CURRENT STATE & FUTURE TRENDS IN AI POLICY IN THE UNITED STATES

Prepared for:

The Center for Juris-Informatics - Japan

Author:

Merve Hickok

Founder, Alethicist.org

President, Center for AI and Digital Policy

January 2026

Contents

Introduction

AI policy changes and trends in the United States have significant impact on both domestic organizations which develop and make available their AI products within the U.S., and the foreign companies interested in entering or expanding their businesses in this jurisdiction. However, this is an area with rapid development. Technology moves very fast, along with the use cases and associated risks. The policy and governance responses follow these developments.

This report is commissioned by the Center for Juris-Informatics (Tokyo – Japan), with an objective is to provide an analysis of the current state and future trends of AI-related legislation, regulatory actions, and litigations in the U.S. to support Japanese companies in their decision-making.[1] Specifically, the report covers the following sections as it relates to the U.S.:

- Sources of AI policymaking
- An overview of the current state and future trends of AI-related legislation
- Trends and forecasts regarding litigation of AI products in the U.S.
- Key legal* considerations for Japanese companies exporting AI products to the U.S. *(*focused on executive orders and US AI Action Plan)*[2]
- Comparative analysis of state-level AI legislation across representative states (California, Colorado, Utah, Texas and New York)

Executive Summary

1. **AI policymaking landscape in the U.S. is complex.** Unlike countries with centralized governance structures, the U.S. system distributes authority among the three branches of federal government, and those of the state government, each approaching AI through their priorities and needs. For businesses intending to do business in different states, or directly with the federal government, it is critical to understand this mix of hard law and soft law expectations even without comprehensive AI legislation.

2. **Executive branch advances an agenda of AI dominance.** The current Administration has prioritized maintaining American leadership in AI development through a deregulatory

[1] The Center for Juris-Informatics. https://ds.rois.ac.jp/en_center7/

[2] Disclaimer: Nothing in this report is intended as legal advice, and should not be treated as such. The report is intended to provide a broad overview of the U.S. institutions, laws, and policies but is not intended to provide legal advice.

approach rather than precautionary governance. This agenda is mostly manifested in executive actions. Main policy directions are to reduce time and effort for AI infrastructure build, resist precautionary safety requirements, and focus federal resources on competing with China. The Administration uses industrial policy, national security tools, and direct engagement with the major AI companies towards its goal of domination in both global competition and technological advancement. This philosophy reflects a belief that regulation will drive innovation offshore and that market forces, combined with targeted enforcement of existing laws, provide sufficient safeguards. The approach has created tension with more regulatory-minded states and advocacy groups who argue that unfettered development poses risks to civil liberties, labor markets, and democratic institutions.

3. **Congress continues to work in bipartisan way in AI issues.** Despite deep partisan divisions on many issues, Congress continues to demonstrate areas of consensus on AI policy, particularly around national security concerns, children's safety, deepfakes, research investment, and the need for some form of regulatory clarity. Bipartisan coalitions have formed around legislation addressing AI's use in critical infrastructure, protecting children online, requiring transparency in government AI systems, and funding computational resources for academic researchers. Both parties recognize that regulatory uncertainty harms American competitiveness and that some baseline standards serve national interests. Public concerns about AI's impact continue to rise, as reflected in public sentiment surveys. Congress is likely to continue incremental progress on narrow issues rather than sweeping and comprehensive legislation.

4. **State-level AI legislation is active.** States have introduced hundreds of bills addressing algorithmic accountability, automated decision-making, and AI-specific consumer protections. This activity reflects both frustration with federal inaction and the traditional role of states in consumer protection and professional regulation. California, Colorado, New York, Utah and Texas have been particularly proactive, passing legislation that imposes impact assessments, transparency requirements, and anti-discrimination provisions on high-risk AI systems. States are also regulating specific applications such as AI-generated recommendations for professional advice, and the use of automated hiring tools, where they perceive immediate harms to their constituents. This experimentation provides valuable data about regulatory approaches and responds to local concerns. Some initial state laws (Illinois' biometric privacy, California's transparency disclosure, or New York's algorithmic pricing laws) hold the potential to become blueprints across multiple states.

5. **There is a division in AI policy between Federal vs State level.** A significant tension has emerged between the Administration's efforts to control most of AI policy, and the state attempts to fill perceived regulatory gaps, creating jurisdictional conflicts that may ultimately require judicial resolution. The Administration signaled its disfavor of state requirements, suggesting that AI governance should remain primarily a federal concern potentially protected by federal commerce clause. States counter that they have traditional authority over consumer protection, employment, and other areas where AI systems cause localized harms, and that federal inaction necessitates state intervention.

6. **Copyright questions remain mostly unresolved.** The intersection of AI and intellectual property law presents profound unresolved questions that courts and policymakers are trying to address. Central controversies include whether training AI models on copyrighted works constitute fair use, who owns the copyright to AI-generated content, and whether existing copyright frameworks adequately protect human creators from AI-enabled displacement. Multiple lawsuits from authors, artists, and publishers against AI companies are working their way through federal courts, with potentially industry-defining implications depending on whether judges view training as transformative use or as unauthorized reproduction. Congress has held hearings but has not advanced legislation.

7. **Regulatory agencies will continue enforcement of existing laws applied to AI.** Federal agencies had previously announced their intent to apply existing statutory authorities to AI systems, viewing them as simply new tools subject to longstanding rules. These include rules on deceptive or unfair business practices (FTC), discriminatory employment practices (EEOC), fair lending (financial regulators), securities disclosures and market integrity (SEC), anti-competition (DOJ), or health and safety of healthcare products (FDA).

8. **There is an increase in AI related litigation.** These cases argue that AI systems are subjects of well-established protections. Class actions have challenged companies for selling AI products that don't perform as advertised, for deploying systems that cause economic harm to consumers, and for failing to adequately warn about algorithmic limitations. More recent cases involve harm related to AI chatbots and possible negligence of their developers. The volume of litigation is creating pressure on companies to improve testing, documentation, and transparency.

9. **Ability to insure for AI harms is in question.** Insurers struggle to model risks for technologies that lack actuarial history, that evolve continuously through learning mechanisms. This uncertainty has led some insurers to consider explicit AI exclusions to

policies. The resulting gaps could create situations where companies face uninsurable risks, or where those who were harmed cannot recover damages because neither the company nor its insurer provides compensation. Developing appropriate insurance products will likely require better AI governance and risk modeling, and clearer liability standards.

10. **Some AI governance mechanisms are gaining popularity.** Risk-based assessments, Bias and Performance testing, Transparency measures (Notices informing users when they are interacting with, or subject to, decisions made by an AI system; Watermarking of synthetically generated content), Disclosures on training data quality are becoming governance mechanisms expected by consumers, regulators, and courts. Federal government continues to support advancements in AI evaluation methods, interpretability, AI control systems, and adversarial robustness, open source and open weight models, and AI incident reporting.

The U.S. market offers enormous commercial opportunity. Companies seeking to export AI products to the United States face a uniquely challenging business environment characterized by uncertainty, unpredictability and complexity. The market demands sophisticated policy navigation, and a good understanding of the clear differences in approach between the current White House, the Congress, and the state-level lawmakers. Similarly, companies need to be able understand the authorities and legal boundaries of each of the sources of AI policymaking in the United States. Japanese companies' commitment to quality and customer trust can provide a competitive advantage in this environment if properly navigated.

Sources of AI policymaking in the U.S.

Due to the different administrative levels in the United States, AI policymaking can be characterized as a multi-layered approach, with an interplay of the federal-level institutions and the state actors. Contrary to popular narratives, AI is regulated in the United States. Many baseline protections exist to counter the risks and challenges of AI systems – particularly as they are deployed in consequential and high-impact areas. Civil rights, consumer protection, product safety, copyright infringement, and anti-trust are domains with existing laws in the United States. Technology-agnostic legislation is applied to the outcomes of this evolving technology.

Both at the federal and state level, lawmakers attempt to address these themes by amending existing codes or introducing new bills. Similarly, regulators apply their existing mandates towards AI vendors, while courts interpret the laws to determine liability and accountability.

However, two questions remain. The first is how to reinterpret and apply these existing frameworks and sector-specific policies to emerging risks from AI systems. The second question concerns how to address the governance gaps where the existing mechanisms are not enough. As technology advances, new use cases create opportunities for such assessments. In the United States, several gaps have been identified: the need for human oversight, privacy, transparency, and risks associated with synthetic / generated outcomes (such as risks to child safety, or those related to deepfakes).

Given the complexity of the actors and their mostly complementary, but sometimes also conflicting approaches, it is critical to first establish a good understanding of the sources of AI policymaking. The rest of this section covers brief information on how these actors impact the ecosystem.

U.S. Congress (Legislative branch – Federal level)

The U.S. Congress holds the authority to enact legislation applicable across the country, including interstate commerce.[3] The Congress can establish binding legislation, new regulatory agencies, or assign new mandates to the existing agencies.

[3] The U.S. Senate. https://www.senate.gov/about/powers-procedures.htm

The U.S. Congress is bicameral, composed of the U.S. House of Representatives, and the Senate.[4] Both side of the Congress have established committees. These committees hold hearings on AI and hear from experts and stakeholders as it relates to the committee's specific mandate.

While the number of bills introduced in the Congress can be overwhelming, the bills with real possibility of enactment are usually those with bipartisan support. The Congress also holds the power to appropriate funding. This means that some critical AI-related clauses may be included in the federal budget appropriation or authorization laws.

Federal Courts (Judiciary branch)

Courts interpret existing laws and protections as they apply to AI systems. In the U.S. the decisions from the courts create precedent. This means that a decision from a federal court, for example, regarding whether or how copyrighted information can be used to train AI models can be binding for similar cases in the future.

Office of the President (Executive branch – Federal level)

The President and the executive branch can establish government-wide policies and supervise federal agencies using executive orders, the Office of Management and Budget (OMB) guidance, and national security directives.[5] These tools are also used to coordinate actions between federal agencies and guide federal procurement and use of AI.[6]

The current Administration's policy direction is mainly guided by the AI Action Plan, announced in July 2025, and the accompanying executive orders. The Action plan lays out recommendations for investment in AI research, development of full stack American AI, and deployment both domestically and internationally. The three strategic pillars are *Accelerating Innovation,* Building American AI Infrastructure, and Lead in International AI Diplomacy and Security.

Currently, a very sharp division exists between the AI policy approach of the current Administration and state-level lawmakers. The state-level lawmakers believe that innovation and regulation should be advanced together. The theory here is that public acceptance and trust for these technologies is critical for further adoption, investment and innovation. The lawmakers

[4] The House of Representatives. https://www.house.gov/the-house-explained
[5] Executive Office of the President. https://www.whitehouse.gov/eop/
[6] Hickok, Merve. *From Trustworthy AI Principles to Public Procurement Practices*, Berlin, Boston: De Gruyter (2024) https://doi.org/10.1515/9783111250182

have clear demand from their constituencies and support for regulation in their respective states. They adopt a proactive, consumer- or public-oriented perspective. In the meantime, White House adopts an investment-friendly, federal-first approach. It also creates new partnership and collaboration opportunities with large technology companies. While the Administration acknowledges the need for a national framework on AI driven by the Congress, it pushes for "a minimally burdensome national standard."[7] Domination of AI market globally is expected to create economic and national security benefits for the United States. The Administration encourages adoption of voluntary AI governance methods.

Executive Orders

An executive order (EO), as the name implies, is a directive from the President, and is addressed to the federal government. EO has the force of a law for federal government actions and does not require approval from Congress. Since EO must be supported by constitutional or statutory powers, an unlawful EO can be overturned due to judicial review. An EO can also be rescinded by a future President due to policy differences or overturned by a congressional legislation. EO provides policy directions to the federal agencies and can require individual departments or agencies to complete specific tasks by a certain date.

President Trump rescinded President Biden's Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110).[8] The executive orders from the first Trump Administration are still valid. As of January 2025, the following ones are in place:

- Ensuring a National Policy Framework for AI (12/11/2025)[9]
- Launching the Genesis Mission (11/24/2025)[10]
- Promoting the Export of the American AI Technology Stack (7/23/2025)[11]

[7] The White House. Executive Order on Ensuring a National Policy Framework for AI. December 11, 2025. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

[8] The White House. Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (Oct 30, 2023). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

[9] The White House. Executive Order on Ensuring a National Policy Framework for AI. December 11, 2025.

[10] The White House. Launching the Genesis Mission. November 24, 2025. https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/

[11] The White House. Executive Order on Promoting the Export of the American AI Technology Stack. July 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/

- Accelerating Federal Permitting of Data Center Infrastructure (7/23/2025)[12]
- Preventing Woke AI in the Federal Government (7/23/2025)[13]
- Advancing Artificial Intelligence Education for American Youth (4/23/2025)[14]
- Restoring Common Sense to Federal Procurement (4/15/2025)[15]
- Unleashing Prosperity Through Deregulation (1/31/2025)[16]
- Removing Barriers to American Leadership in Artificial Intelligence (1/23/2025)[17]
- Initial Rescissions of Harmful Executive Orders and Actions (1/20/2025)[18]
- Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (12/3/2020)[19]
- Maintaining American Leadership in Artificial Intelligence (2/11/2019)[20]

The Office of Science and Technology Policy (OSTP)

The OSTP provides the President with "advice on the scientific, engineering, and technological aspects of national policy and the work of the executive branch."[21] The President's Council of Advisors on Science and Technology (PCAST) operates under the OSTP. PCAST is an "advisory board whose members are drawn from outside the Federal Government, typically from

[12] The White House. Executive Order on Accelerating Federal Permitting of Data Center Infrastructure. July 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/07/accelerating-federal-permitting-of-data-center-infrastructure/
[13] The White House. Executive Order on Preventing Woke AI in the Federal Government. July 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/
[14] The White House. Executive Order on Advancing Artificial Intelligence Education for American Youth. April 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/
[15] The White House. Executive Order on Restoring Common Sense to Federal Procurement. April 15, 2025. https://www.whitehouse.gov/presidential-actions/2025/04/restoring-common-sense-to-federal-procurement/
[16] The White House. Executive Order on Unleashing Prosperity Through Deregulation. January 31, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-prosperity-through-deregulation/
[17] The White House. Presidential Action on Removing Barriers to American Leadership in Artificial Intelligence. January 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
[18] The White House. Presidential Action on Initial Rescissions of Harmful Executive Orders and Actions. January 20, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/
[19] The White House. Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. December 3, 2020. https://trumpwhitehouse.archives.gov/articles/promoting-use-trustworthy-artificial-intelligence-government/
[20] The White House. Executive Order on Maintaining American Leadership in Artificial Intelligence. February 11, 2025. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/
[21] The Office of Science and Technology Policy. https://www.whitehouse.gov/ostp/

industry, academia, and research institutions."[22] The current co-chair of PCAST, David Sacks, also holds the position of Special Advisor for AI and Crypto. Sacks was appointed as a special government employee in March 2025 for a duration of 130 days.[23] Michael Kratsios, Director of OSTP, is the other co-chair. Although President Trump announced that the PCAST will include up to 24 members, public records only show the composition of the PCAST to include David Sacks, Michael Kratsios, Sriram Krishnan, Bo Hines and Benny Johnson.[24]

A comparison of AI policy advice and action shows a clear contradiction between current policies and past policies of the two Trump Administrations. The 2020 EO on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government is important to note as it established a list of Trustworthy AI principles. These principles are also reflected in the OECD AI Principles. The first Trump Administration significantly contributed to the OECD AI Principles adopted in 2019.[25] These principles have also influenced the shape of major international AI governance frameworks adopted since 2019. While the title suggests "use in the federal government," these principles are important for norm setting. The 2025 executive orders, on the other hand, do not reference democratic values or civil rights and freedoms. The focus is how the U.S. could and should win the "race to achieve global dominance" in AI.[26]

The Office of Management and Budget (OMB)

The OMB is part of the executive branch, responsible for coordinating administrative policies across executive agencies, and establishing binding guidance and requirements for federal agencies.[27] Such guidance is issued on matters of budget, regulatory issues and management. The Biden Administration had published memos to implement the Executive Order 14110. However, when this executive order was rescinded, the relevant OMB memos were also rescinded and then replaced with new ones.

[22] Ibid
[23] The White House. Memorandum for David O. Sacks, Special Advisor for A.I. and Crypto. March 5, 2025. https://www.whitehouse.gov/wp-content/uploads/2025/03/Memo-David-Sacks-3.5.2025-1.pdf
[24] The White House. Fact Sheet: President Donald J. Trump Launches PCAST to Restore American Leadership in Science and Technology. January 23, 2025. https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-launches-pcast-to-restore-american-leadership-in-science-and-technology/. This statement reflects the publicly available information on PCAST's composition as of end of 2025.
[25] Center for AI and Digital Policy. CAIDP Index – AI and Democratic Values 2025. https://www.caidp.org/reports/caidp-index-2025/
[26] The White House. AI Action Plan. https://www.ai.gov/action-plan
[27] The Office of Management and Budget. https://www.whitehouse.gov/omb/

Individual Departments (Executive branch – Federal level)

Federal departments and agencies exercise delegated statutory authority to regulate specific sectors and issue guidance within their jurisdictions. They can conduct investigations, issue rules, and enforce compliance with applicable laws. Sometimes the departments may join forces to investigate or enforce a particular issue together. The Department of Commerce is particularly critical for exporters of AI products, and Department of Justice is for possible litigation.

The Department of Commerce

The Department of Commerce (DOC) is tasked to enhance the country's economic development and competitiveness, both domestically and internationally, while promoting fair trade, and collecting and publishing data to advance commerce.[28] The DOC also supports the transformation of technologies and innovation from the lab to marketplace by contributing to research and development, as well as setting standards.

One of the most important tasks for the DOC, as it relates to AI, is to support development and encourage export and adoption of full AI technology stack developed in the United States. DOC also enforces trade rules and sanctions as relevant for advanced computing chips or semiconductors.[29] The DOC has recently launched a new website, AIexports.gov, and established an integrated AI export team.[30]

The DOC also controls several institutes relevant to the R&D and governance of AI.

The National Institute of Standards and Technology (NIST) is a metrology institute, focused on the science of metrology and evaluations, and provides guidance or reference documents which can be adopted voluntarily. The NIST AI Risk Management Framework (AI RMF), has become a foundational reference document for voluntary AI risk management.[31] The AI RMF provides a structured approach organized around four core functions:

1. **Govern**: Cultivate risk-aware organizational culture and establish governance structures
2. **Map**: Contextualize AI systems within operational environments
3. **Measure**: Assess risks through quantitative and qualitative approaches

[28] The Department of Commerce. https://www.commerce.gov/about
[29] The Bureau of Industry and Security. https://www.bis.gov/
[30] The Department of Commerce. American AI Exports Program . October 21, 2025. https://www.trade.gov/press-release/department-commerce-announces-american-ai-exports-program-implementation
[31]The National Institute of Standards and Technology. The NIST AI Risk Management Framework (AI RMF). January 26, 2023. https://www.nist.gov/itl/ai-risk-management-framework

4. **Manage**: Prioritize and address identified risks through controls and safeguards

The NIST also provides further research and frameworks on Cybersecurity,[32] Adversarial Machine Learning,[33] or Managing Misuse Risk for Dual-Use Foundation Models.[34] One of the objectives for the DOC under the Trump Administration is to advance the adoption of NIST's standards globally. Companies exporting AI products to the U.S. could benefit from utilizing the standards.

The Center for AI Standards and Innovation (CAISI) (formerly known as the U.S. AI Safety Institute) is tasked as the "industry's primary point of contact within the U.S. Government to facilitate testing and collaborative research."[35] The CAISI establishes voluntary agreements with AI development and evaluation companies, and conduct evaluations on AI capabilities – especially on risks related to cybersecurity, biosecurity, and chemical weapons. Foreign companies would benefit from integrating learnings from these evaluations into their products.

The Department of Justice

The Department of Justice (DOJ) is tasked to enforce federal laws.[36] The department can investigate and prosecute if there is a violation of federal laws and represents the U.S. government if the government is a party to a legal proceeding. The areas where DOJ will be most involved in terms of AI-related cases will be civil rights enforcement, "AI-washing" practices, and anti-trust / anti-competition issues. The DOJ can keep companies accountable for making misleading statements to customers or investors or engaging in deceptive marketing tactics which allege use of AI in decision-making processes or exaggerating the capabilities of their AI products.

[32] The National Institute of Standards and Technology. Cybersecurity Framework. https://www.nist.gov/cyberframework#csf-2-0

[33] The National Institute of Standards and Technology. NIST Trustworthy and Responsible AI Report Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. March 24, 2025. https://www.nist.gov/news-events/news/2025/03/nist-trustworthy-and-responsible-ai-report-adversarial-machine-learning

[34] The National Institute of Standards and Technology. Updated Guidelines for Managing Misuse Risk for Dual-Use Foundation Models. January 15, 2025. https://www.nist.gov/news-events/news/2025/01/updated-guidelines-managing-misuse-risk-dual-use-foundation-models

[35] The Department of Commerce. Statement from U.S. Secretary of Commerce Howard Lutnick on Transforming the U.S. AI Safety Institute into the Pro-Innovation, Pro-Science U.S. Center for AI Standards and Innovation. June 3, 2025. https://www.commerce.gov/news/press-releases/2025/06/statement-us-secretary-commerce-howard-lutnick-transforming-us-ai

[36] The Department of Justice. https://www.justice.gov/

The Department of Energy[37]

The Department of Energy (DOE) is tasked to advance the national, economic, and energy security; and to promote scientific and technological innovation in support of that mission. Specific to AI, DOE has several responsibilities to advance the Administration's policies. DOE is tasked with the implementation of the Genesis Mission. It is also responsible for accelerating energy infrastructure development. Since DOE controls energy grid permitting, its work is critical for datacenter development and expansion across the United States.

Independent Regulators (Executive branch – Federal level)

The independent regulatory agencies have specific mandates as detailed in legislation. Their statutory mandates allow them to issue rulemaking (binding regulations), conduct investigations, enforce compliance, and sanction entities under their jurisdiction as necessary. Several regulatory agencies in the U.S. have mandates to uphold civil rights legislation, protect consumers and regulate certain sectors of the economy.

In fact, agencies clearly reaffirmed that their existing authorities apply equally to the use of AI. The Justice Department's Civil Rights Division, the Consumer Financial Protection Bureau (CFPB), the Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) previously pledged to "uphold America's commitment to the core principles of fairness, equality and justice as emerging automated systems, including those sometimes marketed as "artificial intelligence" or "AI," become increasingly common in our daily lives – impacting civil rights, fair competition, consumer protection and equal opportunity."[38]

It should be noted that the "independent" nature of these agencies is in question and will be determined in 2026 by the Supreme Court in the case, Trump v. Slaughter. In March 2025, President Trump fired two FTC Commissioners, Alvaro Bedoya and Rebecca Kelly Slaughter, without cause.[39] President Trump had originally nominated Slaughter to the FTC in 2018, and her term was extended by former President Biden in 2023. The FTC Act only allows removals "by the President for inefficiency, neglect of duty, or malfeasance in office."[40] The case now in front of

[37] The Department of Energy. https://www.energy.gov/

[38] The Federal Trade Commission. FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI. April 25, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai

[39] Jody Godoy. Trump fires both Democratic commissioners at FTC. Reuters. March 18, 2025. https://www.reuters.com/world/us/trump-fires-both-democratic-commissioners-ftc-sources-say-2025-03-18/

[40] The FTC Act, 15 U.S.C. §§ 41-58. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim

the Supreme Court which will argue "statutory removal protections for members of the Federal Trade Commission violate the separation of powers."[41] The case may define the future independence of the regulatory agencies at large.

The Federal Trade Commission (FTC)

The FTC has been the most active federal agency in AI enforcement. The FTC's mission is to protect "the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education."[42] This mandate provides the FTC with vast powers to monitor, investigate and enforce sanctions on private companies. Most companies conducting business in the United States fall under the remit of the FTC.[43] Between its Bureau of Consumer Protection, Bureau of Competition, and its Office of Technology, the Commission has provided a significant amount AI guidance documents and warnings. The Commission also enforced sanctions on several companies providing AI products.

The Securities and Exchange Commission (SEC)

The SEC's mission is "protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation."[44] Companies which sell and trade securities and offer advice to investors fall under the mandate of the SEC. The Commission has been active in issuing comments to companies addressing AI-related questions and disclosures. A review of SEC comment letters found that, between 2021 and October 2024, the Commission issued almost 100 separate comments in disclosure review letters to more than 50 companies.[45] Key themes from this review, as well as other SEC guidance include:

- Materiality determinations
- Specific and balanced business and risk disclosures
- Clear definition of AI and use in specific business context
- Reasonable basis for AI-related claims (avoiding "AI-washing")[46]

[41] The Supreme Court. Donald J. Trump v Rebecca Kelly Slaughter. September 22, 2025. https://www.supremecourt.gov/opinions/24pdf/25a264_o759.pdf
[42] The Federal Trade Commission. https://www.ftc.gov/about-ftc/mission
[43] Excluding those already subject to other sectoral regulators such as telecommunications, financial services, pharmaceuticals, airlines, insurance etc.
[44] The Securities and Exchange Commission. https://www.sec.gov/about/mission
[45] Marsha Mogilevich, J.T. Ho, and Bobby Bee. SEC Comment Letter Trend: AI-Related Disclosures. January 16, 2025. Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2025/01/16/sec-comment-letter-trend-ai-related-disclosures/
[46] The Securities and Exchange Commission. Chair Gary Gensler on AI Washing. March 18, 2024. https://www.sec.gov/newsroom/speeches-statements/sec-chair-gary-gensler-ai-washing

- Verification of AI capabilities before making public claims (fraud & deception)[47]
- Conflicts of interest[48]
- Systemic risk[49]

Just like the FTC, the SEC also has enforcement powers to hold companies accountable for misconduct or harming investors if they violate the federal securities laws.

The SEC also created the Cyber and Emerging Technologies Unit (CETU) to combat cyber-related misconduct and protect retail investors, prioritizing enforcement related to fraud committed using emerging technologies. The Unit's priorities are:[50]

- Fraud committed using emerging technologies, such AI & ML
- Use of social media, the dark web, or false websites to perpetrate fraud
- Hacking to obtain material nonpublic information
- Takeovers of retail brokerage accounts
- Fraud involving blockchain technology and crypto assets
- Regulated entities' compliance with cybersecurity rules and regulations
- Public issuer fraudulent disclosure relating to cybersecurity

In other words, the SEC's priorities include both the practices of the companies deploying AI products in the United States, and those actors who maliciously use AI and other emerging technologies to commit fraud.

The Equal Employment Opportunity Commission (EEOC)

The EEOC's mission is "enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, childbirth, or related conditions, transgender status, and sexual orientation), national origin, age (40 or older), disability or genetic information."[51] Similar to other agencies, the EEOC

[47] The Securities and Exchange Commission. Office Hours With Gary Gensler: Fraud and Deception in Artificial Intelligence. October 10, 2024. https://www.sec.gov/newsroom/speeches-statements/gensler-transcript-fraud-deception-artificial-intelligence-101024

[48] The Securities and Exchange Commission. Conflicts of Interest in Artificial Intelligence | Office Hours with Gary Gensler. August 13, 2024. https://www.sec.gov/newsroom/speeches-statements/gensler-transcript-artificial-intelligence-081324

[49] The Securities and Exchange Commission. Office Hours with Gary Gensler: Systemic Risk in Artificial Intelligence. September 19, 2024. https://www.sec.gov/newsroom/speeches-statements/gensler-transcript-systemic-risk-artificial-intelligence-091924

[50] The Securities and Exchange Commission. SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors. February 20, 2025. https://www.sec.gov/newsroom/press-releases/2025-42

[51] The Equal Employment Opportunity Commission. https://www.eeoc.gov/overview

also provides guidance documents, makes rules to enforce legislation, and investigate employers for charges of discrimination.

As it relates to AI products, the EEOC's main target is how employers use AI products to make employment-related decisions – such as hiring, terminations, compensation, disciplinary action. While companies exporting AI products to the U.S. do not directly fall under EEOC's scope, there is still a need to be aware of future expectations from the Commission so that exporters can collaboratively work with their American clients.

The Federal Communication Commission (FCC)

The FCC's mission is to "regulate interstate and international communications by radio, television, wire, satellite, and cable."[52] While this mission may sound too high level or irrelevant for AI products at first instance, the FCC has already engaged in activities to protect consumers from malicious AI uses, especially in the case of using deepfake audio to defraud consumers.

The Food and Drug Administration (FDA)

As one of the regulators of a highly controlled domain in the United States, FDA's primary focus in relation to AI is regulation of medical devices.[53] AI is considered a medical device "if intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."[54] AI may be included under the FDA's mandate as a Software **as** a Medical Device, or Software **in** a Medical Device.[55]

The FDA conducts pre-market authorization reviews of medical devices for safety, effectiveness and performance for their intended use case.[56] It also requires advance change management notices, and real-time monitoring once the devices are available in the market.

Tools mainly used as administrative systems in healthcare settings, certain clinical decision support tools, and wellness apps do not generally fall under the FDA's regulations.

[52] The Federal Communication Commission. https://www.fcc.gov/about/overview
[53] The Food and Drug Administration. https://www.fda.gov/
[54] The Food and Drug Administration. https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device
[55] The Food and Drug Administration. Software as a Medical Device (SaMD). https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd
[56] Bipartisan Policy Center. FDA Oversight: Understanding the Regulation of Health AI Tools. November 10, 2025. https://bipartisanpolicy.org/issue-brief/fda-oversight-understanding-the-regulation-of-health-ai-tools/

However, such tools marketed directly to clinicians, patients, or consumers as a product may fall under the FTC's regulatory mandate.[57] They may also be subject to relevant state-level laws.

Individual States (Legislative, Executive and Judiciary branches – State level)

Under the federal system of government, the states possess independent authority to pass legislation and regulate state commerce, safety, welfare and public health. To be more specific, 10th Amendment of the U.S. Constitution states, "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[58]

With regards to AI products, this means that state lawmakers can pass legislation to assign obligations to companies developing or deploying AI systems within the state territory. Lawmakers can also determine how the rights of both people in the State as well as the businesses should be protected.

State-level courts and regulators are responsible for applying the respective laws, rules and regulations.

Overview of the current state and future trends of AI-related legislation in the United States

Analysis of AI policy trends in the United States must take into account the multi-faceted and layered nature of policymaking. The U.S. legal system enables each branch of the federal government to be an important actor in this discussion. The policy positions and priorities of the Administration, the U.S. Congress, and state lawmakers should be analyzed separately, and not be simply bucketed under "U.S. AI policy" umbrella.

[57] Bipartisan Policy Center. Oversight Beyond the FDA: Understanding the Regulation of Health AI Tools. June 20, 2025. https://bipartisanpolicy.org/report/oversight-beyond-the-fda-understanding-the-regulation-of-health-ai-tools/

[58] Constitution of the United States. 10th Amendment. https://constitution.congress.gov/constitution/amendment-10/

Bipartisan efforts for AI governance

In December 2024, the U.S. Congress Bipartisan House Task Force on AI published a report containing its guiding principles, and forward-looking policy recommendations. The Task Force's report follows multiple expert hearings and roundtables. The report highlights the principle that policymakers should first identify which issues arising from AI are not covered by existing laws and regulations and are hence novel. The Task Force also agrees that responsible innovation advances adoption, trust is a necessary component, and that a "thoughtful, risk-based approach to AI governance can promote innovation rather than stifle it."[59] A final principle is the incremental and agile approach to AI policymaking. In other words, no single comprehensive AI legislation should be expected as the final word in the United States. Rather, stakeholders should be continually informed about the emerging needs and respond accordingly.

In the Congress, bipartisan efforts continue and have the highest chance of moving forward. For example, the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks ("TAKE IT DOWN") Act (S. 146), was adopted in 2025.[60] The bipartisan bill was co-sponsored by Sens. Cruz (Republican) and Klobuchar (Democrat). The bill passed the Senate by unanimous consent, and the House by a vote of 409-2. The law requires the covered platforms to provide the public with a mechanism to notify if non-consensual intimate imagery (NCII) content was published without consent. They must then remove the NCII content within 48 hours and make a reasonable effort to remove possible identical copies. The Act includes federal criminal sanctions for sharing or threatening to share NCII and deepfakes.

In addition to the above, there are currently only a handful of AI-specific federal laws:

- **AI in Government Act of 2020:** requires federal government's use of AI is effective, ethical, and accountable by providing resources and guidance to federal agencies[61]
- **National Artificial Intelligence Initiative Act of 2020:** provides a definition of AI for U.S. government purposes, tasks NIST to develop an AI risk-mitigation framework, technical standards and guidelines that promote trustworthy AI systems[62]

[59] The U.S. Congress. Bipartisan Task Force on AI - Report on AI. December 17, 2024. https://science.house.gov/2024/12/house-bipartisan-task-force-on-artificial-intelligence-delivers-report
[60] The U.S. Congress. TAKE IT DOWN Act. 19 May 2025. https://www.congress.gov/bill/119th-congress/senate-bill/146
[61] The U.S. Congress. AI in Government Act of 2020. Public Law 116-260 (codified at 40 U.S.C. § 11301 note). 2020. https://www.govinfo.gov/content/pkg/USCODE-2023-title40/pdf/USCODE-2023-title40-subtitleIII-chap113-subchapI-sec11301.pdf
[62] The U.S. Congress. National Artificial Intelligence Initiative Act of 2020. Public Law 116–283 (codified at 15 U.S.C. § 941). January 1, 2021. https://www.govinfo.gov/content/pkg/PLAW-116publ283/pdf/PLAW-116publ283.pdf

- **Identifying Outputs of Generative Adversarial Networks Act' or the ''IOGAN Act'' of 2020:** directs the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research on generative adversarial networks, and content and information authenticity[63]
- **AI Training Act:** requires federal procurement and governance workforce to have knowledge of AI capabilities and risks[64]
- **Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022:** establishes a federal assistance program for "the fabrication, assembly, testing, advanced packaging, production, or R&D of semiconductors"[65]
- **Advancing American AI Act:** part of the National Defense Authorization Act (NDAA) of Fiscal Year 2023, to promote adoption of advanced technologies in federal government[66]
- **NDAA Fiscal Year 2026:** tasks Department of Defense with establishing an AI procurement framework related to AI cybersecurity and physical security standards; assessing technical standards for digital content provenance; and establishing a steering committee on artificial general intelligence.[67]

These acts do not create any regulatory obligations on the developers or deployers of AI systems. They are mainly focused on federal AI adoption, AI research and standards development and coordination. The Government Accountability Office provides a timeline of federal efforts which includes both the executive orders and the federal level legislation: [68]

[63] The U.S. Congress. Identifying Outputs of Generative Adversarial Networks Act' or the ''IOGAN Act''. Public Law 116-258. December 23, 2020. https://www.govinfo.gov/content/pkg/PLAW-116publ258/pdf/PLAW-116publ258.pdf

[64] AI Training for the Acquisition Workforce Act. Public Law 117-207 (codified at 41 U.S.C. § 1703). 2022. https://www.govinfo.gov/content/pkg/COMPS-17079/pdf/COMPS-17079.pdf

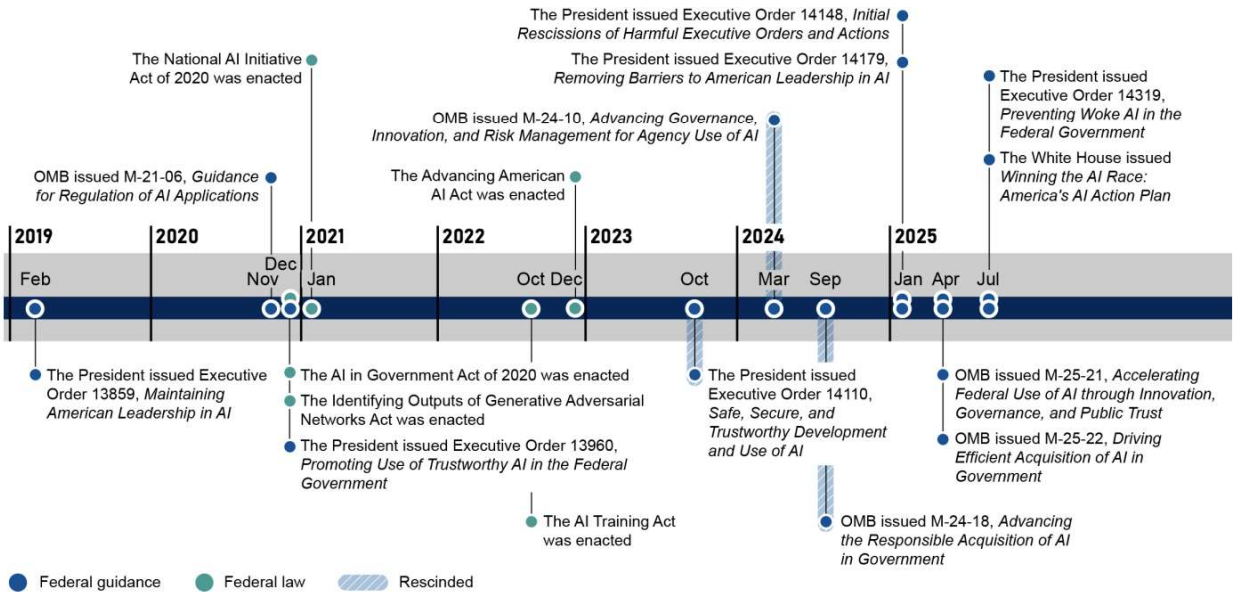
[65] CHIPS Act of 2022. Public Law 117-167 § 101-107. 2022. https://www.congress.gov/bill/117th-congress/house-bill/4346

[66] The U.S. Congress. Advancing American AI Act (under James M. Inhofe National Defense Authorization Act for Fiscal Year 2023). Public Law 117-263. December 23, 2022. https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf

[67] The U.S. Congress. National Defense Authorization Act for Fiscal Year 2026. December 18, 2025. https://www.congress.gov/bill/119th-congress/senate-bill/2296/text

[68] The Government Accountability Office. Federal Efforts Guided by Requirements and Advisory Groups. September 2025. https://www.gao.gov/assets/gao-25-107933.pdf

Figure 1: Timeline of Key Federal Efforts to Advance Artificial Intelligence (AI) with Agency Requirements



Credit: The Government Accountability Office.
Federal Efforts Guided by Requirements and Advisory Groups. September 2025

The bipartisan nature of AI policy was most on display in efforts to resist the Executive Branch's pressure to pre-empt state-level AI legislation. While the Administration's continuous attempts are initially reflected in draft bills, the lawmakers strongly reject attempts to undermine state power to legislate AI and consider these attempts an overreach of federal power. As of end of 2025, two such initiatives received strong bipartisan reaction and were ultimately unsuccessful.

The first attempt was a proposed 10-year moratorium in one of the first versions of the comprehensive One Big Beautiful Bill Act. The proposal for a moratorium on state AI regulation was almost unanimously opposed. Congressional lawmakers were joined by a significant coalition of bipartisan stakeholders composed of state legislators, state Attorneys General, and a large coalition of civil society organizations.[69] During the budget reconciliation process, this proposal was defeated with a 99-1.[70] The attempt was in contradiction with increasing concerns by the

[69] Joint Letter: Opposition to Federal Preemption of State AI Laws within the NDAA. MLex. November 19, 2025. https://www.mlex.com/mlex/articles/2413788/attachments/0

[70] The Washington Post, *In dramatic reversal, Senate votes to kill AI-law moratorium,* Jul. 1, 2025, https://www.washingtonpost.com/politics/2025/07/01/ai-moratorium-big-beautiful-bill/ ; The New York Times, *Defeat of a 10-Year Ban on State A.I. Laws Is a Blow to Tech Industry,* Jul. 1, 2025, https://www.nytimes.com/2025/07/01/us/politics/state-ai-laws.html;

public and the calls to regulate negative outcomes of AI use, as well as the constituency-driven legislative activity at state level.[71]

Second attempt was a proposal to include a preemption clause in the National Defense Authorization Act. This was an attempt to use this federal law to displace or override state or local laws on AI. Such federal law preemption clauses can make the federal laws the "supreme law" of the country. The NDAA is considered a must-pass law, as it outlines national defense priorities and authorizes annual funding for the military. Lawmakers agreed to remove this proposed AI preemption clause from the package.[72]

While these two attempts were rejected, the Executive Branch continues to exert pressure to prevent or restrict states' ability to require AI safeguards to protect consumer and civil rights. The last major step from the White House is an executive order, again attempting to pre-empt state regulations on AI.[73] To briefly summarize, the EO:[74]

- directs U.S. Department of Justice to create an "AI Litigation Task Force" in order to limit the ability of states to pass laws and protect their residents,
- directs U.S. Department of Commerce to identify state AI laws (including those that address transparency or algorithmic discrimination), and label them as "onerous"
- proposes to cut funding for internet access in rural communities if the states pass further laws, or enforce those disfavored by the Administration.
- attempts to direct federal agencies to take action against states that enact consumer protection laws.

Some of these proposals, such as reducing broadband access, have little to do with national AI policies and are in fact counterintuitive for AI adoption. Using an EO to limit the ability of states to pass laws is unconstitutional. Executive orders cannot preempt state laws. One should expect legal challenges to this attempt. In the meantime, one should also expect the Administration to continue its state-level deregulatory pressure in the foreseeable future.

---

[71] Marc Rotenberg, Merve Hickok, Christabel Randolph. Proposed Moratorium on US State AI Laws is Short-Sighted and Ill-Conceived. Tech Policy Press. May 21, 2025. https://www.techpolicy.press/proposed-moratorium-on-us-state-ai-laws-is-shortsighted-and-illconceived/

[72] Alexander Bolton. Hawley applauds decision to drop AI-related provision from Defense bill. The Hill. December 3, 2025. https://thehill.com/homenews/senate/5631558-hawley-ai-ndaa/

[73] The White House. Executive Order on Ensuring a National Policy Framework for AI. December 11, 2025. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

[74] The Center for AI and Digital Policy. December 12, 2025. https://www.linkedin.com/posts/center-for-ai-and-digital-policy_proposed-moratorium-on-us-state-ai-laws-is-activity-7405332875044323328--elK?utm_source=share&utm_medium=member_desktop&rcm=ACoAAADpeFUBow5sY9-7sQbWkB32kFw7xsp7zgs

Only Congress can preempt state legislation if the target of legislation falls under federal powers (such as interstate commerce or national security). Efforts to establish a federal framework for AI will continue to be one of the most pressing topics for the Congress. On this note, the last 2025 EO (Executive Order on Ensuring a National Policy Framework for AI) also directs the Chair of the President's Council of Advisors on Science and Technology (PCAST) to "prepare a legislative recommendation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order."[75] While some individual lawmakers may adopt the proposal, there is no requirement for lawmakers in general to advance such recommendations. They may instead advance the bipartisan legislative efforts to establish an affirmative baseline for safeguards (for example for transparency, privacy, child safety),[76] and only then consider preemption of state regulations.

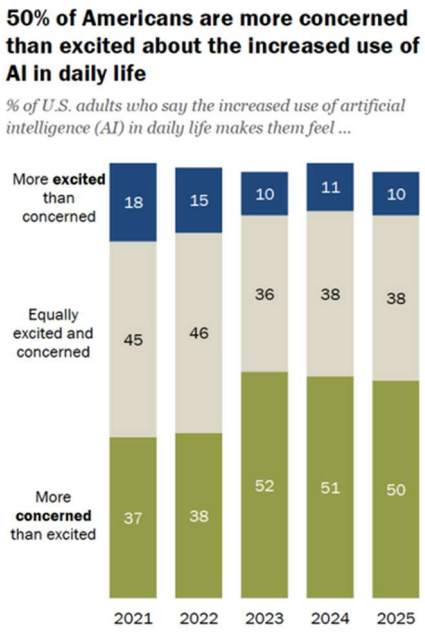
In summary, AI priorities at the U.S. Congress level include civil rights and liberties, child safety, deepfakes, intellectual property, liability concerns, privacy, research and development capabilities, education and workforce impacts, and national and economic security issues (such as energy resources, critical sectors (agriculture, healthcare and finance), and support for small businesses).

Public sentiment surveys

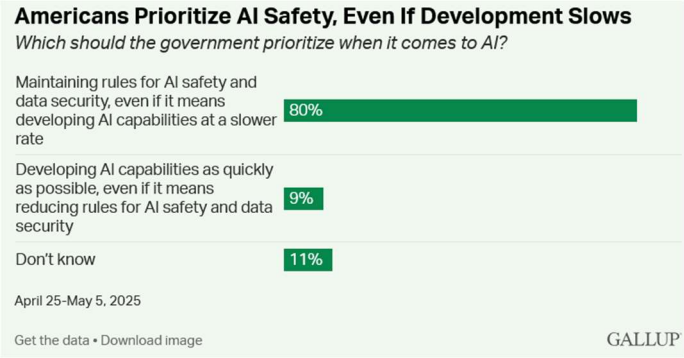
Public sentiment polls provide policymakers and private organizations alike with a good picture of how the mainstream public understands and reacts to AI technology and its impact. Understanding the response and trends in sentiments are important because these show the expectations from lawmakers and regulators alike.

Recent surveys from Pew Research show that since 2021, the level of concern from the public regarding AI's impact on their personal lives has been increasing.[77]

[75] The White House. Executive Order on Ensuring a National Policy Framework for AI. December 11, 2025.
[76] Marc Rotenberg, Merve Hickok, Christabel Randolph. Proposed Moratorium on US State AI Laws is Short-Sighted and Ill-Conceived. Tech Policy Press. May 21, 2025. https://www.techpolicy.press/proposed-moratorium-on-us-state-ai-laws-is-shortsighted-and-illconceived/
[77] Pew Research Center. How Americans View AI and Its Impact on People and Society. September 17, 2025. https://www.pewresearch.org/science/2025/09/17/how-americans-view-ai-and-its-impact-on-people-and-society/



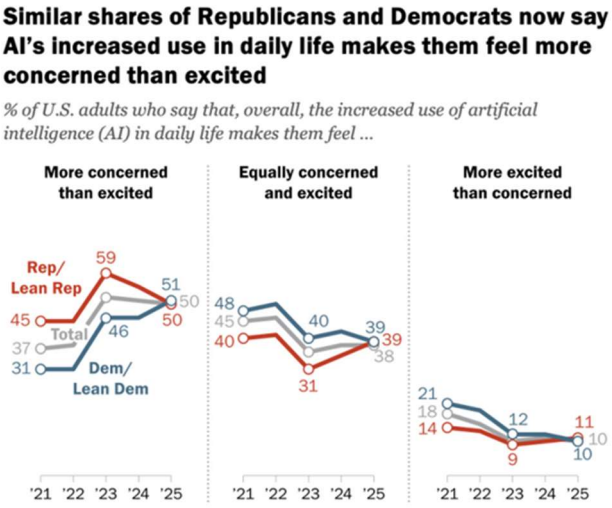
Similarly, a 2025 Gallup survey shows that almost all Americans (97%) agree that AI safety and security should be regulated, with 80% believing the "government should maintain rules for AI safety and data security, even if it means developing AI capabilities more slowly."



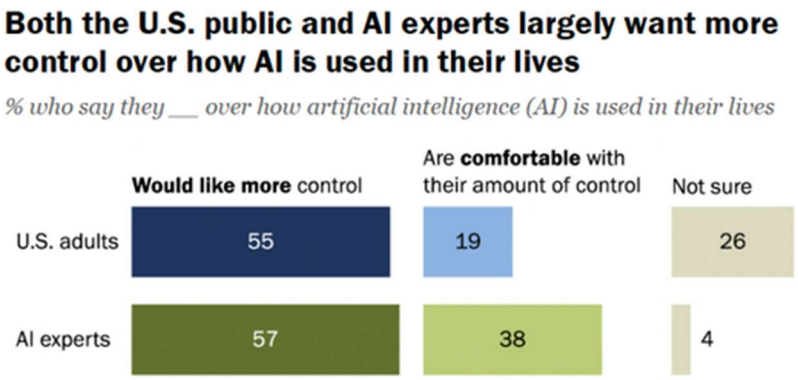
The survey results highlight a bipartisan approach at the societal level too - with 88% of Democrats and 79% of Republicans and independents favoring maintaining rules for safety and security.[78]

[78] Gallup. Americans Prioritize AI Safety and Data Security. September 16, 2025. https://news.gallup.com/poll/694685/americans-prioritize-safety-data-security.aspx

The Pew Research also shows similar sentiments from Republicans and Democrats - equally concerned about AI in daily life.[79] According to this survey conducted in June 2025, Pew analysts underline that "nearly identical shares of Republicans and Democrats say they are *more concerned than excited* about the increased use of AI in daily life – 50% and 51%, respectively."



Other Pew Research from 2025 compare the views of U.S. public versus the AI experts, and the convergence on concerns across the party lines. The Pew Research "How the U.S. Public and AI Experts View Artificial Intelligence"[80] survey covers responses from both the public and AI experts. Both groups want more control over how AI is used in their lives, and worry that the regulations will fall short. In the meantime, the level of enthusiasm for AI is significantly different between these groups.

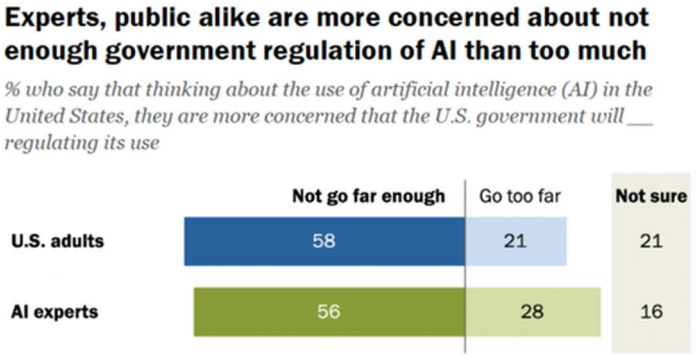


[79] Pew Research Center. Republicans, Democrats now equally concerned about AI in daily life, but views on regulation differ. November 6, 2025. https://www.pewresearch.org/short-reads/2025/11/06/republicans-democrats-now-equally-concerned-about-ai-in-daily-life-but-views-on-regulation-differ/

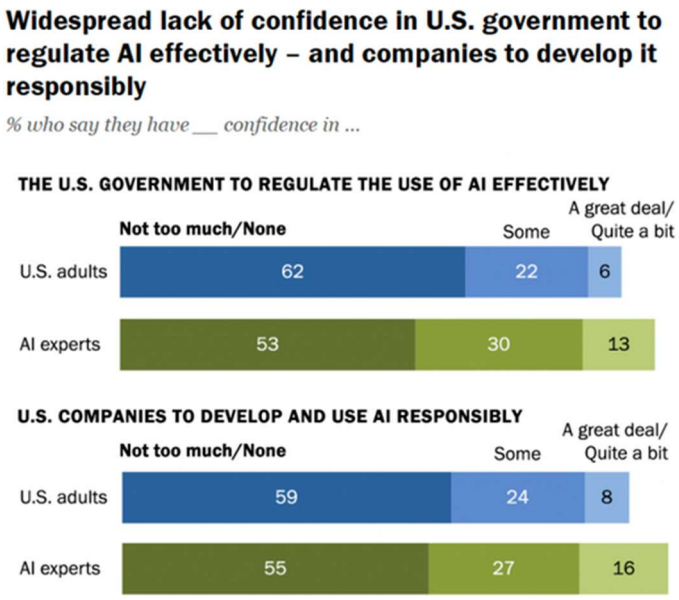
[80] Pew Research Center. How the U.S. Public and AI Experts View Artificial Intelligence. April 3, 2025. https://www.pewresearch.org/internet/2025/04/03/how-the-us-public-and-ai-experts-view-artificial-intelligence/

66% of all surveyed overall and 70% of experts are highly concerned about people getting inaccurate information from AI. Similarly, both groups are concerned about bias in decisions made by AI (each at 55%).

With regards to level of regulation of AI, both groups concerned that use of AI is not regulated enough in the U.S. The differences in political party affiliation are minimal, where majorities in both parties are more concerned about insufficient protections (Democrats - 64% vs. Republicans - 55%).



Both groups are similarly skeptical that the U.S. companies will develop and use AI responsibly.



In short, American public is increasingly more concerned about the unfair and opaque AI systems used to make determinations in their daily lives. Their confidence in both the

government and the companies to act responsibly is low. These systems "will diminish public trust and thus slow down AI adoption."[81]

Trends and forecasts regarding litigation of AI products in the U.S.

AI products can be subject to litigation in courts, or enforcement action by the sectoral regulators. The following section covers both these activities and provides insights into the trends.

Litigation

Over the last few years, many lawsuits were filed for both predictive and generative AI systems. In fact, there are now several online sources which track the status of AI-related litigation in the United States.[82] While the majority of the more recent lawsuits are clustered around copyright and protection of likeness, there are several cases which are useful for Japanese companies to understand. The results (some of them class action lawsuits) can provide precedent on how the courts interpret the current legislation. While most of the AI-related litigation is ongoing, the trends show preference for civil rights discrimination cases, along with negligence, and product liability (failure to warn, psychological harm, psychological manipulation and dependency).

The cases will be helpful to understand how current civil rights and consumer protection legislation is interpreted by the courts. It is also important for lawmakers to understand the emerging governance gaps – especially in relation to child safety, CSAM (Child Sexual Abuse Material), deepfake frauds, systemic bias, and transparency disclosures.

The following cases focus on traditional (predictive) AI products:

Baker v. CVS Health Corporation: "A job candidate alleged that CVS violated the Massachusetts Lie Detector Statute (Mass. Gen. Laws. Ch. 149, §19B) by subjecting the candidate to an artificial intelligence-based test (to help evaluate an individual's integrity and cultural fit) during a job interview without notifying the candidate of his statutory rights. The Court denied CVS' motions

[81] Center for AI and Digital Policy. *Comments to OSTP on the Development of an Artificial Intelligence (AI) Action Plan,* March 14, 2025. https://files.nitrd.gov/90-fr-9088/CAIDP-AI-RFI-2025.pdf

[82] George Washington University. GW Law ETI AI Litigation Database, and American Bar Association.

to dismiss for failure to state a claim and for lack of standing."[83] The case is ongoing. The human resources software in question is HireVue.

Importance: The software used by the employer is based on biometric emotion analysis. While not prohibited in the United States, such AI system used to infer personality characteristics using biometric information is prohibited under the EU AI Act. In 2021, HireVue announced a decision to remove visual analysis from the companies "new assessment models."[84] Emotion analysis lacks scientific validity.[85] HireVue's announcement leaves the status of 'existing' models used by employers unclear. Lack of disclosure from the employer was another concern in this particular case.

Mobley v. Workday: The plaintiff, Mobley, alleges that Workday (a human resources software company) operates as an "agent" since it performs functions like that of employers. The court ordered Workday to produce customer list that has used its AI features since September 2020, while allowing a national collective action under the Age Discrimination in Employment Act (ADEA).[86] The case is ongoing.

Importance: The Court certified this AI bias case as a collective action case. While this case is about employment decisions, one may expect similar AI bias cases in other domains where civil rights and anti-discrimination protections apply – such as housing, insurance and financial services. Additionally, the case can expand liability to the HR software vendors.

United States v. RealPage: The Department of Justice and eight states initially filed a complaint against RealPage, claiming that its rent pricing algorithm may be enable price fixing. RealPage was "accused of having agreed to share the landlords' nonpublic, competitively sensitive information to train and run RealPage's algorithmic pricing software"[87] which then maximizes the pricing for the landlords and does not leave renters with options.

---

[83] Bradford Newman and Adam Aft. Recent Developments in Artificial Intelligence Cases and Legislation 2025. American Bar Association. August 5, 2025. https://www.americanbar.org/groups/business_law/resources/business-law-today/2025-august/recent-developments-artificial-intelligence-cases-legislation/

[84] HireVue. Industry leadership: New audit results and decision on visual analysis. January 12, 2021. https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis

[85] Roy Maurer. HireVue Discontinues Facial Analysis Screening. SHRM Blog. February 3, 2021. https://www.shrm.org/topics-tools/news/talent-acquisition/hirevue-discontinues-facial-analysis-screening

[86] Mobley v. Workday, Inc., 3:23-cv-00770, (N.D. Cal.) Civil Rights Litigation Clearinghouse database. https://clearinghouse.net/case/44074/

[87] Khushita Vasant. RealPage sued by DOJ, eight states for algorithmic price-fixing, monopolizing revenue management software market. MLex. August 23, 2024. https://www.mlex.com/mlex/articles/2076626/realpage-sued-by-doj-eight-states-for-algorithmic-price-fixing-monopolizing-revenue-management-software-market

A further amended complaint added two more states as plaintiffs and added six rental real estate companies as defendants.[88] In November 2025, RealPage settled with the DOJ, without admitting any wrongdoing. However, the settlement requires RealPage to "stop using competitively sensitive information, discontinue any incentives for users to accept pricing recommendations, and "cooperate fully and truthfully" with the DOJ's pursuit of remaining claims against landlords."[89]

Importance: The settlement shows that competing companies must make their pricing decisions independently and not create a monopolistic pricing situation. Algorithms shared between providers that rely on competitively sensitive information is likely to face challenges from antitrust enforcers both at federal and state level.

United States v Meta: The Department of Justice complaint alleged that Meta

- "enabled and encouraged advertisers to target their housing ads by relying on race, color, religion, sex, disability, familial status and national origin to decide which Facebook users will be eligible and ineligible to receive housing ads."
- its ad targeting tool used machine-learning to "find Facebook users who share similarities with groups of individuals selected by an advertiser using several options provided by Facebook."
- And that the algorithms "rely in part on FHA-protected characteristics — such as race, national origin and sex — to help determine which subset of an advertiser's targeted audience will actually receive a housing ad."[90]

Importance: The settlement was the first case of algorithmic discrimination undermining the Fair Housing Act. In addition to the financial penalty, the settlement agreement requires Meta to stop using the related algorithms, train another algorithm that does not use protected characteristics or its proxies, and have an independent, third-party reviewer to investigate and verify on an ongoing basis the compliance of the product.

Estate of Gene B. Lokken et al. v. UnitedHealth Group, Inc. et al.: The estates of two patients who died but were insured by UnitedHealth Group allege that UnitedHealth "knowingly used an

[88] George Washington University. GW Law ETI AI Litigation Database. United States v. RealPage, Inc. https://blogs.gwu.edu/law-eti/ai-litigation-database/case-detail-page/?pid=252
[89] Clayton Vickers and Chris May. RealPage settles with US DOJ, agrees to restrict on rent-setting algorithms. MLex. November 24, 2025. https://www.mlex.com/mlex/artificial-intelligence/articles/2415090
[90] The Department of Justice. Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising. June 21, 2022. https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known

AI tool with a high error rate to override physician recommendations and to deny elderly patients care owed to them through Medicare Advantage healthcare plans."[91] The case is ongoing.

Importance: The case is one of the three current lawsuits where plaintiffs allege improper use of AI by the insurers to make coverage decisions, while ignoring clinical determinations.[92] Across these cases arguments are made for breach of good faith and fair dealing, breach of contract, unjust enrichment, or insurance bad faith. The ultimate decisions may have further implications on how these concepts are interpreted for use of AI systems.

Arnold v. Target Corp: This case is not at federal level but utilizes the Illinois Biometric Information Privacy Act (BIPA). If a company is to collect, use or store an individual's biometric data in the State of Illinois, the law requires private companies to obtain written consent prior to such data actions. The plaintiffs allege that "Target Corp. violated BIPA in possessing, collecting, and disclosing their biometric data (face geometry captured by facial recognition technology in Target stores). The Court denied Target's motion to dismiss on the basis that plaintiffs' claims were plausible."[93] The case is ongoing.

Importance: This case is one of the latest examples of BIPA litigation. Since its adoption in 2018, plaintiffs utilizing BIPA protections have been successful in both individual and class action lawsuits. BIPA is likely to be a blueprint for other states advancing privacy protections and governing biometric data collection.

Clearview AI, Inc. consumer privacy class action: Eleven cases were brought against Clearview since 2020. These cases include allegations of unlawful collection of biometric data, violations of BIPA, violating privacy and civil rights of the plaintiffs, and unlawful scraping and profiting of photographs online. In 2025, the Court approved a class action settlement agreement filed nationwide (with Illinois, California and New York as sub-classes due to the individual cases that were filed in these states). Instead of monetary damage payment, the settlement provides members of the class action equity ownership in Clearview AI.[94]

Importance: Clearview AI is banned in Canada, Australia, and several countries in Europe, as the data protection authorities found it to be in violation of the General Data Protection Regulation (GDPR). These countries include Austria, Belgium, Germany. Some other countries

[91] Court Listener. Estate of Gene B. Lokken, The v. UnitedHealth Group, Inc. (0:23-cv-03514) https://www.courtlistener.com/docket/68006832/estate-of-gene-b-lokken-the-v-unitedhealth-group-inc/
[92] Other cases are Barrows et al. v. Humana, Inc., and Kisting-Leung et al. v. Cigna Corporation et al.
[93] Bradford Newman and Adam Aft (Aug 2025)
[94] George Washington University. GW Law ETI AI Litigation Database. In Re Clearview Litigation. https://blogs.gwu.edu/law-eti/ai-litigation-database/case-detail-page/?in-re-clearview-litigation&pid=48

issued fines against Clearview AI such as France, Greece, Italy. While Clearview AI is not fully banned in the U.S., the settlement "permanently bans it from making its faceprint database available to most businesses and other private entities nationwide."[95] The case is important for those companies building products on biometric data.

Louis v. SafeRent Solutions, LLC: The two plaintiffs alleged that SafeRent's tenant-screening algorithm produced outcomes which had disproportionate negative effect on Black, Hispanic, and low-income housing voucher holders. The plaintiffs claimed this was a violation of the Fair Housing Act. Plaintiffs also added two classes to their lawsuit - all rental applicants using publicly funded housing vouchers but were denied housing in Massachusetts due to SafeRent Score, and all Black and Hispanic rental applicants within above category. The class action settlement has been reached in 2024, where SafeRent agreed to pay up to $2.275 million in settlement compensation. SafeRent also agreed to modify its screening methods for at least five years.[96]

Importance: The case highlights the importance of bias testing, especially in regulated domains.

In addition to predictive AI systems or automated decision-making systems, companies should also pay attention to litigation involving generative AI technologies.

Montoya v. Character Technologies: The case is filed by the parents of a teen who committed suicide after engagement with Character's AI chatbots. The parents, filing a wrongful death lawsuit, allege that the chatbot manipulated the teen and subjected to sexual abuse leading to mental health decline and the suicide. The plaintiffs argue that the company "launched these products without adequate safety features and with knowledge of the inherent dangers."[97]
The case is ongoing.

Importance: The case may require AI vendors to be more responsible about the impact of their products and establish accountability for harm. Several lawsuits are ongoing involving parents of minors impacted by chatbots and the companies deploying such products.[98]

---

[95] American Civil Liberties Union. ACLU v. Clearview AI. May 11, 2022. https://www.aclu.org/cases/aclu-v-clearview-ai

[96] Civil Rights Litigation Clearinghouse. Case: Louis v. SafeRent Solutions, LLC. https://clearinghouse.net/case/45888/

[97] Court Listener. Montoya v. Character Technologies, Inc. (1:25-cv-02907). https://www.courtlistener.com/docket/71355059/montoya-v-character-technologies-inc/

[98] Some example lawsuits are Raine, et al. v. OpenAI, Inc. ; Garcia v. Character Technologies; A.F., on behalf of J.F. v. Character Technologies, Inc.; E.S. v. Character Technologies, Inc.; Garcia v. Character Technologies

The next set of lawsuits focus on questions of copyright protection and use of a person's likeness (image, voice, style). The proliferation of generative AI models since 2022 has given rise to a similar explosion in the lawsuits. There are now too many copyright-related lawsuits for the purposes of this report. The following is a selected subset of the major cases which demand attention. Copyright cases mostly focus on whether use of copyrighted material for AI model training constitutes 'fair use' of those materials, and whether the training process is 'transformative' of such copyrighted works.

Bartz v Anthropic PBC (later class action): Three authors initially claimed that Anthropic had downloaded books from online libraries with pirated copies of copyrighted books. Evidence showed that the company had both purchased and digitized physical books and downloaded pirated books. Judge ruled that Anthropic' s digitization of physical purchased books and creation of a central digital library was fair use. The judgement also ruled that the use of copyrighted material to train its models was highly transformative and as such considered fair use. However, the use of pirated works was not fair use, thus requiring further litigation. [99] The case was later certified as a class action by the judge to cover all materials in the pirated datasets. Anthropic agreed to pay $1.5 billion into the settlement fund.

Importance: The settlement opens further questions on the context of training material acquisition and use of copyrighted material. Developers need to answer how the datasets containing protected material were acquired, the purpose of transformation of materials, and the impact or harm such transformation may bring on the original content creators.

Amazon v Perplexity: Amazon claims that Perplexity's automated agent system is intentionally disguised as a human-operated browsing activity, thus undermining privacy and data protection safeguards for its customers. The case is ongoing.

Importance: The case involves the use of agentic AI features which are expected to become more prevalent in the future. Agentic AI systems work to complete the user's objectives by breaking down the goal into smaller tasks and completing such tasks mostly without human intervention and supervision. In this case, an agentic system can take the user instruction "buy grocery items necessary for recipe of xyz" and complete such orders (including the payment) on Amazon's marketplace. The result of this case may impact how such agentic systems are deployed for commercial activities (especially as they have cybersecurity, data protection, consent, fraud, and liability implications).

[99] Court Listener. Bartz v. Anthropic PBC (3:24-cv-05417). https://www.courtlistener.com/docket/69058235/bartz-v-anthropic-pbc/; George Washington University. GW Law ETI AI Litigation Database. Bartz v. Anthropic PBC. https://blogs.gwu.edu/law-eti/ai-litigation-database/case-detail-page/?pid=251

Consolidated cases of copyright infringement against OpenAI and Microsoft: 12 separate lawsuits against these companies were consolidated into one.[100] The case is ongoing.

Importance: The result of the consolidated case will have significant impact on setting precedent on copyright infringement claims, and the ability of the original content owners to have future licensing agreements with AI companies.

Andersen v. Stability AI Ltd: The plaintiffs, a group of visual artists, allege that defendants (Stability AI Ltd. Stability AI Inc., Midjourney Inc., and DeviantArt Inc.) used their creative works without permission train an image generation tool. The judge found the copyright infringement allegation plausible, allowing the claims to proceed, finding.[101]

Importance: The image generation tool in question uses a different method (diffusion) to those training methods litigated in above examples. The case is also the first copyright protection claim for image-based tools. The case is still ongoing.

Other copyright infringement cases which will be worth following are: The New York Times v Microsoft and OpenAI, The Intercept v Microsoft and OpenAI, The Authors Guild v Microsoft and OpenAI, and Getty Images v Stability AI.

A final consideration is the ability for companies to insure their AI products against liability claims. Major insurers such as AIG, Great American and WR Berkley seek permission from the U.S. regulators on the possibility to exclude liabilities tied to businesses deploying AI tools (including chatbots and agents).[102] No decision or guidance from regulators is yet published. The insurance companies above have not yet implemented such exclusions. However, one can easily see a scenario where cybersecurity policies set precedent. In the future, insurers may require certain AI risk management and governance mechanisms to be in place for full coverage or base their pricing according to the maturity of the client's AI risk management. [103]

---

[100] As per GW Law ETI AI Litigation Database, the cases include Authors Guild v. OpenAI, Alter v. OpenAI, New York Times v. Microsoft, Basbanes v. Microsoft, Raw Story Media v. OpenAI, The Intercept Media v. OpenAI, Daily News v. Microsoft, The Center for Investigative Reporting v. OpenAI, Tremblay v. OpenAI, Silverman v. OpenAI, Chabon v. OpenAI, Millette v. OpenAI. https://blogs.gwu.edu/law-eti/ai-litigation-database/case-detail-page/?pid=309

[101] GW Law ETI AI Litigation Database. Andersen v. Stability AI Ltd. https://blogs.gwu.edu/law-eti/ai-litigation-database/case-detail-page/?andersen-v-stability-ai-ltd&pid=82

[102] Lee Harris and Cristina Criddle. Insurers retreat from AI cover as risk of multibillion-dollar claims mounts. The Financial Times (Nov 23, 2025)

[103] Merve Hickok. Why insurance companies should encourage solid AI risk management instead of excluding it. OECD The AI Wonk blog. December 17, 2025. https://oecd.ai/en/wonk/why-insurance-companies-should-encourage-solid-ai-risk-management-instead-of-excluding-it

Regulatory investigations

As noted previously, independent regulatory agencies are mandated to uphold civil rights and consumer protection, and supervise products and private sector business behavior in certain sectors. While the investigative priorities of the agencies may change from one administration to another, these entities are still accountable to enforce their mandates. Congress has oversight powers over these agencies and can supervise implementation via review, monitoring, investigations and use of the appropriations (allocation of funds) process.[104]

For example, the FTC has previously launched Operation AI Comply, taking action against multiple companies that have relied on AI and conducted deceptive or unfair acts that harm consumers.[105]

- **DoNotPay:** "According to the FTC's complaint, DoNotPay promised that its service would allow consumers to "sue for assault without a lawyer" and "generate perfectly valid legal documents in no time." DoNotPay also claimed that its robot lawyer could replace a human lawyer with its expertise. The FTC alleged that the "company did not conduct testing to determine whether its AI chatbot's output was equal to the level of a human lawyer, and that the company itself did not hire or retain any attorneys." The company eventually agreed to a Commission Order which prohibits it from making similar claims without any evidence. The company also agreed to "pay $193,000, provide a notice to consumers who subscribed to the service between 2021 and 2023 warning them about the limitations of law-related features on the service."[106]

- **Ascend Ecom:** The FTC filed a lawsuit against the company which alleged that "its 'cutting edge' AI-powered tools would help consumers quickly earn thousands of dollars a month in passive income by opening online storefronts." The FTC claimed that customers were defrauded of at least $25 million.[107] A federal court temporarily halted the scheme and put it under the control of a receiver.

- **Ecommerce Empire Builders (EEB):** The company claimed that it could help consumers build an "AI-powered Ecommerce Empire" where they could "Skip the guesswork and

[104] The United States Congress. Congressional Oversight and Investigations. https://www.congress.gov/crs-product/IF10015
[105] The Federal Trade Commission. FTC Announces Crackdown on Deceptive AI Claims and Schemes. September 25, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes
[106] Ibid
[107] The Federal Trade Commission. FTC Case Leads to Order Banning Ascend Ecom and Its Owners from Business Opportunity Marketing. June 23, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/06/ftc-case-leads-order-banning-ascend-ecom-its-owners-business-opportunity-marketing

start a million-dollar business today" by harnessing the "power of artificial intelligence.""[108] The FTC claimed that customers were defrauded due to these unsubstantiated claims. Another company, **FBA Machine,** with similar promises of guaranteed income through online storefronts utilizing AI was charged by the FTC.[109] In both cases, a federal court temporarily halted the schemes of each company, and put them under the control of a receiver. Both these cases were preceded by the settlement with **Automator AI**, whose owners had claimed they had a "proven system" and the powers of AI to help others make "passive investment income" in online storefronts. The settlement required the owners to pay monetary fine of $21.8 million and prohibits them from making deceptive earnings claims without evidence.[110]

- **Rytr LLC:** The company marketed an AI writing tool where subscribers could generate an unlimited number of detailed consumer testimonials and reviews on the products they themselves were selling. The FTC alleged that such generated reviews "would deceive potential consumers who were using the reviews to make purchasing decisions," and that "at least some of Rytr's subscribers used the service to produce hundreds, and in some cases tens of thousands, of reviews potentially containing false information."[111] The FTC claims "Rytr engaged in an unfair business practice by offering a service that is likely to pollute the marketplace." The Commission order "prohibits Rytr from engaging in similar illegal conduct in the future. It also bars the company from advertising, promoting, marketing, or selling any service dedicated to – or promoted as – generating consumer reviews or testimonials."[112]

[108] The Federal Trade Commission. FTC Announces Crackdown on Deceptive AI Claims and Schemes. September 25, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

[109] The Federal Trade Commission. FTC Obtains Permanent Ban of E-Commerce Business Opportunity Scheme Operator. July 30, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-FTCvFBAMachine-et-al.pdf

[110] The Federal Trade Commission. FTC Action Leads to Ban for Owners of Automators AI E-Commerce Money-Making Scheme. February 27, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-action-leads-ban-owners-automators-ai-e-commerce-money-making-scheme

[111] The Federal Trade Commission. FTC Announces Crackdown on Deceptive AI Claims and Schemes. September 25, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

[112] The Federal Trade Commission. FTC Approves Final Order against Rytr, Seller of an AI "Testimonial & Review" Service, for Providing Subscribers with Means to Generate False and Deceptive Reviews. December 18, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-approves-final-order-against-rytr-seller-ai-testimonial-review-service-providing-subscribers

In December 2025, the FTC reopened and set aside the Rytr final consent order, noting that the previous condemnation of the company (because its technology could be potentially misused by others) is not consistent with FTC's mandate.[113]

In addition to Operation AI Comply, we have also seen several enforcement action and settlement deals which set precedent for companies on the kind of behavior to avoid. The following provides examples of actions which can be instructive for any company looking to conduct business in the U.S.:

- **Evolv Technologies:** The FTC alleged that Evolv made false claims about its AI-powered security screening system and sensor technology. The company claimed the product could detect weapons and differentiate these from harmless personal items, reduce false alarm rates and reduce labor costs.[114] Evolv's products were used in many schools, hospitals and event venues. In the settlement, the company is banned from making such misleading claims without robust evidence and notifying some school customers that they can cancel contracts if they wish without penalty.[115]

- **IntelliVision:** The FTC alleged that IntelliVisions's claim that its facial recognition software operated without bias for race or gender was false and unsubstantiated. The company's products did perform differently across different demographics, and they were not adequately tested. The final settlement bars IntelliVision from making false or misleading claims about its AI technology and requires it to rely on reliable testing and evidence.[116]

- **RiteAid:** The FTC charged RiteAid for failing to take reasonable measures to prevent harm to consumers with its use of AI-based facial recognition technology deployed to detect shoplifting or problematic behavior. Some customers were erroneously accused by employees of wrongdoing due to errors (false-positive matches) in the software. RiteAid has been prohibited from using FRT for surveillance purposes for five years. The

[113] The Federal Trade Commission. FTC Reopens and Sets Aside Rytr Final Order in Response to the Trump Administration's AI Action Plan. December 22, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-reopens-sets-aside-rytr-final-order-response-trump-administrations-ai-action-plan
[114] The Federal Trade Commission. Evolv Technologies. March 11, 2025. https://www.ftc.gov/legal-library/browse/cases-proceedings/evolv-technologies
[115] The Federal Trade Commission. FTC Takes Action Against Evolv Technologies for Deceiving Users About its AI-Powered Security Screening Systems. November 26, 2024. https://www.ftc.gov/news-events/news/press-releases/2024/11/ftc-takes-action-against-evolv-technologies-deceiving-users-about-its-ai-powered-security-screening
[116] The Federal Trade Commission. Intellivision, In the Matter of. January 13, 2025. https://www.ftc.gov/legal-library/browse/cases-proceedings/232-3023-intellivision-matter

company is also required to delete all collected facial images/videos and destroy all related models or algorithms derived from the data.[117]

In the majority of enforcement actions, the cases are brought against companies which make misleading, deceptive, false or unsubstantiated claims regarding their AI products. This means that the capability of the AI system as it is advertised must be substantiated with evidence.

There are also a few ongoing investigations into AI companies which may have important implications for the industry:

- **OpenAI investigation:** In March 2023, the Center for AI and Digital Policy (CAIDP) filed an extensive complaint to the FTC on OpenAI, arguing that OpenAI released GPT-4 despite knowing about risks, violating FTC guidance. CAIDP requested an investigation into the vendor. CAIDP raised concerns about bias, children safety, consumer protection, cybersecurity, deception, transparency, privacy, and public safety.[118] At the beginning of July 2023, CAIDP followed with a supplemental complaint.
  In mid-July, the New York Times[119] and The Wall Street Journal[120] reported that the FTC sent a civil investigative demand letter to OpenAI,[121] and had opened the investigation CAIDP requested. In November 2023, CAIDP filed another supplemental complaint, urging the FTC to issue an order to establish safeguards and guardrails for ChatGPT.[122] The investigation is still ongoing.

[117] The Federal Trade Commission. Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards. December 19, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[118] The Center for AI and Digital Policy. *Complaint and Request for Investigation, Injunction, and Other Relie*f - OpenAI. March 30, 2023. https://www.caidp.org/app/download/8450269463/CAIDP-FTC-Complaint-OpenAI-GPT-033023.pdf . Disclosure: The author is the President of CAIDP.

[119] Cecilia Kang and Cade Metz. F.T.C. Opens Investigation Into ChatGPT Maker Over Technology's Potential Harms. The New York Times. July 13, 2023. https://www.nytimes.com/2023/07/13/technology/chatgpt-investigation-ftc-openai.html

[120] John D. McKinnon and Ryan Tracy. ChatGPT Comes Under Investigation by Federal Trade Commission. The Wall Street Journal. July 13, 2023. https://www.wsj.com/tech/chatgpt-under-investigation-by-ftc-21e4b3ef

[121] The Federal Trade Commission. Civil Investigative Demand Schedule – FTC File: 232-3044. https://www.caidp.org/app/download/8467488463/FTC-CID-OpenAI-CAIDP.pdf

[122] The Center for AI and Digital Policy. In the Matter of OpenAI - Second Supplement to the Complaint. November 14, 2023. https://www.caidp.org/app/download/8485816363/CAIDP-Supplement-FTC-OpenAI-11142023.pdf

- **Instacart investigation:** Following investigative journalist report of Instacart showing shoppers different prices for the same grocery items,[123] Reuters reported that the FTC is asking for information from Instacart regarding its Eversight pricing tool. [124] The FTC sent a civil investigative demand letter to the company.

- **Snapchat referral:** In January 2025, the FTC referred a complaint about Snap, and its chatbot My AI, to the Department of Justice. The Commission alleges the product results in "risks and harms to young users of the application" and noting that a "proceeding is in the public interest."[125] The case is still open.

An important thing to also note is that the now Chair Ferguson, had concurrent opinions on some of the above cases while he was an FTC Commissioner. The FTC's new Chair Andrew Ferguson will no doubt have pressure from the Administration. However, he also stated the agency will "regulate AI claims through its existing consumer protection authorities," enforcing "existing laws against illegal conduct when it involves AI no differently than when it does not".

The approach emphasizes:
- No AI exemption from consumer protection laws
- Substantiation requirements for all AI-related claims
- Prohibition of AI-enabled deceptive or unfair practices
- Algorithmic disgorgement (mandated deletion of unlawfully trained algorithms)

In fact, since the start of the new Administration, the FTC took following actions:

- **Workado LLC:** The FTC alleged that Workado's claim about high performance of its product to detect AI-generated content was false. The suggested accuracy or efficacy of AI product did not have competent and reliable evidence. The settlement prohibits Workado from making misleading representations and requires the company to email eligible consumers to inform them about the Commission settlement.[126]

[123] Groundwork Collaborative, Consumer Reports, and More Perfect Union. Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout. December 9, 2025. https://groundworkcollaborative.org/work/instacart/
[124] Jody Godoy. Exclusive: FTC probes Instacart's AI pricing tool, source says; shares drop. Reuters. December 17, 2025. https://www.reuters.com/legal/litigation/ftc-investigating-instacarts-ai-pricing-tool-source-says-2025-12-17/
[125] The Federal Trade Commission. Statement of the Federal Trade Commission In the Matter of Snap, Inc. Matter No. 2323039. January 16, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/commission-statement-snap.pdf
[126] The Federal Trade Commission. FTC Approves Final Order against Workado, LLC, Which Misrepresented the Accuracy of its Artificial Intelligence Content Detection Product. August 28, 2025. https://www.ftc.gov/news-

- **Air AI:** Air AI claims that its "conversational AI" can replace human customer service representatives and lead to significant profits. The FTC alleges that Air AI is making false, deceptive, and unsubstantiated claims about business growth, earnings potential, and refund guarantees.[127] The complaint is filed in the U.S. District Court for the District of Arizona.

- **Inquiry into AI Chatbots Acting as Companions:** The FTC is collecting information from seven companies that provide consumer-facing AI-powered chatbots. The FTC is looking to understand how these companies "measure, test, and monitor potentially negative impacts of this technology on children and teens," and how they monetize the data collected from users.[128]

The Securities Exchange Commission also has enforcement action against companies with deceptive and misleading claims:

- **Albert Saniger:** The SEC charged the former CEO of Nate, Inc. for fraudulently soliciting investments in its AI product, and "raising over $42 million through the sale of Nate stock by making false and misleading statements about the company's use of AI."[129] Saniger misled the investors that the AI-powered product completes purchases made through its app without any human involvement. However, the purchase orders were mostly completed by contract employees who manually completed received orders. The SEC "seeks permanent injunctions, conduct-based injunctions, an officer-and-director bar, disgorgement with prejudgment interest, and civil penalties."

  In a parallel case, the DOJ also charged Saniger for making materially false and misleading statements about company's AI systems and its capabilities. The AI system was portrayed as "fully automated and scalable."[130]

events/news/press-releases/2025/08/ftc-approves-final-order-against-workado-llc-which-misrepresented-accuracy-its-artificial

[127] The Federal Trade Commission. FTC Sues to Stop Air AI from Using Deceptive Claims about Business Growth, Earnings Potential, and Refund Guarantees to Bilk Millions from Small Businesses. August 25, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-sues-stop-air-ai-using-deceptive-claims-about-business-growth-earnings-potential-refund

[128] The Federal Trade Commission. FTC Launches Inquiry into AI Chatbots Acting as Companions. September 11, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions. The companies are Alphabet, Character Technologies, Instagram, Meta, OpenAI, Snap, and X.AI Corp.

[129] The Securities and Exchange Commission. Alberto Saniger Mantinan, a/k/a Albert Saniger. April 11, 2025. https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26282

[130] The Department of Justice. United States v Albert Saniger. https://www.justice.gov/usao-sdny/media/1396131/dl?inline

- **Delphia (USA) Inc. and Global Predictions Inc:** The SEC settled with these two investment companies for their misleading claims. Delphia falsely claimed, "use of AI and machine learning that incorporated client data in its investment process." And Global Predictions "falsely claimed to be the 'first regulated AI financial advisor' and misrepresented that its platform provided "[e]xpert AI-driven forecasts."[131] Delphia settled to pay $225,000, while Global Predictions agreed to pay $175,000 as civil penalties.

- **Presto Automation Inc.:** The SEC settled with the restaurant-technology company for making materially false and misleading statements about its AI speech-recognition software (Presto Voice). As per the SEC, the company "failed to disclose that, for a period of time, the AI speech recognition technology in all units of Presto Voice that the company had then deployed was owned and operated by a third party," and that it also "falsely claimed that its own AI product eliminated the need for human order-taking." It was found that human intervention was necessary for majority of drive-thru orders placed through the software.[132]

- **Ilit Raz:** The SEC charged the CEO and founder of AI recruitment startup Joonko for "defrauding investors of at least $21 million by making false and misleading statements about the quantity and quality of Joonko's customers, the number of candidates on its platform, and the company's revenue."[133]

The SEC will continue acting against public companies and investment advisors engaging in AI-washing. It is critical for AI companies to be transparent and accurate in their statements to customers and investors. Senior SEC officials reiterated this focus in May 2025, noting the SEC will continue to look at "whether there's transparency around the technology, whether it's described accurately, whether there's responsible communications to customers."[134]

[131] The Securities and Exchange Commission. SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence. March 18, 2024. https://www.sec.gov/newsroom/press-releases/2024-36

[132] The Securities and Exchange Commission. SEC Charges Restaurant-Technology Company Presto Automation for Misleading Statements About AI Product. January 14, 2025. https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11352-s

[133] The Securities and Exchange Commission. SEC Charges Founder of AI Hiring Startup Joonko with Fraud. June 11, 2024. https://www.sec.gov/newsroom/press-releases/2024-70

[134] Jonathan D. Uslaner and Alec Coquin. 'AI washing': regulatory and private actions to stop overstating claims. Reuters. May 30, 2025. https://www.reuters.com/legal/legalindustry/ai-washing-regulatory-private-actions-stop-overstating-claims-2025-05-30/

As mentioned before, SEC's priorities include fraud committed using AI; use of social media, the dark web, or false websites to perpetrate fraud; and hacking to obtain material nonpublic information. These priorities can take more significance in the future where deepfakes can be used to fraud companies and investors, or where agentic AI systems can be manipulated via prompt injections to extract nonpublic information.

The Equal Employment Opportunity Commission so far charged one company for employment related discrimination charges:

- **iTutorGroup:** The EEOC filed a complaint against the recruitment company alleging it "intentionally discriminated against older applicants because of their age."[135] The company agreed on paying $365,000 to over 200 job candidates who were impacted by iTutor's automatic decision.

It is clear from all regulatory activity that the focus has been on misleading and deceptive claims to consumers and investors, as well as discriminatory results. Most of the regulatory investigations and settlements involve false claims about an AI tool's capability, scalability, profit returns, or ability to automate tasks previously completed by humans.

Key legal considerations for Japanese companies exporting AI products to the U.S.

This section focuses on the policy proposals from U.S. AI Action Plan and the relevant orders. It is not intended as legal advice on trade legislation.

AI Action Plan

The current Trump administration frames the global AI engagement as one of 'race,' particularly in relation to China. This means the policy assessments are mainly conducted through an economic and national security lens. The Plan aims to prevent or slow down future regulations which may impact development of datacenters, deployment or export of AI stack. Framing AI as a national security imperative seeks to establish federal supremacy over state AI regulation. Such positioning can also reduce the challenges against these AI policies. The

[135] The Equal Employment and Opportunities Commission. iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit. September 11, 2023. https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit

Administration frames regulatory oversight of AI not as consumer protection mechanism, but as possible obstacle to American competitiveness.

The Plan also requires Federal agencies to revise or remove guidance already in place if such guidance conflicts with Administration's policy objectives. The Administration's "Winning the AI Race: America's AI Action Plan"[136] details federal government's plans under three strategic pillars:

- *Accelerating Innovation*

    - All Federal agencies are instructed to " identify, revise, or repeal regulations, rules, memoranda, administrative orders, guidance documents, policy statements, and interagency agreements that unnecessarily hinder AI development or deployment."[137]
    - Federal Trade Commission (FTC), while an independent agency, is instructed not to "unduly burden AI innovation."
    - Other Federal agencies are instructed to evaluate State-level legislative environment when making funding decisions.

    At the same time, this pillar also encourages advancements in open-source, and AI evaluation and governance methods.

    - Freely available and modifiable open-source and open-weight AI models ("founded on American values") are encouraged.
    - Procurement guidelines should be updated to ensure acquisition of objective and bias-free large language models (LLMs).
    - The Food and Drug Administration (FDA), the Securities and Exchange Commission (SEC), with support from the NIST, are recommended to establish regulatory sandboxes or AI Centers of Excellence.
    - Funding to advance AI evaluation methods, interpretability, AI control systems, and adversarial robustness are prioritized.

[136] The White House. White House Unveils America's AI Action Plan. July 23, 2025. https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/

[137] These deregulatory instructions are also in alignment with Executive Order 14192 - Unleashing Prosperity Through Deregulation. January 31, 2025.https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-prosperity-through-deregulation/

- Building American AI Infrastructure
    - Similar to the first pillar, regulations on construction and permitting of datacenters and power generation infrastructure are expected to be eased.
    - Removing restrictions or policy requirements for especially semiconductor manufacturing programs are prioritized.

  This pillar also encourages funding and research to keep AI models and their infrastructure secure:
    - Secure-by-design, robust, and resilient AI systems are encouraged as they also enable detection of performance shifts, and adversarial attacks.
    - AI incident reporting, and ability to learn from vulnerabilities is critical for secure systems. The Plan recommends establishment of AI incident standards, response frameworks, best practices, and technical capabilities.
    - Plan recommends development of an "AI Procurement Toolbox."

- Leading in International Diplomacy and Security
    - Since AI is defined within an "AI Race" framework, this pillar focuses on the U.S. exporting its full AI technology stack (hardware, models, software, applications, and standards) to counter Chinese stack.
    - AI Compute export control enforcement is to be strengthened.

The AI Action Plan, however, does not set any deadlines or a priority structure on any of these policy recommendations. Therefore, it is not clear which of these actions will be funded or advanced in what time frame.

Exporter of AI products to the U.S. should pay attention to utilizing ideally open-source software and/or models, as well as American technology stack. Products with Japanese models should be cautious about not including any components from the People's Republic of China for alignment with Chinese Communist Party, or its values. The Action Plan proposes Department of Commerce, through the NIST's Center for AI Standards and Innovation (CAISI), conduct evaluations of frontier models from PRC. The evaluation from CAISI responding to this request is already published.[138]

Companies engaged in datacenter construction or semiconductor exports should focus on the specific EOs and the Department of Commerce's ongoing guidance on these topics.

[138] The Center for AI Standards and Innovation. CAISI Evaluation of DeepSeek AI Models Finds Shortcomings and Risks. September 30, 2025.
https://www.nist.gov/system/files/documents/2025/09/30/CAISI_Evaluation_of_DeepSeek_AI_Models.pdf

Genesis Mission

A major action taken to implement the AI Action Plan is the launch of the Genesis Mission. This initiative unsurprisingly also highlights a "race for global technology dominance in the development of AI." The Mission will "build an integrated AI platform to harness Federal scientific datasets," using national high-performance computing resources and resources available through industry partners, to train scientific foundation models and create AI agents accelerate scientific breakthroughs.[139]

The Administration compares this effort to that of Manhattan Project to signal ambitions. On the other hand, the actual outcomes for the research communities and the public currently remain vague. The launch document provides a single reference to collaboration with universities, while the focus is mostly on private sector partnerships. The direction of scientific research is likely to be controlled centrally or at least dominated by the Department of Energy and the White House Office of Science and Technology Policy, with a focus on commercialization.

The Mission website notes this to be a 'national mission' yet does not mention any public input or visibility mechanisms. Neither is there any reference to independent reviews or oversight.[140] The website further states that the platform will "accelerate discovery science, strengthen national security, and drive energy innovation."[141]

OMB Memorandums

The Office of Management and Budget's guidance to federal agencies is critical. While the guidance is only binding on the federal government, the requirements can act as a norm-setting tool for private sector due to the expectations from federal contractors.

The OMB Memorandum M-25-21 on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust: [142]

Scope: Provides guidance on how federal agencies should use and govern AI systems; requires agencies to elevate AI adoption and innovation as a priority, while increasing transparency

[139] The White House. Launching the Genesis Mission. November 24, 2025. https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/
[140] The Department of Energy. Genesis Mission. https://genesis.energy.gov/
[141] Ibid
[142] Executive Office of the President, Office of Management and Budget. Memorandum M-25-21 on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust. April 3, 2025. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

Requirements:

- appropriately resource data governance, information technology (IT), infrastructure, quality data assets, integration and interoperability, accessibility, privacy, confidentiality, and security
- enable an AI-Ready Federal Workforce
- appoint Chief AI Officer, Agency AI Governance Board
- update AI use case inventories, develop compliance plans and agency AI strategies
- implement minimum risk management practices for AI that could have significant impacts when deployed ("high-impact AI")
- high-impact AI is defined as *"AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on: 1. an individual or entity's civil rights, civil liberties, or privacy; or 2. an individual or entity's access to education, housing, insurance, credit, employment, and other programs; 3. an individual or entity's access to critical government resources or services; 4. human health and safety; 5. critical infrastructure or public safety; or 6. strategic assets or resources"*
- minimum risk management practices include *pre-deployment testing, AI impact assessment, ongoing monitoring for performance and potential adverse impacts, human oversight, fail-safe mechanisms, and remedy/appeal process.*

The OMB Memorandum M-25-22 on Driving Efficient Acquisition of Artificial Intelligence in Government:[143]

Scope: Provides guidance on how federal agencies should procure AI responsibly

Requirements:

- maximize the use of AI products and services that are developed and produced in the United States
- protect privacy, IP rights and use of government data
- avoid vendor lock-in and promote competition
- prioritize obtaining documentation that facilitates transparency and explainability

[143] Executive Office of the President, Office of Management and Budget. Memorandum M-25-22 on Driving Efficient Acquisition of Artificial Intelligence in Government. April 3, 2025. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf

The OMB Memorandum M-26-04 on Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles:[144]

Scope: Provides guidance on how federal agencies should procure Large Language Models (LLMs)

Requirements:

- LLMs shall prioritize historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory.
- LLMs shall be neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas

As noted before, the OMB memos are only binding on the federal government procurement, use and governance of AI and not the private sector. However, they do have the soft power impact of setting the expectations and norms for private sector such as those laid out in the federal procurement requirements.[145] The author testified in the U.S. Congress in 2023, urging the Congress to enact legislation for AI governance, to promote algorithmic transparency, limit algorithmic bias, and advance trustworthy AI. The author also provided several recommendations for the OMB to pass guidance on federal procurement of AI.[146]

As can be seen from the above requirements, the OMB still prioritizes necessary risk management tools such as documentation, testing, impact assessments, ongoing monitoring, cybersecurity controls, as well as principles such as explainability, interpretability, robustness, and human oversight.

Comparative analysis of state-level AI legislation across representative states

States are the most active parties in AI legislation. State lawmakers are more directly connected to their electoral base, and the public pressure can be more direct at that level. This

[144] Executive Office of the President, Office of Management and Budget. Memorandum M-26-04 on Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles. December 11, 2025. https://www.whitehouse.gov/wp-content/uploads/2025/12/M-26-04-Increasing-Public-Trust-in-Artificial-Intelligence-Through-Unbiased-AI-Principles-1.pdf

[145] Center for AI and Digital Policy. AI Policy Sourcebook 2025. https://www.caidp.org/resources/ai-policy-sourcebook/

[146] The U.S. Congress. House Oversight Committee Subcommittee on Cybersecurity, Information Technology, and Government Innovation. Merve Hickok testimony in hearing “Advances in AI: Are We Ready For a Tech Revolution?” March 8, 2023. https://www.caidp.org/events/in-congress-house-oversight/

allows for policy responses to move more rapidly. In the absence of federal level AI legislation, state legislatures respond to the growing pressure and concern from their constituencies.

The Democrat and Republican states alike enact laws to ensure civil rights and consumer protection, as well as product safety. The current legislative trends show significant focus on use and disclosure of synthetic (generated) outputs, as well as liability rules for high-impact domains. According to the National Conference of State Legislatures (NCSL), consumer protection, deepfakes and government use of AI lead in the legislative trends.[147]

While the current Administration walks in tandem with the major technology companies, the state legislators reject the narrative that AI safeguards hinder the development, deployment, and adoption of AI. The current Administration argues that reduced oversight lowers business costs and boosts economic growth. On the other hand, the states' civil rights and consumer protection argument emphasizes the importance of rules in ensuring fair practices, fair competition, maintaining safety standards, and preventing market failures or consumer exploitation. The AI-specific legislation originates from the states where constituencies demand safeguards for trustworthy AI systems, and smaller businesses, which lack the resources of Big Tech, demand legal clarity.

The following section provides details of the most consequential AI-related laws enacted laws across selected states as of end of 2025.

California

California leads the nation in both AI innovation and state-level AI legislation. As the fourth largest economy in the world, [148] California's legislative choices and strategy have impact beyond its borders in the wider regulatory environment.[149] So far Californian lawmakers preferred multiple targeted interventions addressing specific risks, rather than a comprehensive omnibus regulation on AI.[150]

---

[147] The National Conference of State Legislatures (NCSL). *3 Trends Emerge as AI Legislation Gains Momentum*, Jan. 23, 2025. https://www.ncsl.org/state-legislatures-news/details/3-trends-emerge-as-ai-legislation-gains-momentum

[148] Hannah Fry and Clara Harter. California overtakes Japan to become world's fourth-largest economy. But tariffs pose threat. April 24, 2025. Los Angeles Times. https://www.latimes.com/california/story/2025-04-24/californias-economy-overtakes-japan-to-become-4th-largest-in-world

[149] Marc Rotenberg. The California Effect: AI Redux Journal of AI Law and Regulation Volume 2, Issue 4. 2025. https://doi.org/10.21552/aire/2025/4/7

[150] Christabel Randolph. United States · California AI Policy: A Review of the 2025 Legislative Outcomes Journal of AI Law and Regulation Volume 2, Issue 4. 2025. https://doi.org/10.21552/aire/2025/4/16

In late 2024, Governor Newsom convened a group of world-leading AI academics and experts to report on the state AI models and recommend AI guardrails, based on an empirical, science-based analysis of the capabilities. The Joint California Policy Working Group on AI Frontier Models published the final report, California Report on Frontier AI Policy, in June 2025. [151] While the report itself does not have any legislative position, it does note that greater transparency "can advance accountability, competition, and public trust." The report also notes that "[I]n building a robust and transparent evidence environment, policymakers can align incentives to simultaneously protect consumers, leverage industry expertise, and recognize leading safety practices."[152]

AB 316 (AI defense):[153]

Target: developer of a generative artificial intelligence system or service
Scope: civil liability
Requirements:

- establishes that human accountability is paramount and a defendant who developed, modified, or used AI cannot assert a defense that the AI autonomously caused the harm to the plaintiff

Sanction: no further sanction is defined
Effective date: January 1, 2026

AB 325 (Preventing Algorithmic Price Fixing Act):[154]

Target: any person
Scope: algorithmic price fixing
Requirements:

- amends California's antitrust law
- prohibits restraining of commerce with use or distribution of a common pricing algorithm
- prohibits coercive practices a recommended price or term of conditions via a common pricing algorithm

Sanction: creates liability for coercion
Effective date: January 1, 2026

[151] R. Bommasani, S.R. Singer, R.E. Appel, S. Cen, A.F. Cooper, E. Cryst, L.A. Gailmard, I. Klaus, M.M. Lee, I.D. Raji, A. Reuel, D. Spence, A. Wan, A. Wang, D. Zhang, D.E. Ho, P. Liang, D. Song, J.E. Gonzalez, J. Zittrain, J.T. Chayes, M.F. Cuéllar, L. Fei-Fei. "The California Report on Frontier AI Policy." The Joint California Policy Working Group on AI Frontier Models. June 17, 2025. https://www.cafrontieraigov.org/
[152] Ibid
[153] The California Assembly Bill 316: https://legiscan.com/CA/text/AB316/id/3268860
[154] The California Assembly Bill 325: https://legiscan.com/CA/text/AB325/2025

AB 361 (Data brokers: data collection and deletion):[155]

Target: data brokers

Scope: data practice disclosures

Requirements:

- report to the CPPA and register with data broker status if they collect data on certain categories
- disclose whether collected data is shared or sold to certain actors (such as law enforcement, federal or state governments, foreign actor, or developer of a generative AI system)
- access the Delete Request and Opt-Out Platform (DROP) which allows a consumer to direct every data broker to delete consumer's personal information related to that consumer through a single verifiable request
- Beginning January 1, 2028, and every 3 years thereafter, data brokers must undergo an independent third party audit to determine compliance

Sanction: administrative fine of $200 for each day the data broker fails to register; administrative fine of $200 for each deletion request for each day the data broker fails to delete information

Effective date: January 1, 2026

AB 489 (Health care professions: deceptive terms or letters: artificial intelligence):[156]

Target: developers of AI or generative AI systems

Scope: professional healthcare practice

Requirements:

- prohibits false or misleading representations by using specified terms to indicate or imply possession of a professional healthcare practice license or certificate
- prohibits false or misleading representations that advice or assessments from AI are being provided by a person with a professional healthcare practice license or certificate

Sanction: expands the scope of existing crimes

Effective date: January 1, 2026

AB 621 (Deepfake pornography):[157]

Target: any person

Scope: protection of minors against nonconsensual deepfakes

Requirements:

[155] The California Senate Bill 361: https://legiscan.com/CA/text/SB361/id/3120338

[156] The California Assembly Bill 489: https://legiscan.com/CA/text/AB489/id/3268592

[157] The California Assembly Bill 621: https://legiscan.com/CA/text/AB621/id/3268979

- strengthen existing law by establishing that minors cannot consent to the creation
- and distribution of a sexually explicit material depicting themselves
- any person who "knowingly facilitates" or "recklessly aids or abets" the creation or intentional disclosure of nonconsensual deepfakes content is held liable – if they receive evidence that they are enabling such an operation and do not stop that service within 30 days.

Sanction: maximum statutory damages available to a depicted individual up to $50,000 if the violation was not malicious and $250,000 for a malicious violation and would authorize certain public attorneys to bring a civil action to enforce these provisions.

Effective date: January 1, 2026

AB 853 (California AI Transparency Act - *As Amended by AB 853 (2025):*[158]

Target: certain large online platforms and generative AI developers

Scope: transparency of provenance data

Requirements:

- provide an interface for users to access the generated content's provenance data
- starting January 1, 2028, "capture device manufacturers" (e.g., camera, mobile phone, audio recorder manufacturers, etc) are required to embed a latent disclosure in content captured by the device by default

Sanction: up to $5,000 per violation

Effective date: January 1, 2027. The bill also delays the operation of the California AI Transparency Act until August 2, 2026.

AB 1008 (Personal Information and AI Systems - amendment to the California Consumer Privacy Act (CCPA):[159]

Target: any business collecting consumer's personal information

Scope: amended to reiterate the definition of personal information in the California Consumer Privacy Act (CCPA), including requirements for notice, consent, and data subject rights (access, deletion, correction).

Requirements:

- reiterates that personal information within AI systems is still personal information, and therefore subject to existing CCPA obligations
- classifies AI systems as capable of outputting "personal information"

Sanction: No explicit penalties. Enforcement is expected through the CCPA.

Effective date: January 1, 2025

[158] The California Assembly Bill 853: https://legiscan.com/CA/text/AB853/id/3269811

[159] The California Assembly Bill 1008: https://legiscan.com/CA/text/AB1008/id/3013509

AB 1836 (Amendment to Deceased Personality Protections):[160]

Target: any person

Scope: production, distribution, making available digital replica of a deceased person

Requirements:

- expands existing post-mortem rights to include digital replicas of deceased persons
- unlawful to produce, distribute, or make available the digital replica of a deceased personality's voice or likeness in an expressive audiovisual work or sound recording without appropriate consent
- exemptions if the use is in connection with any news, public affairs, or sports broadcast or account; is for purposes of comment, criticism, scholarship, satire, or parody; is a representation of the individual as the individual's self in a documentary or in a historical or biographical manner; is fleeting or incidental; or if the use is in an advertisement or commercial announcement for further exemptions detailed in the law.

Sanction: Greater of $10,000 or the actual damage suffered by a person controlling the rights to the deceased personality's likeness.

Effective date: January 1, 2025

AB 2013 (Generative AI Training Data Transparency Act):[161]

Target: any entity—person, company, or government agency which develops or "substantially modifies" a generative AI system for use in California

Scope: training data transparency

Requirements:

- post information on the website about training data (including a high-level summary of the datasets used, the sources or owners of the datasets, a description of how the data is used, the number of data points in the set, whether copyrighted / IP protected or licensed data is included, and the time period the data was collected (among other information)
- information must be in place by on or before January 1, 2026, and before each time thereafter that a generative AI system or service is made publicly available, or a substantial modification is made

Sanction: No explicit penalties. Enforcement is expected through California's Unfair Competition Laws.[162]

Effective date: January 1, 2026

[160] The California Assembly Bill 1836: https://legiscan.com/CA/text/AB1836/id/3021237

[161] The California Assembly Bill 2013: https://legiscan.com/CA/text/AB2013/id/3023192

[162] Kevin D. DeBré, Stubbs Alderton & Markiles. The National Law Review. December 17, 2025. https://natlawreview.com/article/client-alert-new-ai-laws-will-prompt-changes-how-companies-do-business

AB 2602 (Replica of Voice or Likeness Law):[163]

Target: employers

Scope: contracts for personal or professional services to include digital replicas

Requirements:

- requires explicit, specific consent in contracts before employer can use a digital replica of a performer's voice or likeness for new performances
- prohibits broad clauses allowing digital replicas, and mandates representation by a union or legal counsel

Sanction: Enforcement through the California Labor Code.

Effective date: January 1, 2025

AB 2905 (AI Call Disclosures Law):[164]

Target: callers using an automatic dialing-announcing device

Scope: disclosure on use of AI to generate / alter voice

Requirements:

- inform the person receiving the call if the prerecorded message uses an artificial voice generated or significantly altered using AI

Sanction: criminal penalties for violations enforced by the California Public Utilities Commission

Effective date: January 1, 2025

AB 3030 (Healthcare services, AI):[165]

Target: healthcare providers

Scope: use of generative AI for communications

Requirements:

- requires a disclaimer indicating to the patient that a communication was generated by generative AI
- requires providing clear instructions describing how a patient may contact a human health care provider, employee, or other appropriate person.

Sanction: No specific penalties noted, but the entity would be subject to the disciplinary proceedings

Effective date: January 1, 2025

[163] The California Assembly Bill 2602: https://legiscan.com/CA/text/AB2602/id/3021235
[164] The California Assembly Bill 2905: https://legiscan.com/CA/text/AB2905/id/2981302
[165] The California Assembly Bill 3030: https://legiscan.com/CA/text/AB3030/id/2979649

SB 53 (Transparency in Frontier Artificial Intelligence Act):[166]

Target: developer of a foundation model (trained on greater than 10^26 FLOPS)

Scope: catastrophic risk *(foreseeable and material risk that the development, storage, use, or deployment of a frontier model will materially contribute to the death, or serious injury of more than 50 people, or generate material harm for more than 1 billion dollars)*

Requirements:

- public disclosure of AI safety report, including how national standards, international standards, and industry-consensus best practices were incorporated
- critical safety incident reporting (within 15 days of discovery, and within 24 hours in certain circumstances)
- no materially false or misleading statements about catastrophic risks of their models, or risk management practices
- whistleblower protection procedures and no intimidation
- large frontier model developers with over $500 million in annual revenue have additional reporting requirements

Sanction: civil penalty up to $1 million per violation

Effective date: January 1, 2026

SB 243 (Companion chatbots):[167]

Target: companion chatbot providers

Scope: child safety re companion chatbots

Requirements:

- recurring notifications to users that chatbot responses are not human and artificially generated
- implement protocols to prevent AI-generated content related to suicide or self-harm
- implement heightened safeguards for children to prevent conversations with minors about self-harm, sexually explicit content, or suicidal ideation

Sanction: establishes a private right of action; penalty of up to $1,000 per violation

Effective date: July 1, 2027

SB 926 (Amendment of California Law Governing Distribution of Intimate Images):[168]

Target: any person

Scope: intimate images

[166] The California Senate Bill 53: https://legiscan.com/CA/text/SB53/id/3270002

[167] The California Senate Bill 243: https://legiscan.com/CA/text/SB243/id/3269137

[168] The California Senate Bill 926: https://legiscan.com/CA/text/SB926/id/2999964

Requirements:

- distribution of intimate images is already prohibited
- prohibition now includes intentional creation and distribution of any sexually explicit image of another identifiable person
- if a reasonable person would believe the image to be an authentic image of the person depicted,
- where distributor knows or should know that the image will cause serious emotional distress, and the person depicted suffers that distress.

Sanction: criminal and civil penalties

Effective date: January 1, 2025

SB 942 (AI Transparency Act):[169]

Target: person or entity who produces AI-generated content that has over 1 million monthly visitors and is accessible within California
Exemptions exist for providers of non-user-generated video games, streaming content, movies, shows, or interactive experiences.

Scope: AI-generated / materially altered consumer-facing media content

Requirements:

- clear, conspicuous and appropriate disclosures that the content was AI-generated or altered
- offer users the ability to include a disclosure in content generated / altered
- provide users with an AI detection tool to assess whether content was created or altered by generative AI.

Sanction: allows for civil action by the California Attorney General's office or city/county counsel of $5,000 per violation.

Effective date: January 1, 2026

Updates to California Consumer Privacy Act Regulations:[170]

In addition to the new legislation introduced in California, the Privacy Protection Agency also announced in 2025 updates to its regulations. The changes are focused on automated decision-making technology (ADMT), privacy risk assessments, and cybersecurity audits.

[169] The California Senate Bill 942: https://legiscan.com/CA/text/SB942/id/3013546

[170] The California Privacy Protection Agency (CPPA). California Finalizes Regulations to Strengthen Consumers' Privacy. September 23, 2025. https://cppa.ca.gov/announcements/2025/20250923.html

Scope: addresses the use of ADMT when used to make Significant Decisions regarding consumers. This is especially relevant for systems used in financial or lending services, housing, education, employment, and healthcare.

Requirements:

- conduct a risk assessment when using ADMT to make significant decisions, or when using personal information to train ADMT.
- provide downstream business with all facts available and necessary for the recipient-business to conduct its own risk assessment on the ADMT
- provide Pre-Use Notice to consumers to inform about ADMT's purpose, types of personal information used, type of outputs generated, and how those outputs are used in the decision-making process
- provide consumers with the right to opt out, and right to access to information about the ADMT's use and logic.
- conduct a risk assessment if consumers' personal information is processed and presents significant risks to privacy
- conduct cybersecurity audits by a qualified independent professional

Sanction: allows for civil action by the California Attorney General's office or city/county counsel of $5,000 per violation.

Effective date:

- risk assessment requirements: compliance by January 1, 2026, documentation to the CPPA by April 1, 2028.
- ADMT requirements: compliance by January 1, 2027.
- cybersecurity audits: certifications to be submitted by April 2028 through April 2030 depending on the size of the business.

Colorado

On May 17, 2024, Colorado Governor Jared Polis signed into law Senate Bill 24-205, known colloquially as the Colorado Artificial Intelligence Act (CAIA), making Colorado the second U.S. state to enact a major AI consumer protection law.[171] Originally designed to take effect on February 1, 2026, lawmakers passed a special-session bill on August 26th to delay the Colorado law's effective date five months to June 30, 2026.

In the 2026 legislative session, Colorado lawmakers are likely to continue the debates over the implementation details of the CAIA, as well as further liability measures on big technology companies.

[171] National Association of Attorneys General. A Deep Dive into Colorado's Artificial Intelligence Act. October 26, 2024. https://www.naag.org/attorney-general-journal/a-deep-dive-into-colorados-artificial-intelligence-act/

SB 24-205 (An Act Concerning Consumer Protections for Interactions with AI - *as amended by SB205-004):*[172]

Target: developer and deployers of a high-risk AI system

Scope: high-risk systems which makes (or is a substantial factor in making) "consequential decisions" in education, employment, housing, insurance, financial and lending services, legal, healthcare, and government services

Requirements:

- developer and deployers to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination
- developers need to ensure documentation for model characteristics and risk management measures, and meet transparency obligations are complete and available to deployers
- disclose to consumers that they are interacting with an AI system
- deployers need to implement risk management program, conduct impact assessments, and meet transparency obligations are complete and available to consumers
- provide mechanisms to consumers with right to correct their information
- provide mechanisms to consumers to appeal if the use of a high-risk AI system results in an adverse decision
- review annually the deployment of each high-risk system to ensure it is not causing algorithmic discrimination

Sanction: Up to $20,000 per violation
Provides reduced penalties if organizations comply with National Institute of Standards and Technology AI Risk Management Framework, ISO/IEC 42001, or other nationally or internationally recognized AI risk management frameworks.

Effective date: June 30, 2026

Utah

Utah Governor Spencer Cox explains Utah's AI policy as a proactive and 'pro-human' approach where AI must always be used for human flourishing." The Governor states that in the next legislative session, Utah will discuss "harm reduction in AI companions, transparency around deepfakes, and an upcoming study around data ownership and control more broadly, as well as the interaction with AI and health care."[173]

[172] The Colorado Senate Bill 24-205: https://content.leg.colorado.gov/sites/default/files/2024a_205_signed.pdf
[173] Keely Quinlan. Utah governor announces 'pro-human' AI plan, condemns federal preemption scheme. StateScoop. December 3, 2025. https://statescoop.com/utah-gov-spencer-cox-pro-human-ai-plan/

Utah's approach focuses on transparency and flexibility in AI policymaking. The state has established a learning lab for AI where real-world impact specific use cases (such as AI and mental health) are studied to gather evidence and offer recommendations to the legislature.[174]

SB 226 (Artificial Intelligence Consumer Protection Amendments):[175]

Target: "regulated occupations" requiring state licensure or certification

Scope: use of generative AI during "high-risk" interactions that involve sensitive data or significant decisions

Requirements:

- disclose use of AI if collecting sensitive personal information, or providing advice for a significant personal decision

Sanction: up to $2,500 per violation
safe harbor if clear disclosures were provided at the start or during the interaction

Effective date: July 1, 2027 (as extended by Senate Bill 332)

HB 452 (Artificial Intelligence Amendments):[176]

Target: supplier of a mental health chatbot

Scope: mental health chatbots

Requirements:

- disclose user is interacting with AI
- disclose any advertisements and any sponsorship or similar relationships
- restricts sale or share of individually identifiable health information or user inputs of Utah users

Sanction: up to $2,500 per violation, additional penalties for each violation of an administrative order up to $5,000 each, and possibility of injunctive relief or disgorgement

Effective date: May 7, 2025

SB 271 (Unauthorized AI Impersonation Amendments):[177]

Target: any person

Scope: abuse of personal identity through generative AI or digital manipulation

---

[174] Spencer Cox & Margaret Busse. Utah Has Found the Right Middle Ground on Artificial Intelligence. Utah Department of Commerce. June 12, 2025. https://commerce.utah.gov/2025/06/12/utah-has-found-the-right-middle-ground-on-artificial-intelligence/

[175] The Utah Senate Bill 226: 226 Artificial Intelligence Consumer Protection Amendments, https://legiscan.com/UT/text/SB0226/id/3174279

[176] The Utah House Bill 452: https://le.utah.gov/~2025/bills/static/HB0452.html

[177] The Utah Senate Bill 271: https://le.utah.gov/~2025/bills/static/SB0271.html

Requirements:

- prohibits the knowing sale, distribution, or licensing of any tool whose intended primary purpose is the unauthorized creation or modification of content which includes personal identity

Sanction: up to $2,500 per violation
provides for private right of action
exemptions for certain fair uses of personal identity

Effective date: May 7, 2025

Texas

On June 22, 2025, Texas Governor Greg Abbott signed into law House Bill 149, the "Texas Responsible Artificial Intelligence Governance Act" (the Act or TRAIGA). Unlike other laws focused on impact, the Texas lawmakers decided to adopt an intent-based liability framework. In other words, the law requires proof of intentional misconduct or discriminatory intent.[178] The comprehensive protections originating from Republican-majority states such as Texas and Utah are notable in understanding how the state lawmakers advance both economic advancements and consumer protections in their jurisdictions.

HB 149 (Texas Responsible Artificial Intelligence Governance Act (TRAIGA)):[179]

Target: developers and deployers of AI systems (public and private sector)

Scope: prevent intentional discrimination, harmful content generation, and social scoring

Requirements:

- clarifies that existing biometric privacy law in Texas applies to AI training, development, and deployment. Individuals must have made their biometric media publicly available themselves to count as consent.
- prohibits certain AI systems from deployment:
  - use of AI with the intent to discriminate against protected classes
  - AI designed to encourage self-harm, illegal acts, or suicide
  - AI deployed with the sole intent of
    - infringing upon constitutional rights
    - producing, assisting or aiding in producing, or distributing CSAM
- For government:
  - prohibits social scoring by government

[178] Victor D Vital and Alexander M Clark. Texas Enters the AI Sandbox with TRAIGA: Implications for Business Trials. July 14 2025. American Bar Association. https://www.americanbar.org/groups/business_law/resources/business-law-today/2025-july/texas-enters-ai-sandbox-with-traiga-implications-business-trials/

[179] The Texas House Bill 149: https://legiscan.com/TX/text/HB149/id/3180120

- prohibits use of biometric data obtained from publicly available sources without consent to uniquely identify persons
- requires disclosure to users when they are interacting with an AI system

Sanction: civil penalties up to $200,000 per violation with a sixty-day cure period, and an additional $2,000 to $40,000 per day for continued violations.
The TRAIGA provides certain safe harbor protections for good faith behavior and also establishes a 36-month program where companies can sandbox test their AI models under state oversight with possible legal immunity.

Effective date: January 1, 2026

SB 815 (AI in Insurance):[180]

Target: health insurance plan providers

Scope: algorithm-driven insurance utilization reviews and coverage determinations

Requirements:

- bans insurance utilization review agent from using algorithms to "make, wholly or partly, an adverse determination" (i.e. determination whether a suggested care is medically necessary, appropriate, or is experimental or investigational, must be made by a human)

Sanction: provides the Texas Department of Insurance (TDI) the authority to audit health plan's use of AI to ensure compliance

Effective date: September 1, 2025

New York

Governor Kathy Hochul signed the first-in-the-nation surveillance pricing law. While California's Assembly Bill 325 takes a wide lens to prevent algorithmic price fixing and constraining trade, NY's law requires notification to consumers when the prices of a good are changed due to personalized algorithmic pricing. The law may become a blueprint for other states interested in regulating surveillance pricing or amending consumer protection laws.

Governor Hochul also signed the Responsible AI Safety and Education Act (RAISE Act), in alignment with California's SB 53. This intentional alignment provides a model for other states on how different AI legislative obligations can be aligned and strengthened at the same time.

[180] The Texas Senate Bill 815: https://legiscan.com/TX/text/SB815/id/3061127

Responsible AI Safety and Education Act (RAISE Act):[181]

Target: developers of "frontier" AI who spend over $100 million in computational resources training advanced models (or use greater than 10^26 integer or floating-point operations in training)

Scope: safety protocols and incident reporting for frontier AI models

Requirements:

- implement safeguards against "critical harm" and describe in detail how they handle safety risks
- submit safety protocols
- report safety incidents within 72 hours

Sanction: Initial infractions up to $1 million, with subsequent violations potentially up to $3 million

Effective date: January 1, 2027

New York State - Algorithmic Pricing Disclosure Act[182]

Target: entities domiciled or doing business in New York

Scope: dynamic pricing algorithms ("pricing that fluctuates dependent on conditions") using personal data

Requirements:

- inform customers when prices are set using personalized algorithms
- disclose the phrase "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA" along with the price

Sanction: Attorney General must first issue a cease-and-desist notice, then can pursue penalties of up to $1,000 per violation.

Effective date: November 10, 2025

New York State - AI Companions Models (*under General Business Law*)[183]

Target: operators of AI companion models

Scope: AI companions (defined as those AI systems "designed to simulate a sustained human or human-like relationship with a user by: (i) retaining information on prior interactions or user sessions and user preferences to personalize the interaction and facilitate ongoing engagement with the AI companion; (ii) asking unprompted or unsolicited emotion-based questions that go beyond a direct

[181] The New York State Senate Assembly Bill A6453N: https://www.nysenate.gov/legislation/bills/2025/A6453/amendment/B

[182] The New York State, Amendment to Article 22-A of Consumer Protection From Deceptive Acts and Practices. https://www.nysenate.gov/legislation/laws/GBS/349-A

[183] The New York State, General Business Law Article 47, https://www.nysenate.gov/legislation/laws/GBS/A47

response to a user prompt; and (iii) sustaining an ongoing dialogue concerning matters personal to the user.

Exclusions include customer service models, and those providing efficiency improvements or, research or technical assistance; or those used solely for internal business purposes.

Requirements:

- clearly and regularly notify users that they are interacting with AI, not a human
- embed protocol to detect a user's expression of self harm or suicidal ideation
- where such expressions are detected, direct users to crisis service providers

Sanction: civil penalties of up to $15,000 per day for a violation

Effective date: November 5, 2025

New York City Local Law 144 (Automated employment decision tools):[184]

Target: employers and employment agencies in NYC

Scope: use of automated employment decision tools (AEDT) to screen a candidate or employee for an employment decision

Requirements:

- ensure the tool has been subject to a recent bias audit and a summary of the audit is made publicly available on the website of the employer / agency
- notify each candidate that such a tool will be used
- provide information about the type of data collected, and qualifications and characteristics the tool will use in the assessment

Sanction: Up to $500 per violation on the first day of violations

Up to $1,500 per subsequent violation

Effective date: January 1, 2023

In addition to these laws, another topic concerns algorithms used to dynamically change prices based on a consumer's location or other individual characteristics. Also termed as **"surveillance pricing," "algorithmic price fixing," or "dynamic pricing,"** such algorithms used by any vendor creates possible case for economic losses from discriminatory algorithms, unfair practices, and sometimes even non-competitive environments. The California and New York lawmakers passed legislation to regulate algorithmic pricing. Analysis by the Consumer Reports

[184] The New York City Local Law 144: https://rules.cityofnewyork.us/rule/automated-employment-decision-tools-updated/

show 24 states have more than 50 bills in place to regulate algorithmic pricing.[185] Other analysis suggest legislators may have a more targeted approach, focusing AI-driven rental prices.[186]

In conclusion, despite the pressures from federal government to prevent any further state regulatory activity on AI, the states are likely to continue their activities to ensure fair competition, fair business practices, and allocate liability correctly in high-impact domains.

[185] Consumer Reports. How U.S. States are Tackling Algorithmic Pricing: 2025 Bill Tracker and Analysis. https://innovation.consumerreports.org/How-U.S.-States-are-Tackling-Algorithmic-Pricing.pdf
[186] LexisNexis. State Lawmakers Seek to Regulate AI Pricing. August 13, 2025. https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/state-lawmakers-seek-to-regulate-ai-pricing

About the Author

Merve Hickok is the President and Policy Director at Center for AI and Digital Policy (CAIDP), deeply engaged in global AI policy and regulatory work. CAIDP educates AI policy practitioners and advocates across 120+ countries. Merve provides AI policy expertise to the UNESCO, Council of Europe, OECD, EU AI Office Working Group, and Hiroshima AI Friends Group, GPAI Tokyo Expert Support Center. She has provided testimony to the U.S. Congress, the Turkish National Assembly, the State of California, the New York City and the Detroit City councils. She is a Visiting AI Researcher at Chiba Tech, and a 2024 Council on Foreign Relations – Hitachi International Affairs Fellow.

Merve Hickok is the founder of AIethicist.org. She is a globally renowned, award-winning expert on AI policy, ethics and governance. Her contributions and perspective have featured in The New York Times, Washington Post, Guardian, CNN, Forbes, Bloomberg, Wired, Scientific American, The Atlantic, Politico, Protocol, Vox, The Economist and MIT Technology Review.