolving to ensure fairness, particularly in domains like employment, housing, and healthcare.

Human oversight

Human oversight of AI systems is not federally mandated in the U.S., but some states have passed related laws, particularly for high-risk applications.

At the federal level, the NIST AI RMF encourages organizations to implement human oversight mechanisms throughout the AI lifecycle. It defines oversight as the ability for humans to understand, monitor, and, when necessary, intervene in AI system operations. While not legally binding, the framework is widely adopted across industries and referenced in agency guidance.

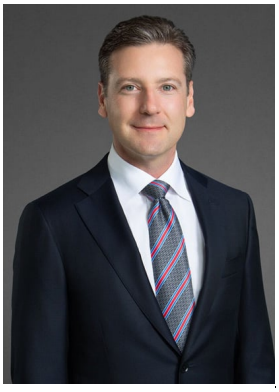
Since the Biden Administration, some federal enforcement agencies, such as the FTC and SEC, have continued to stress the value of human accountability, particularly in cases where AI is used to make decisions that affect consumers or investors. However, these expectations are grounded in broader legal principles, rather than AI-specific statutes.

At the state level, human oversight is more explicitly addressed in certain laws, such as:

- Colorado's AI Act, which requires deployers of high-risk AI systems to implement appropriate levels of human oversight to ensure the system operates as intended and does not result in algorithmic discrimination
- California's Physicians Make Decisions Act, which prohibits healthcare coverage denials made on the sole basis of an AI or algorithmic tool
- New York City's Local Law 144, which mandates that employers using automated employment decision tools conduct bias audits and provide human-readable explanations of how such tools may influence hiring decisions

These developments reflect a growing belief that human oversight may be a key to ensuring accountability, safety, and fairness in AI use.

Key contacts



Danny Tobey
Partner
Global Co-Chair AI and Data Analytics
DLA Piper
danny.tobey@us.dlapiper.com
View bio

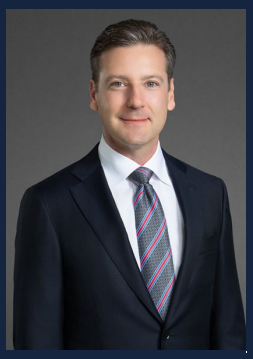
Ashley Carr
Partner
DLA Piper
ashley.carr@us.dlapiper.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:

Gareth Stokes
Partner
Global Co-Chair, AI Practice
gareth.stokes@dlapiper.com
Full bio

Jeanne Dauzier
Partner
Global Co-Chair, AI Practice
jeanne.dauzier@dlapiper.com
Full bio



Danny Tobey
Partner
Global Co-Chair AI and Data Analytics
danny.tobey@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com

This publication is for general information only. The information presented is not legal advice, and your use of it does not create a lawyer-client relationship. All legal matters are unique and any prior results described in this publication do not guarantee a similar outcome in future matters. DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information, please refer to dlapiper.com. Attorney Advertising. Copyright © 2026 DLA Piper LLP (US). All rights reserved.