Washington State Artificial Intelligence Task Force

Final Report

Addendum

Overview of Existing State and Federal AI Regulation

By Vi Tran and John T. Bender

June 2026

Prepared for:

Washington State Artificial Intelligence Task Force

This Addendum to the AI Task Force Final Report addresses the requirement in ESSB 5838 that the Task Force provide a "review of existing protections under state and federal law for individual data and privacy rights, safety, civil rights, and intellectual property rights, and how federal, state, and local laws relating to artificial intelligence align, differ, conflict, and interact across levels of government."

TABLE OF CONTENTS

I. INTRODUCTION

The report begins by providing an overview of the existing federal and state landscape, including key decisions necessary in regulating AI, then provides examples of varying approaches to AI regulation, and then summarizes state and federal AI laws relating specifically to data, safety, civil rights, and intellectual property. There is significant overlap between the various subjects requested by statute. Safety is broken into consumer protection, physical safety, and high-risk decisions affecting safety. Civil rights include traditional civil rights issues (e.g., discrimination) but also include AI use in decisions determining access to benefits.

II. EXECUTIVE SUMMARY

No comprehensive federal AI-specific legislation providing protection for AI harms currently exists. Apart from federal legislation concerning nonconsensual intimate imagery ("NCII"), federal protections for AI harms primarily rely on agencies and private litigation enforcing existing law as applied to AI. As a result, to the extent agency enforcement requires novel application of existing law, the breadth of federal protections may depend on the policy of the Presidential Administration currently in office. The current Trump Administration has a "minimally burdensome" policy toward AI and seeks to preempt conflicting state law. Targeted state laws grounded in traditional police powers—laws regulating the general health, safety, morals, and welfare of state citizens—are less likely to face preemption.

In the absence of federal legislation, State legislation is the main source of AI-specific legislation. State AI laws are highly fragmented, filling gaps in existing laws and primarily addressing specific sectors (e.g., healthcare, finance, elections) or specific harms or uses (e.g., NCII). Some states have enacted cross-sector AI legislation, either by (1) regulating vertically by focusing on particular areas of law (e.g., consumer protection or data privacy) that may involve regulation across different sectors or use cases, or by (2) targeting the most advanced or widely used models (e.g., OpenAI's GPT series), with statutes or guidance covering "frontier," "foundation," or "general purpose" models. States and authorities differ on how to define or categorize these advanced or widely used models. A third approach, adopted by the European Union (the "EU"), regulates horizontally by imposing requirements depending on the risk associated with categories of AI use—without regard to vertical or sector—and separately regulates advanced or widely used models.

Key verticals and sectors that States have focused on most closely involve AI harms related to data privacy, access to benefits (including employment, housing, and healthcare), AI use in government operations (including law enforcement), and consumer protection and Unfair and Deceptive Acts and Practices ("UDAP"). Specific issues that States have focused on involve automated decision-making; algorithmic pricing; chatbots, deepfakes and NCII; eliminating use of AI as a defense to liability; name and image likeness ("NIL") and intellectual property ("IP") ownership; intentional misuse of AI; and advanced or widely used models.

State legislators face several key decision points: the method, the scope, the type of obligations imposed, and the means of enforcement:

- **Method.** Legislation may be **piecemeal** or **omnibus**, including legislation covering broad verticals (CO), targeting intentional AI misuse (TX), targeting high-impact models (NY, CA), or broad, horizontal regulation based on use risks (EU).
- **Scope.** Legislation may cover different **types of AI** (from all automated systems to advanced AI systems or generative AI), or different **AI actors** (developers, deployers, distributors)
- **Obligations.** Legislation may impose procedural obligations involving **transparency** (disclosure, documentation, incident reporting), **governance** (human oversight, training, risk assessments and frameworks), **validation** (data quality requirements, registration, audit) or provide substantive **prohibitions** or **individual rights** (opt-out rights, appeal of decision-making).
- **Enforcement.** Legislation may provide a private right of action in addition to civil and criminal penalties and may include equitable remedies such as algorithmic disgorgement, which involves deleting models or algorithms (in whole or in part) that used improperly obtained or invalid data.

Legislation gaining the most traction tends to be most narrowly tailored to address specific, non-controversial issues. For example, many states have enacted legislation extending existing laws (e.g., extending NCII legislation to cover deepfakes) or to protect specific classes of people (e.g., children).

III. OVERVIEW OF FEDERAL AND STATE AI REGULATION

A. KEY ELEMENTS OF AI REGULATION

Definition of AI. There is no uniform definition of AI. AI is not a single form of technology but is a catchall term generally referring to a system that can, within a given set of objectives, analyze data to generate outputs such as predictions, recommendations, or decisions, often in a way that simulates human intelligence.[1] For example, California defines AI as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments."[2]

AI is traceable to the mid-20th century with recognizable AI systems emerging in the late 1990s, including the landmark chess match between then-world chess champion Garry Kasparov and IBM's Deep Blue supercomputer.[3] As a result, legal definitions of AI may cover not just recently developed AI systems but also broader forms of technology and automated decision-making. Some states have enacted broadly applicable uniform definitions for AI that serve as a baseline for other legislation regulating AI.

Types of covered AI. Existing laws regulating AI differ on how they define AI and to what extent they cover different types of AI systems or models. The types of systems covered by existing laws can be categorized into four types:

> (1) automated decision-making systems, which can be defined as any technology processing information through computation that replaces or substantially replaces human decision-making, most commonly involving automated systems making consequential decisions (e.g., a medical insurer using automated software to determine whether to deny coverage or reimbursement);[4]
>
> (2) advanced AI systems such as those that (a) are so advanced, applicable to such a wide variety of contexts, used by so many users, or trained on so much data that they are viewed as having higher risk, or (b) exhibit high levels of performance at tasks that pose serious risks (e.g., national security) sometimes referred to as "frontier," "dual-use foundation," or "general-purpose" models, typically limited to a handful of the largest systems, such as OpenAI's GPT series or Anthropic's Claude models;[5]

---

[1] *See* Nat'l Inst. Standards & Tech., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[2] California AB 2885 (effective Jan. 1, 2025).

[3] 20 Years after Deep Blue: How AI Has Advanced Since Conquering Chess, Larry Greenemeir, Scientific American (June 2, 2017), https://www.scientificamerican.com/article/20-years-after-deep-blue-how-ai-has-advanced-since-conquering-chess/.

[4] *E.g.*, Colorado Privacy Act (Col. Rev. Stat § 6-1-1301 et seq. (effective July 1, 2023)), California Consumer Privacy Act Regulations (11 CCR § 7001 et seq (effective Jan. 1, 2027)).

[5] *E.g.*, California Transparency in Frontier Artificial Intelligence Act (CA TFAIA), SB53 (effective Jan. 1, 2026); New York Responsible AI Safety and Education (RAISE) Act, N.Y. Gen. Bus. Law Art. 44-B (effective Jan. 1, 2027); Executive Order 14110 (Oct. 30, 2023) (issued by President Biden but rescinded by President Trump).

(3) generative AI systems or synthetic content, which are systems using AI to create new or unique content (e.g., ChatGPT);[6]

(4) all AI systems, defined broadly.[7]

These categories overlap and laws may define coverage over a particular AI system through subjective evaluation of the model's characteristics and/or an objective, technical evaluation of the model, such as the amount of computing power on which the model was trained.[8]

Types of AI actors. Existing laws regulating AI also distinguish between the type of AI actors being regulated, which can be categorized into four types:

(1) **developer**, an entity developing an AI system;

(2) **deployer** or **user**, an entity using or operating an AI system in practice;

(3) **provider**, other entities within the supply chain including resellers, importers, integrators, and may include distributors of the outputs of AI systems, e.g., websites that publish deepfakes.

Types of protection. Existing laws regulating AI also distinguish between the type of protection afforded or obligations imposed, procedural and substantive:

(1) **procedural** obligations and protections cover the processes by which an AI system is developed or deployed and fall into three categories:

(a) **transparency** (*e.g.*, notices and disclosures, incident reporting);

(b) **governance** (*e.g.*, training, impact assessments, testing, documentation, risk management policies, designation of a responsible individual);

(c) **validation** (*e.g.*, registration, audits, third-party assessments).

(2) **substantive** obligations or protection involve individual rights or protection from specific harms caused by AI, *e.g.*, opt-out rights, non-consensual use of deepfakes, and misuses of name image or likeness.

Means of enforcement. Existing laws regulating AI also distinguish between the means of enforcement, whether (1) **only by the State** and/or (2) by **private rights of action**, with varying penalties or enforcement mechanisms (*e.g.*, injunctions).

---

[6] *E.g.*, New York Synthetic Performer Disclosures, S8420A (effective June 9, 2026).

[7] *See, e.g.*, Texas Responsible Artificial Intelligence Governance Act, HB 149 (effective Jan. 1, 2026) (defining AI system as "any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions or recommendations, that can influence physical or virtual environments").

[8] For example, California's TFAIA covers certain "frontier" models trained using a quantity of computing power greater than 10^{26} integer or floating-point operations ("FLOP") with a training cost floor of $100 million.

B. FEDERAL REGULATION

1. There Is No Current Comprehensive Federal AI Regulation

Congress has not enacted a comprehensive federal AI regulatory framework. AI-specific federal laws that currently exist are narrowly tailored to specific use cases. For example, the federal Take It Down Act[9] criminalizes non-consensual deepfake pornography.

Federal regulation consists primarily of applying existing statutes and regulations such as federal consumer protection and privacy laws to the AI context. As a result, federal regulation relies heavily on agency enforcement on a case-by-case basis, particularly through the Department of Justice, the Federal Trade Commission, the Consumer Financial Protection Bureau, and the U.S. Equal Employment Opportunity Commission.[10]

In 2023, for example, a leaked civil investigative demand ("CID") shows that the Federal Trade Commission (FTC) invoked its authority under Section 5 of the FTC Act to investigate unfair or deceptive practices to request consumer-protection information from OpenAI about its customers, products, and privacy and data security policies and procedures.[11] The CID does not yet appear to have resulted in a formal lawsuit or public enforcement action by the FTC.

Similarly, in 2024, the U.S. Department of Justice (DOJ) sued RealPage, a company contracting with competing landlords to train its algorithmic pricing software, for alleged price-fixing under Section 1 of the Sherman Act.[12] In December 2025, the DOJ filed a proposed settlement prohibiting RealPage from using nonpublic competitor information ("CSI") when actually running the models (e.g., to set or recommend prices), but allowing use of nonpublic CSI when training the models if the information was older than 12 months.

2. Federal AI Policy Shifts: Current Policy Removes Barriers to AI Innovation

The focus of federal AI policy has shifted across Presidential Administrations. While the policy under the Biden Administration mandated guardrails in the development of AI and protection of individual rights, the current Trump Administration mandates a "minimally burdensome" national policy focused on accelerating and achieving U.S. global dominance in AI innovation. The current Trump Administration has expressed its intent to seek preemption of state laws that conflict with the "minimally burdensome" policy.

---

[9] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, S. 146, 119th Cong. (enacted May 19, 2025).

[10] *E.g.*, Rohit Chopra et al., *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[11] David Hamilton, *FTC investigating ChatGPT creator OpenAI over consumer protection issues*, AP News (July 13, 2023), https://apnews.com/article/openai-chatgpt-investigation-federal-ftc-76c6218c506996942282d7f5d608088e.

[12] Dep't of Justice, Justice Department sues RealPage for algorithmic pricing scheme that harms millions of American renters (Aug. 23, 2024), https://www.justice.gov/archives/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters.

Biden Administration.

The Biden Administration's policy emphasized ethical governance and regulating the potential risks associated with AI use, including:

- **AI Bill of Rights (October 2022)**: Issuing a non-binding framework to guide the development of safe, ethical, and equitable AI systems to help protect Americans' civil rights. The AI Bill of Rights articulated five principles for the design, use, and deployment of AI systems: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternatives and oversight.[13]
- **Executive Order 14110 (October 2023)**: Directing federal agencies to develop guidance on safety testing, content authentication, cybersecurity, privacy, anti-bias measures, and AI procurement.

Current Trump Administration.

The second Trump Administration has shifted the focus back toward a federal policy of maintaining U.S. competitiveness in AI development with "minimally burdensome" regulation and federal preemption of state laws limiting AI development. The Trump Administration has revoked President Biden's Executive Order 14110,[14] directed the development of an action plan to achieve the goal of sustaining and enhancing America's "global AI dominance" by removing "barriers" to AI development,[15] and issued an Executive Order and created a National AI Legislative Framework expressly adopting a "minimally burdensome" national policy that seeks to preempt conflicting state laws.

Executive Order 14365 (December 2025).[16] Executive Order 14365 specifically references the Colorado AI Act's focus on algorithmic discrimination and directed a multi-agency strategy to identify and challenge state laws regulating AI, imposing penalties on states that do not comply. The EO establishes an AI Litigation Task force "whose sole responsibility shall be to challenge State AI laws inconsistent" with the Administration's policy. The EO further directs the Secretary of Commerce to conduct an evaluation of state AI laws that identify "onerous laws" and restrict non-deployment funding from the Administration's Broadband Equity Access and Deployment Program to states with identified "onerous laws." The EO requires the FTC to issue a policy statement that certain state laws restricting AI outputs are preempted by federal UDAP law, and mandates preparation of a legislative recommendation for a uniform federal AI framework that preempts State AI laws.

---

[13] White House, Office of Science & Tech. Pol. ("OSTP"), *Blueprint for an AI Bill of Rights* (Oct. 2022), https://www.govinfo.gov/content/pkg/GOVPUB-PREX23-PURL-gpo193638/pdf/GOVPUB-PREX23-PURL-gpo193638.pdf.

[14] Exec. Order No. 14148, 90 Fed. Reg. 8237 (Jan. 28, 2025), https://www.federalregister.gov/documents/2025/01/28/2025-01901/initial-rescissions-of-harmful-executive-orders-and-actions.

[15] Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 31, 2025), https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence; White House, *Winning the Race: America's AI Action Plan* (July 23, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[16] White House, *President Donald J. Trump Unveils National AI Legislative Framework* (Mar. 20, 2026), https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/.

National AI Legislative Framework (March 2026).[17] The National AI Legislative Framework issued pursuant to the EO provided six policy issues to balance aggressive AI development with certain necessary safeguards (including protecting children, protecting intellectual property and NIL, and free-speech protections for AI providers). The framework re-emphasizes "removing barriers to innovation," and preempting state laws that "impose undue burdens to ensure a minimally burdensome national standard." The framework recommends that the legislature establish a federal AI policy framework to preempt state laws that impose "undue burden" on AI innovation. The framework recommends preempting (a) state attempts to regulate AI development; (b) state regulation of use of AI that would be lawful if performed without AI; (c) state laws penalizing developers for third-party conduct. The framework does not recommend preempting (a) traditional police powers of states, "including particular laws to protect children, prevent fraud, and protect consumers," (b) state zoning laws, (c) state laws governing a state's own use of AI.

The current Administration's posture toward a "minimally burdensome" national policy on AI has had meaningful effects on the extent to which federal agencies can be relied upon to provide AI protections. For example, in December 2024 and under the Biden Administration, the FTC issued a consent order against Rytr, an AI writing assistant, asserting that one of Rytr's tools facilitated creation of fake reviews, constituting unfair or deceptive practices under Section 5 of the FTC Act.[18] A year later, in response to President Trump's Executive Order 14179 and AI Action Plan, on December 22, 2025, the FTC took the highly uncommon step of re-opening and vacating its order against Rytr.[19]

3. Voluntary Frameworks and Federal Guidance/State Adoption

Several voluntary federal frameworks have provided guidelines for AI development and deployment and have in some cases been incorporated into State laws governing AI, including:

- **NIST AI Risk Management Framework (Jan. 2023) and Generative AI Profile (July 2024)**. The "AI RMF 1.0" was released by the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") as a best-practices guide for AI actors to assess and mitigate AI risks.[20] In July 2024, NIST released a supplement to the AI RMF to address best practices to mitigate specific risks associated with generative AI, including hallucinations, deepfakes, intellectual property, and data privacy and security.[21]

---

[17] White House, Legislative Recommendations for a National Policy Framework for Artificial Intelligence (Mar. 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf.

[18] Complaint, *Rytr LLC*, *Rytr LLC*, FTC Docket No. C-4806 (Dec. 16, 2024).

[19] FTC, *FTC Reopens and Sets Aside Rytr Final Order in Response to the Trump Administration's AI Action Plan* (Dec. 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.

[20] *See* Nat'l Inst. Standards & Tech., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[21] *See* Nat'l Inst. Standards & Tech., *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1)* (July 2024), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=958388.

- **Safe harbor.** The NIST frameworks are cited by federal regulators and several states, including Texas[22] and Colorado,[23] provide a safe harbor in their AI laws for AI actors substantially complying with AI RMF or other nationally or internationally recognized risk management frameworks.[24] A safe harbor provision is a provision that expressly protects an individual from liability or penalties if they comply with specified requirements.

- **OECD AI Principles (revised 2024).** A set of principles adopted by the Organization for Economic Cooperation and Development ("OECD") and endorsed by over 40 countries, including the United States, reflecting a consensus on what AI governance should address, including inclusive growth and sustainable development; human rights and democratic values, including fairness and privacy; transparency; accountability; and robustness, security, and safety.[25]

4. Preemption

Federal law may in the future preempt state laws on AI, but the risk of preemption may vary between different Administrations' policies and the makeup of Congress. The One Big Beautiful Bill Act (2025) proposed a 10-year moratorium on state and local AI regulation that was approved by the House but removed by the Senate.[26] The current Trump Administration's policy creates substantial preemption concerns for states regulating AI, but indicates that state AI protections anchored in established state police powers—consumer protection, civil rights, criminal law, and privacy—would not be subject to preemption.[27]

C. STATE REGULATION

State AI legislation is primarily a gap filler. In the absence of federal legislation, the States have enacted their own laws governing AI-related harm: in 2025, state legislators introduced over 1,000 AI-focused bills.[28] State regulation is highly piecemeal, with states focusing legislation on specific industry sectors or specific uses or harms, and enacting different obligations, protections, and remedies (if any) based on the type of AI actor and the type of AI involved.

---

[22] Texas Responsible Artificial Intelligence Governance Act ("TRAIGA"), HB149 Section 552.105(e)(D) (effective Jan. 1, 2026).
[23] Colorado AI Act, Co. Rev. Stat. § 6-1-1701 et seq. (effective June 30, 2026).
[24] Other recognized risk management frameworks include https://www.iso.org/standard/42001.
[25] OECD, (Mar. 05, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents.
[26] Tambudzai Charumbira, *AI Regulation and Federalism* (Sept. 16, 2026), https://regulatorystudies.columbian.gwu.edu/ai-regulation-and-federalism-what-moratorium-wasnt-debate-revealed.
[27] White House, Legislative Recommendations for a National Policy Framework for Artificial Intelligence (Mar. 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf.
[28] Chelsea Canada, *New Trends Emerge as States Refine AI Legislation*, National Conference of State Legislatures (Jan. 22, 2026), https://www.ncsl.org/state-legislatures-news/details/new-trends-emerge-as-states-refine-ai-legislation.

Some states, including Colorado[29] and Texas[30] have enacted broad, cross-sectoral legislation; other states, including California[31] and New York,[32] have enacted cross-sectoral legislation for high-risk types of AI (including advanced models that may be defined as "frontier," "general use," or "foundation" models) with extensive piecemeal legislation covering specific circumstances. Piecemeal legislation focuses new AI legislation as a gap filler in areas where AI creates novel issues that are not adequately addressed by existing law, receiving less friction in enactment and allowing legislators to avoid duplicative mandates, take an incremental approach, and fine tune regulations to specific needs.[33]

States with legislation most closely focus on issues involving AI harms related to data privacy, access to benefits (including employment, housing, and healthcare), AI use in government operations (including law enforcement), and consumer protection and Unfair and Deceptive Acts and Practices ("UDAP"). Many states have enacted legislation that address AI harms involving automated decision-making; algorithmic pricing; chatbots, deepfakes and NCII; eliminating use of AI as a defense to liability; NIL and IP ownership; intentional misuse of AI; and advanced or widely used models.

Washington recently enacted legislation broadly requiring disclosures from large generative AI providers to disclose to consumers when content is AI-generated and to embed data necessary to track when content is AI-generated.[34] Apart from that legislation, Washington's enacted legislation has been targeted, with laws on CSAM,[35] use of name image and likeness ("NIL"),[36] chatbots,[37] and health carriers' use of AI in the prior authorization determination process.[38]

Local regulation. Cities and counties have enacted more narrowly tailored procedural protections focused on traditional city and county governance, primarily in government functions (e.g., police surveillance or facial recognition, and labor and employment), such as New York City's regulation over automated employment decision tools.[39]

---

[29] Colorado AI Act, Co. Rev. Stat. § 6-1-1701 et seq. (effective June 30, 2026).
[30] Texas Responsible AI Governance Act, HB 149 (effective Jan. 1, 2026).
[31] California Transparency in Frontier AI Act, SB 53 (effective Jan. 1, 2026).
[32] New York Responsible AI Safety and Education (RAISE) Act, N.Y. Gen. Bus. Law Art. 44-B (effective Jan. 1, 2027.
[33] Bipartisan House Task Force, *Report on Artificial Intelligence* at vi–viii (Dec. 2024), https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/A163BDBF496ADA741F831E5BEBBCA06699B6AFF8CC34F4FDC4065BDA298295DF.ai-task-force-report-final.pdf.
[34] Washington HB 1170 (effective Feb. 1, 2027).
[35] Washington HB 1999 (effective June 6, 2024).
[36] Washington SB 5886 (effective June 11, 2026); Washington HB 1205 (effective July 27, 2025).
[37] Washington HB 2225 (effective Jan. 1, 2027).
[38] Washington SB 5395 (effective June 11, 2026).
[39] N.Y.C. Local Law 144 (effective Jan. 1, 2023).

IV. COMPARATIVE APPROACHES

A. VARYING STATE APPROACHES TO CROSS-SECTOR LEGISLATION

Colorado, Texas, Utah, New York, and California have led the way in enacting cross-sector omnibus AI legislation and take two approaches: comprehensive and frontier model. Both approaches involve a primary AI act that regulates AI across various sectors and use cases, with piecemeal legislation filling in gaps in specific circumstances. The comprehensive approach focuses on regulating varying forms of AI in high-risk uses and sectors, whereas the frontier-model approach focuses on regulating high-impact models, such as the very largest models extensively used throughout many industries or that serve as the foundation for many secondary AI-based applications.

On the other hand, states like Montana have enacted or are proposing "Right to Compute" Acts,[40] which view AI as an extension of existing property and free expression rights and seek to require government regulation to be "narrowly tailored to fulfill a compelling government interest."

1. Comprehensive

Colorado. The Colorado AI Act[41] (the "CAIA") focuses on the broad consumer protections and addresses concerns about how AI systems interact with consumer protection goals. The CAIA applies to high-risk AI systems defined as systems making consequential decisions (e.g., employment, education, housing).

The CAIA (1) imposes a duty on **developers and deployers** to avoid algorithmic discrimination; (2) requires **developers** to document, disclose, and report (a) the purpose, benefits, limitations, risks, of the system; (b) the data used to train; (c) how they evaluated the systems; (d) how the systems should or should not be used; (e) measures taken to mitigate risks; and (f) situations where the system may have caused algorithmic discrimination; (3) requires **deployers** to (a) create risk management policies similar to the NIST'S AIRMF or ISO 42001; (b) complete regular impact assessments; (c) disclose to consumers if the system is a substantial factor in making a consequential decision; (d) describe the reason for any adverse decision, the data used, and the impact of AI and (4) allow **consumers** the right to correct personal data and appeal decisions. The CAIA provides legal protection for entities that comply with NIST's AIRMF or ISO 42001.

Texas. The Texas Responsible Artificial Intelligence Governance Act ("TRAIGA")[42] focuses on AI use in **government** and **intentional misuses** of AI. TRAIGA requires government entities to disclose to consumers when they are interacting with AI, prohibits governments from assigning social scores to consumers, and restricts the government's use of biometric data. TRAIGA prohibits use of AI intended to manipulate behavior, discriminate, infringe upon rights,

[40] Montana SB 212 (effective Apr. 16, 2025).
[41] Co. Rev. Stat. § 6-1-1701 et seq. (effective June 30, 2026).
[42] Texas HB 149 (effective Jan. 1, 2026).

or distribute unlawful explicit content. TRAIGA provides legal protections for developers and deployers who self-identify potential violations or comply with NIST's AIRMF or similar RMFs.

Utah. The Utah Artificial Intelligence Policy Act[43] is narrower than CAIA and TRAIGA. The Act clarifies that existing consumer protection laws extend to conduct carried out with generative AI, requires persons in regulated occupations to make proactive disclosures to consumers that they are interacting with AI, and requires other businesses to disclose if asked.

Washington. Washington has not enacted general-purpose, comprehensive legislation regulating AI, but has recently enacted legislation broadly requiring disclosures from large generative AI providers to disclose to consumers when content is AI-generated and to embed data necessary to track when content is AI-generated.[44] Other attempts at broad AI legislation, including aimed at increasing transparency in AI,[45] high-risk AI uses[46] and broad consumer-protection regulation,[47] have been introduced but have not been passed.

2. Frontier model

New York and California. New York's Responsible AI Safety and Education Act (the "RAISE" Act)[48] and California's Transparency in Frontier Artificial Intelligence Act (the "TFAIA")[49] apply to "frontier" models defined similarly in both acts as foundation models that meet a large computational training or financial threshold that would include under 10 companies around the size of OpenAI and Anthropic. Both acts require frontier model developers to (1) publish a transparency report describing capabilities, intended uses, limitations, and risk assessments, and (2) create, implement, and publish frameworks for mitigating catastrophic risk, protecting against unauthorized access, using third-party evaluators, governing internal use, and responding to safety incidents.

B. EU APPROACH

The EU AI Act is a cross-sector comprehensive law that imposes obligations based on four tiers of risk: (1) **minimal risk** (no regulation), like video games or spam filters, which are not regulated; (2) **limited risk** (transparency), like applications generating or manipulating images, which require disclosures to inform users they are interacting with AI; (3) **high risk** (governance and transparency), like systems used in health, education, employment, and critical infrastructure, which have transparency, quality, oversight, and safety obligations; and (4) **unacceptable risk** (prohibited), like systems used to manipulate behavior, real-time biometric identification, and social scoring.

---

[43] Utah Code § 13-72-301 et seq. (effective May 1, 2024).
[44] Washington HB 1170 (effective Feb. 1, 2027).
[45] Washington HB 1168 (2025).
[46] Washington HB 2157 (2025); SB 6120 (2026).
[47] Washington HB 2667 (2025); SB 2684 (2026).
[48] N.Y. Gen. Bus. Law Art. 44-B (effective Jan. 1, 2027).
[49] California SB 53 (effective Jan. 1, 2026).

The EU AI Act also regulates general purpose models that can perform a wide range of tasks, imposing transparency, copyright, and safety and security obligations, as well as models designated as posing systemic risk, which must carry out additional testing.

V. DATA PRIVACY PROTECTIONS

Because a critical component of an AI system is its training data and other inputs, data privacy laws are a key mechanism for regulating AI systems. Key concerns with respect to AI-data privacy are similar to broader concerns about general data privacy, and involve data collection and retention, model training, data use, and transparency. Data privacy protections primarily arise from existing non-AI specific data privacy state and federal laws, with approximately twenty states having comprehensive data privacy laws.

A. FEDERAL LAW

There is currently no comprehensive federal data privacy law or AI-specific legislation. In 2022, Congress introduced a comprehensive data privacy act, the American Data Privacy and Protection Act (the "ADPPA") but the ADPPA was never enacted and faced strong opposition in part due to the grant of a private right of action and preemption concerns from states with stronger privacy protections.[50]

Federal protections are sector-specific and rely on existing data privacy protections. Currently, there is a patchwork of federal privacy legislation that protects data usage and privacy in specific contexts or industries that have been applied to the AI context. For example, the Children's Online Privacy Protection Act ("COPPA")[51] imposes data privacy restrictions on operators of websites or services when their content is "directed to children under 13 years of age."[52] The FTC has actively enforced and investigated COPPA concerns in the AI context where companies were marketing to children, collecting their personal information, or providing AI chatbots.[53]

Other existing federal laws may be ill-equipped to address developments in AI. AI may raise issues in the application of existing privacy statutes because AI may raise the bar for what is considered unidentifiable data, particularly where privacy statutes contain a reasonability or subjective test. Washington's My Health My Data Act, for example, defines "deidentified data" as "data that cannot reasonably be used to infer information about" an identifiable consumer.[54] For example, in the context of the Health Insurance Portability and Accountability Act ("HIPAA"),[55] which governs health data, a lawsuit against Google alleged HIPAA violations arising from otherwise de-identified health data because the health data could allegedly be re-

[50] Lydia Rudden, *Fragmented Data Privacy Laws: Time for Federal Legislation*, Boston College Intellectual Prop. & Tech. Forum (Jan. 8, 2025), https://lira.bc.edu/works/publication-article/5zdd1-78j83.
[51] 16 C.F.R. § 312 (2000).
[52] Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034, 2034 (Jan. 11, 2024).
[53] *E.g.*, Federal Trade Comm'n, *FTC Launches Inquiry into AI Chatbots Acting as Companions* (Sept. 11, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions#:~:text=The%20FTC%20inquiry%20seeks%20to,X.AI%20Corp.
[54] Chapter 19.373.010 RCW.
[55] Public Law 104-191, 100 Stat. 2548 (1996).

identified through AI.[56] The lawsuit was ultimately dismissed and upheld on appeal because the plaintiff failed to allege re-identification had actually occurred. Similarly, in the context of the Video Privacy Protection Act ("VPPA"), which prohibits video providers from sharing personally identifiable information, AI may be able to decode information that would not have previously been considered personally identifiable.[57] For example, AI may be able to recognize patterns in unredacted information to piece together redacted information.

B. STATE LAW

1. States also primarily rely on existing data privacy protections.

At least twenty states have enacted comprehensive data privacy laws regulating consumer or personal data—CA, CO, CT, DE, FL, IN, IA, MT, OR, TN, TX, UT, VA[58]—and others have broad data privacy laws with respect to specific types of data (e.g., health data). States with comprehensive data privacy laws already provide general rights to access, correct, delete, or opt out and cover particular types of personal data, e.g., biometric information that would be equally applicable to data used in AI systems, and these states have enacted AI-specific data privacy protections as gap fillers or to clarify the applicability to AI systems.

Washington does not have a general purpose, comprehensive data privacy law, but has enacted a comprehensive act governing health data, the My Health My Data Act.

2. AI-specific data privacy protections.

Washington. Washington has not enacted AI-specific data privacy protections but has enacted legislation clarifying that the Office of Privacy and Data Protection within the WaTech agency's review of major state agency projects involving personally identifiable information includes projects using artificial intelligence.[59] A bill proposed this year sought to impose data disclosure obligations on generative AI developers, including disclosure of the sources of data, but was adjourned in committee.[60]

Other states. Areas where state AI-specific data privacy protections have been enacted typically involve (a) procedural guardrails for particular forms of AI, including disclosure requirements and data-protection assessments, and (b) substantive rights to access, delete, or opt-out to the extent not already provided for in the state's existing data privacy laws. AI-specific data privacy protections include:

Automated Processes or Decision-making Technology (ADMT). This section focuses on the data privacy concerns related to ADMT. States regulating ADMT also provide, in the same regulations, procedural and substantive protections relating to the decisions made by ADMT

---

[56] *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561 (N.D. Ill. 2020).
[57] Ufonobong Umanah, *AI Tools Likely to Muddy Reach of Video Privacy Protection Law*, Bloomberg Law (Oct. 27, 2025), https://news.bloomberglaw.com/litigation/ai-tools-likely-to-muddy-reach-of-video-privacy-protection-law.
[58] *US State Privacy Legislation Tracker*, International Association of Privacy Professionals (Apr. 13, 2026), https://iapp.org/resources/article/us-state-privacy-legislation-tracker.
[59] Washington HB 2606 (effective June 11, 2026).
[60] Washington HB 2503.

depending on the type of data used and the risk associated with their use (e.g., critical infrastructure, healthcare, government, criminal justice decisions, employment decisions) addressed *infra* at VI.C, VII.B.

- Controllers of personal data must conduct and document a data protection assessment for certain high-risk activities and decision-making, including uses of ADMT.[61]

- Consent requirements are heightened for use of ADMT on children's personal data.[62]

Generative AI:

- Developers must disclose data used to train generative AI.[63]

- Data brokers must disclose whether they sold or shared consumer data to a developer of generative AI.[64]

Large Language Models (LLMs):

- Controllers of personal data must disclose whether they collect, use, or sell personal data for the purpose of training LLMs.[65]

Sector-specific:

- **Healthcare.** Patient data may not be used beyond intended and stated purpose.[66]

- **Employment.** Employers using ADMTs in employment decisions must disclose the type of data collected and the employer's data retention policy.[67]

- **Name image and likeness.** Many states also provide data or property protections in an individual's name, image, and likeness (NIL) that are also applicable to AI uses, *infra* at VIII.

Definitional:

---

[61] *E.g.*, 11 CCR § 7001 et seq. (effective Jan. 1, 2027); Col. Rev. Stat § 6-1-1301 (effective July 1, 2023); Conn. Gen. Stat § 42-515 et seq. (effective July 1, 2023); Del. Code tit. 6, § 12D-101 et seq. (effective Jan. 1, 2025); Florida SB 262 (effective July 1, 2024); Ind. Code. § 24-15-1 (effective Jan. 1, 2026); Ky. Rev. Stat. § 367.3611 et seq. (effective Jan. 1, 2026); Md. Code Ann. § 14-4601 et seq. (effective Oct. 1, 2025); Minn. Stat. § 325O et seq. (effective July 31, 2025); Montana Code Ann. § 30-14-2801 et seq. (effective Oct. 1, 2024); Nebraska LB 1074 (effective Jan. 1, 2026); N.H. Rev. Stat. § 507-H:8 (effective Jan. 1, 2025); N.J. Rev. Stat. § 56:8-166.4 et seq. (effective Jan. 15, 2025); Oregon SB 619 (effective July 1, 2024); R.I. Gen. Law § 6-48.1-1 et seq. (effective Jan. 1, 2026); Tenn. Code Ann. § 47-18-3301 (effective July 1, 2025); Tex. Bus & Com. Code § 541.051(b)(5)(C) (effective July 1, 2024); Va. Code Ann. § 59.1-577A(A)(5) (effective Jan. 1, 2023).
[62] Va. Code Ann. § 59.1-577A(A)(5) (effective Jan. 1, 2023).
[63] *E.g.*, California AB 2013 (effective Jan. 1, 2026).
[64] *E.g.*, Cal. Civ. Code § 1798.99.82 (effective Jan. 1, 2026).
[65] *E.g.*, Connecticut SB1295 (effective July 1, 2026).
[66] *E.g.*, Md. Code Ann., Ins. § 15-10B-05.1 (effective Oct. 1, 2025).
[67] *E.g.*, N.Y.C. Local Law 144 (effective Jan. 1, 2023).

- California has redefined "personal information" to clarify that information in various formats expressly including AI systems capable of outputting personal information is considered personal information.[68]

Remedies. Most States do not expressly provide private rights of action for violations of these AI data privacy protections, except in California for data breaches and in Washington under the My Health My Data Act. The primary means of enforcement is through the State, who may impose civil penalties (ranging from $5,000 to up to $50,000 per violation). One potential remedy that the FTC has sought in data privacy cases involves model disgorgement, which involves deleting or destroying models that used improperly obtained or invalid data.[69]

VI. SAFETY

Key public concerns with respect to safety-related AI harms involve general **consumer protection**, including deceptive and unfair practices, fraud, and deepfakes; **physical safety**, including torts, product liability, property damage and the use of products with integrated AI that may cause harm; and **high-risk decision-making**, including healthcare determinations, emergency services, critical infrastructure, emergency services, or in fields where reliance on misinformation or hallucinations can cause harm, e.g., medical or legal advice.

A. CONSUMER PROTECTION

1. Federal Law

Federal consumer protection AI protections primarily consists of agencies applying existing enforcement authority, including the FTC under Sections 5, 6, and 18 of the FTC Act to regulate unfair and deceptive practices in AI marketing and deployment, the CFPB under Consumer Financial Protection Act in regulating financial-sector AI tools, and the SEC under the Investment Advisers Act in regulating AI used in investment advice.

These agencies originally focused on "AI-washing" and other misleading claims about AI but have also addressed novel AI claims under their consumer protection authority, including challenging racially biased algorithms,[70] algorithmic pricing,[71] and addressing potential conflicts

[68] California AB 1008 (effective Jan. 1, 2025).
[69] Brandon LaLonde, *Explaining model disgorgement*, International Association of Privacy Professionals (Dec. 13, 2023), https://iapp.org/news/a/explaining-model-disgorgement.
[70] *FTC: Racially Biased AI Violates FTC Act*, Electronic Privacy Information Center (Apr. 20, 2021), https://archive.epic.org/2021/04/ftc-racially-biased-ai-violate.html.
[71] FTC, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

of interest for robo-advisors.[72] The FTC has imposed substantial remedies under its authority to regulate unfair and deceptive practices that include model or algorithmic disgorgement.[73]

Federal legislation has been limited to the Take It Down Act,[74] which criminalizes non-consensual deepfake pornography.

2. State Law

State consumer protections on AI-related harms continue to rely on existing consumer protection and deceptive and unfair practices laws, as well as data privacy laws that implicitly limit data use, but key areas where states have enacted AI-specific legislation include ADMT; algorithmic pricing; use of AI in advertisements (across industries); deepfakes, intimate images, and CSAM; chatbots and AI companions; obligations for social media platforms; and biometric information. These AI-specific laws focus on transparency, disclosure, and consent, with some laws requiring distributors of AI content to develop procedural guardrails that include training, reporting, and AI detection mechanisms. Other state laws expressly eliminate using AI as a defense to liability, but the defenses do not limit generally applicable law.

Washington. Washington recently enacted broad legislation covering generative AI providers with over 1,000,000 monthly users requiring that these providers include provenance data (data embedded into content) that allow users to determine whether content is AI generated.[75] Government agencies providing AI systems interacting with consumers must disclose that the consumer is interacting with AI. Washington has also enacted legislation regulating AI with respect to deepfakes, intimate images, CSAM, and chatbots. Bills have been introduced that broadly regulate high-risk decision-making that implicate consumer protection, but those bills were adjourned in committee.[76]

Safety and Automated Decision-making Technology (ADMT).

- Many states have enacted ADMT laws to address AI-related harms that include consumer protection issues, *infra* at VI.C, VII.B. These laws largely establish procedural and governance requirements.

- **Washington** has not enacted general legislation on ADMT. WaTech has issued guidance on government procurement and use of ADMT.[77]

Algorithmic or Surveillance Pricing. Algorithmic or surveillance pricing refers to the use of algorithms and consumer data to set individualized prices for goods and services. State Attorneys

---

[72] SEC, *SEC Proposes New Requirements to Address Risks to Investors from Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers* (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-140.

[73] Brandon LaLonde, *Explaining model disgorgement*, International Association of Privacy Professionals (Dec. 13, 2023), https://iapp.org/news/a/explaining-model-disgorgement.

[74] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, S. 146, 119th Cong. (enacted May 19, 2025).

[75] Washington HB 1170 (effective Feb. 1, 2027).

[76] *E.g.*, Washington SB 6284; Washington HB 2157; Washington SB 6120.

[77] WaTech, *Automated Decision Systems Procurement and Use Guidance* (Dec. 2023), https://watech.wa.gov/sites/default/files/2024-01/ADS%20Procurement%20Guidance%20-%2012-2023.pdf.

General, including in Washington, have used existing state unfair practices, antitrust, or privacy laws as a means of regulating or investigating algorithmic or surveillance pricing. For example, the California Attorney General has announced a broad investigative sweep focused on businesses' use of consumer information to set targeted, individualized prices under state privacy laws.[78] Privacy laws are likely to focus on disclosure or consent; antitrust and unfair practices laws are likely to focus on substantive limitations.

- **Washington.** Washington has not enacted legislation on algorithmic pricing, and a recent bill introduced in 2026 that sought to impose substantive limitations on algorithmic pricing on retail goods was adjourned in committee.[79] In 2025, the City of Seattle passed Ordinance 127241, that regulates algorithmic pricing for residential rent, and prohibits landlords from using aggregated nonpublic data in setting rents.

- **Other states.**

    - **Antitrust.** California amended its antitrust laws to prohibit "common pricing" algorithms, which involves multiple individuals using an algorithm using competitor data to set pricing.[80] California imposes criminal and civil penalties up to $6 million dollars and grants a private right of action that has lowered the standard of proof to a "plausible" conspiracy. New York prohibits residential landlords from setting prices, occupancy levels, or other lease terms based on software or algorithms performing a coordinating function among landlords, imposing criminal and civil penalties and a private right of action that includes indirect purchasers.[81]

    - **Privacy/Disclosures.** New York requires entities using algorithmic pricing using personal data specific to a consumer to clearly and conspicuously disclose to the consumer that algorithmic pricing was used.[82] Civil penalties may be up to $1,000 per occurrence but there is no private right of action.

    - **Dynamic Pricing.** Connecticut requires "transportation network" companies (like rideshare apps) using dynamic pricing to disclose to riders that dynamic pricing is in effect before the rider requests a ride, provide a fare estimator, provide a feature requiring the rider to confirm they understand dynamic pricing may apply, and refrain from charging more than 2.5x usual price during surge pricing.[83]

---

[78] *See, e.g.*, *On Data Privacy Day, Attorney General Bonta Focuses on Surveillance Pricing, Compliance with California Consumer Privacy Act*, State of California Dep't Justice Office of Att'y General (Jan. 27, 2026), https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-focuses-surveillance-pricing-compliance; *see also,* Wash. Office of the Att'y General, *Washington AG says RealPage and landlords conspired to harm tenants, violate Consumer Protection Act* (Apr. 3, 2025), https://www.atg.wa.gov/news/news-releases/washington-ag-says-realpage-and-landlords-conspired-harm-tenants-violate. s

[79] Washington SB 6312.

[80] California AB 325 (effective Jan. 1, 2026)

[81] N.Y. Gen. Bus. Law Art. 22, § 340-B (effective Dec. 15, 2025).

[82] N.Y. Gen. Bus. Law Art. 22-A, § 349-A (effective Nov. 10, 2025).

[83] Conn. Gen. Stat. § 13b-118 (effective Jan. 1, 2018).

Deepfakes, Intimate Images, and CSAM.

- **Washington.** Washington has enacted legislation extending criminalization of intimate image and CSAM laws to deepfakes or other content generated with AI.[84] Washington has also enacted legislation providing that individuals have a property right in their NIL, and providing criminal and civil remedies for forged NIL, including through the use of generative AI.[85]

- **Other states.**

    - **Deepfakes.** States have prohibited the use of deepfakes for certain purposes, including in furtherance of a crime or to harm (e.g., financial or reputational harm), to harass, or to mislead.[86] Remedies vary depending on the use of the deepfake and include criminal and civil penalties, equitable and monetary relief, and private rights of action.

        - **Political uses.** States have separately addressed the use of deepfakes, synthetic performers, or other AI-generated or altered content in political advertisement, requiring disclosure from distributors of the content that such content was generated by AI, particularly within certain proximity to an election (most often 90 days).[87] These prohibitions are enforced by the state with primarily civil monetary and equitable remedies and subsequent criminal penalties for repeat offenses.

        - **Commercial uses or advertisements.** While states may use existing laws on deceptive practices in advertisements, New York recently enacted a law expressly requiring disclosure of the use of synthetic performers (i.e., AI-generated actors) for commercial purposes or in advertisements.[88] The law imposes a civil penalty of $1,000 for a first violation and $5,000 for subsequent violations, but does not appear to provide a private right of action.

    - **Intimate images.** States addressing unlawful disclosure of intimate images of a person extend the prohibition to computer generated, identifiable images of the

[84] Washington HB 1999 (effective June 6, 2024).
[85] Washington SB 5886 (effective June 11, 2026); Washington HB 1205 (effective July 27, 2025).
[86] *E.g.*, Arizona HB 2394 (effective June 4 ,2024); New Hampshire HB 1432 (effective Jan. 1, 2025); New Jersey A3540 (effective Apr. 2, 2025); Texas SB 2373 (effective Sept. 1, 2025).
[87] Alabama HB172 (effective Oct. 1, 2024); Arizona, SB 1359 (effective June 4, 2024); California AB 2355 (effective Jan. 1, 2025); Co. Rev. Stat. 1-45-115.5 to 111.7 and 1-46-101 to 106 (effective July 1, 2024); Florida HB 919 (effective July 1, 2024); Hawaii SB 2687 (effective July 3, 2024); Ky. Rev. Stat. 117.001 (effective Dec. 1, 2025); Michigan HB 5144 (effective July 1, 2024); Michigan HB 5141 (effective Feb. 13, 2024); Mississippi SB 2577 (effective July 1, 2024); Montana SB25 (effective Oct. 1, 2025); Nev. Rev. Stat. 294A.347-95 (Jan. 1, 2026); New Hampshire HB 1596 (effective Mar. 27, 2024); N.M. Stat. Ann. § 1-19-26 et seq. (effective May 15, 2024); N.Y. Election Law § 14-106 (effective Apr. 20, 2024); N.D. Century Code, Ch. 16.1-10 (effective Aug. 1, 2025); Oregon SB 1571 (effective Mar. 27, 2024); RI Gen. Laws 17-30-1 to 4 (effective July 2, 2025); South Dakota SB 164 (effective July 1, 2025); Utah SB 131 (effective May 1, 2024); Vermont S23 (effective Mar. 5, 2026); Wis. Stat. § 11.1303 (effective Mar. 23, 2024).
[88] New York S8420A (effective June 9, 2026).

person.[89] Most states impose criminal and civil penalties, including equitable and monetary relief with private rights of action. Some states impose statutory damages ranging between $10,000 to over $100,000.[90]

- Since most states are extending existing prohibitions, the primary focus is on distributors of AI-generated content (e.g., websites).[91] Texas, however, is more AI-specific and has expanded liability to **developers**, **deployers**, and **payment processors** to the extent they have not taken measures to safeguard against prohibited uses, including training, reporting tools, and filtering tools.[92]

- A key derivative issue that may need to be addressed is what constitutes as "identifiable," and whether that term refers to identifiability by a human viewer or potentially by available AI systems.

- **CSAM.** States addressing CSAM expand the prohibition on child pornography in CSAM laws to include AI-generated depictions.[93] Most states impose criminal and civil penalties, including equitable and monetary relief with private rights of action.

Chatbots or AI companions.

- State laws focus on disclosure requirements to make clear the user knows they are not speaking with a human,[94] particularly in the commercial context,[95] in the mental health,

[89] *E.g.*, Arizona Rev. Stat. § 13-1425 (effective Sept. 25, 2025); California SB 926 (effective Jan. 1, 2025); Colorado SB 288 (effective Aug. 6, 2025); Delaware HB 353 (effective Aug. 7, 2024); Ga. Code § 16-11-90 (effective May 2, 2022); Hawaii SB 309 (effective June 23, 2021); Idaho Code § 18-6606); Indiana HB 1047 (effective Mar. 12, 2024); Iowa Code § 708.7 (effective July 1, 2024); 14 La. Rev. Stat. Ann. § 73.13 (effective Aug. 1, 2023); Massachusetts HB 4744 (effective June 20, 2024); Minnesota HF 1370 (effective Aug. 1, 2023); Mont. Code Ann. 45-5-6 (effective May 12, 2025); New York SB1042A (effective Nov. 28, 2023); North Carolina HB 591 (effective Dec. 1, 2024); N.D. Cent. Code § 12.1-27.1-01 (effective Aug. 1, 2025); Oklahoma 21 O.S. 2021 § 1040.13b (effective Nov. 1, 2025) (criminal); Pennsylvania SB 1213 (effective Dec. 28, 2024) (criminal); Texas HB 581 (effective Sept. 1, 2025); Texas SB 1361 (effective Sept. 1, 2023); Utah HB 148 (May 1, 2024); Vermont H 878 (effective June 6, 2024); Virginia HB 2678 (effective July 1, 2019); Washington HB 1999 (June 6, 2024); West Virginia SB 198 (July 9, 2025); Wy. Code § 6-4-307 (effective July 1, 2026).

[90] Colorado SB 288 (Aug. 6, 2025); *see also* Delaware HB 353 (effective Aug. 7, 2024) ($10,000 statutory damages); Minnesota HF 1370 (effective Aug. 1, 2023) ($100,000 statutory damages); N.D. Cent. Code § 12.1-27.1-01 (Aug. 1, 2025) ($10,000 statutory damages).

[91] *E.g.*, California SB 926 (effective Jan. 1, 2025); Indiana HB 1047 (Mar. 12, 2024); New York. SB1042A (effective Nov. 28, 2023); Wy. Code § 6-4-307 (effective July 1, 2026).

[92] Texas SB 441 (effective Sept. 1, 2025)

[93] *E.g.*, Alabama HB 168 (effective Oct. 1, 2024); Cal. Penal Code 1-9-7.5; Washington HB 1999 (effective June 6, 2024).

[94] Cal. Bus. & Prof. Code § 22601 et seq. (effective Jan. 1, 2026); N.Y. Gen. Bus. Law, Art. 47 (effective Nov. 5, 2025); Utah Code 13-75-101 to 106 (effective May 7, 2025) (disclosure required if asked).

[95] Cal. Bus. & Prof. Code § 17940-43; Maine 10 MRSA c. 239 (effective Sept. 24, 2025).

self-harm or other high-risk or regulated context,[96] or when the user is a minor.[97] Some states mandate that AI companions have a protocol for addressing suicidal ideation or self-harm and for referring to a crisis support specialist.[98] Some states provide a private right of action[99] in addition to enforcement by the State. Criminal penalties may be available in the self-harm context.[100]

- **Washington** recently enacted legislation requiring AI companion chatbot platforms provide a clear disclosure that a companion chatbot is artificially generated not human, and to have a public protocol for detecting and addressing self-harm or suicide, connecting users to crisis hotlines, and limiting manipulative or explicit content for minors.[101]

Social media platforms.

- California and Minnesota have enacted legislation imposing broad obligations on social media platforms.
    - California requires social media platforms to provide a user interface that can reliably indicate whether content was generated or altered by generative AI.[102] California imposes civil penalties enforceable by the State and grants a private right of action.
    - Minnesota requires social media platforms to provide information on the platform's algorithmic ranking system, including the algorithm's "signals" and how those algorithms assess content preferences and quality of content.[103] The algorithms' "signals," include information about a post (e.g., likes, comments, shares, saves), the account making the post (e.g., number of interactions with the account), and the viewing account's activity and history.[104] Minnesota's law is enforced by the State and expressly excludes a private right of action.
- Other states impose obligations on social media platforms relating to AI-generated sexual or political material.[105]

Sectoral.

---

[96] Cal. Bus. & Prof. Code § 22601 et seq. (effective Jan. 1, 2026); Illinois HB 1806 (effective Aug. 1, 2025); Nev. Rev. Stat. Chapter 433 (July 1, 2025); Utah Code 13-75-101 to 106 (effective May 7, 2025); Wy. Code § 6-4-701 (effective July 1, 2026).
[97] Cal. Bus. & Prof. Code § 22601 et seq. (effective Jan. 1, 2026); N.H. Chapter 270:1 (effective Jan. 1, 2026).
[98] N.Y. Gen. Bus. Law, Art. 47 (effective Nov. 5, 2025) (AI companion must contain a protocol to take reasonable efforts for addressing suicidal ideation or self-harm).
[99] Cal. Bus. & Prof. Code § 22601 et seq. (effective Jan. 1, 2026); N.H. Chapter 270:1 (effective Jan. 1, 2026).
[100] Wy. Code § 6-4-701 (effective July 1, 2026).
[101] Washington HB 2225 (effective Jan. 1, 2027).
[102] Cal. Bus. & Prof. Code § 22757 et seq. (effective Aug. 2, 2026).
[103] Minn. SF 4097 (effective July 1, 2025).
[104] *E.g.*, *Shedding More Light on How Instagram Works*, Adam Mosseri (June 8, 2021), https://about.instagram.com/blog/announcements/shedding-more-light-on-how-instagram-works.
[105] *E.g.*, Texas HB 441 (effective Sept. 1, 2025).

- **Real estate.** Several states require disclosure of the use of AI in real estate advertisements.[106]

- **Telecommunications.** California requires callers using automatic dialing-announcing to inform the person called if the prerecorded message uses an AI-generated or altered voice.[107]

AI as a defense.

- Utah amended its consumer protection law to clarify that it is not a defense to violations of the consumer protection law that generative AI made a prohibited statement or action or was otherwise used in furtherance of prohibited conduct.[108]

- California restricts using AI as a defense more broadly, enacting legislation establishing AI is not a defense in any civil action alleging harm to a plaintiff.[109] California's statute clarifies that it does not limit a defendant's ability to assert other defenses, including evidence related to causation, foreseeability, or comparative fault.

B. PHYSICAL SAFETY (TORTS, PRODUCT LIABILITY)

1. Federal Law

Consistent with federal law generally governing physical safety, regulation of safety in the AI-specific context has been limited to specific industries with existing federal oversight, primarily involving product liability. For example, the Food and Drug Administration (FDA) has exercised oversight over AI- or machine learning-enabled medical devices[110] and use of AI in drug development.[111] As another example, the National Highway Traffic Safety Administration (NHTSA) exercises oversight into AI used in vehicles.[112]

2. State Law

State laws governing physical safety rely on existing criminal, tort, and product liability laws. Tort and product liability laws rely on statutory and flexible common law principles, e.g., negligence, as applied to AI. AI-specific state laws concerning physical safety have been limited

[106] Cal. Bus. & Prof. Code § 10140.8 (effective Jan. 1, 2026); S.C. Code Ann. § 40-57-820 (effective May 21, 2024); Wis. Stat. § 452.136(1m) (effective Jan. 1, 2027).
[107] California AB 2905 (Jan. 1, 2025).
[108] Utah Code § 13-75-102 (effective May 7, 2025).
[109] Cal. Civ. Code § 1714.46.
[110] U.S. Food & Drug Admin., *Artificial Intelligence-Enabled Medical Devices* (Mar. 4, 2026), https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices.
[111] U.S. Food & Drug Admin., *Artificial Intelligence for Drug Development* (Jan. 14, 2026), https://www.fda.gov/about-fda/center-drug-evaluation-and-research-cder/artificial-intelligence-drug-development.
[112] *See, e.g.*, U.S. Dep't of Transportation, *Trump's Transportation Secretary Unveils New Automated Vehicle Framework as Part of Innovation Agenda* (Apr. 24, 2025).

to clarifying that the use of AI is not a defense to existing theories of liability.[113] Remedies are limited to criminal enforcement and civil tort remedies.

Challenges applying existing tort and product liability doctrines to AI. AI has created challenges in applying existing tort and product liability doctrines, including how to assign fault when the harm or product incorporates AI. For example, challenges include determining who in the multi-party development and integration chain is responsible (e.g., a car manufacturer or the developer of an integrated self-driving system); if use of an AI system requires human input, determining to what extent the human is responsible; since AI decision-making can be a black box and involves self-learning, how to tell if the system performed as expected (design defect) or was improperly made (manufacturing defect), and in either case, how to determine which entity would be responsible.

Doctrine	AI Challenges
Negligence	Standard of care and foreseeability are difficult to establish when AI is intended to act autonomously and outputs are unexplainable or unpredictable. Questions exist about what standard of care applies when AI is used. Causation can be difficult to establish due to AI's black-box self-learning process and multi-party development and integration chains (developer vs. deployer vs. distributor vs. others in the product development or use). These standards may also be difficult to apply in situations involving both AI and human input, e.g., partially self-driving cars.
Breach of warranty	Difficulties in classifying AI as product or as a service (which determines whether state-law versions of Article 2 of the UCC, which governs the sale of goods, applies).
Failure to warn	The more general and powerful an AI system is, the more difficult it can be for a developer to sufficiently anticipate foreseeable uses and warn users.
Strict liability	Requires product to reach user without substantial change but is complicated by AI's black-box self-learning process and multi-party development and integration chains.

Options for mitigating the challenges or risks associated with AI. Proposals and legislation have included creating a rebuttable presumption of causation against **developers** or **deployers** of high-risk AI systems;[114] imposing strict liability on developers, deployers, or distributors; mandating AI-related insurance; creating a compensatory fund for specific uses (e.g., automated vehicles); expressly allocating or requiring allocation of liability between AI actors; requiring guardrails, including quality assurance testing, human oversight, or

[113] *E.g.*, Cal. Civ. Code § 1714.46 (effective Jan. 1, 2026) (use of AI is not a defense in civil actions); Utah Code § 13-75-102 (effective May 7, 2025) (use of AI is not a defense to consumer protection violations); Wy. Code § 6-1-206 (effective July 1, 2026) (AI is not a defense to criminal charges).
[114] *E.g.*, European Commission, *Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)* (Sept. 28, 2022), https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf.

identification of a responsible individual; and/or requiring developers of high-risk AI systems disclose potential evidence in systems suspected of having caused damage.

Autonomous vehicles. A key area where physical harms arise from AI use involves automated vehicles (AVs) or vehicles using automated driving systems (ADS). While most states rely on existing tort and product liability doctrines to protect consumers, the role of AI complicates questions of liability.

- Most states regulate AVs or ADS, including with respect to testing, reporting, and data concerns. Tennessee has enacted legislation expressly shifting liability from the driver to the manufacturer by specifying that highly or fully-autonomous ADS is considered the driver for liability purposes when it is fully engaged and properly operated.[115] Many other states have allowed automated vehicles (AVs) to be cited with traffic violations.[116]

- In *Benavides* v. *Tesla*,[117] a jury returned a verdict totaling $243 million against Tesla in an action where a distracted driver driving a Tesla in full autopilot mode failed to stop at a stop sign, hit a parked car, and killed or seriously injured two pedestrians. The award was based on a jury apportionment of 1/3 fault to Tesla on the basis that the autopilot technology was defective (design defect) (the driver previously settled out of court). Notably, the Florida court granted summary judgment dismissing the manufacturing defect claims because there was no evidence the autopilot departed from Tesla's intended design and the negligent misrepresentation claims because Tesla did not owe a duty of care to the plaintiffs.

C. HIGH-RISK DECISION-MAKING AND USE OF AI SYSTEMS

ADMT and other AI systems can pose risks to health and safety, including AI components in critical infrastructure or critical harms (e.g., chemical or biological systems), ADMT or AI-guided healthcare (e.g., medical decision-making, or robot-assisted surgery) or other professional operations that may cause harm (e.g., legal or financial advice).

1. Federal Regulation

Federal regulation has largely consisted of agency oversight and regulation, in areas including AI use in government operations, managing physical and cyber security, and critical infrastructure.[118] Agencies are required to inventory and report their planned and existing use of AI in government operations in a yearly Federal Agency Artificial Intelligence Use Case

[115] Tenn. Code Ann. § 55-30-106 (effective June 6, 2017).
[116] Cal. Veh. Code § 38752.
[117] *Benavides* v. *Tesla*, No. 1:21-cv-21940 (S.D. Fla. Aug. 4, 2025).
[118] *E.g.*, Report to Congressional Addressees, U.S. Gov't Accountability Office, *Artificial Intelligence: DHS Needs to Improve Risk Assessment Guidance for Critical Infrastructure Sectors* (Dec. 2024), https://www.gao.gov/assets/gao-25-107435.pdf; CISA, *Principles for the Secure Integration of Artificial Intelligence in Operational Technology* (Dec. 4, 2025).

Inventory repository[119] initiated by Executive Order 13960 and administered by the Office of Management and Budget.[120]

2. State Regulation

Apart from existing criminal, civil, and regulatory enforcement mechanisms, State legislative protections from safety concerns arising from systems or decision-making integrating AI have involved governance, disclosure, and opt-out requirements for ADMT and AI use in government function, and in some states, sector-specific requirements for ADMT and AI use for providers of key services, including healthcare.

Washington has not enacted legislation specifically regulating high-risk AI uses involving safety.

AI Use in the Public Sector:

- Several states have enacted legislation to ensure the safety of AI use in the public sector, requiring governments to inventory high-risk AI uses or ADMT, including functions, benefits, data usage, and risk mitigation measures,[121] and in some states also requiring the establishment of policies and procedures concerning the development, procurement, implementation, and impact assessment of AI systems.[122]

- Other states have prohibited government use of particular AI platforms or of particular businesses offering AI-related services.[123]

- These statutes are broad enough to regulate the use of AI in government to the extent the use affects individuals' rights, e.g., access to benefits, discrimination, etc., *see infra* at VII.

Critical Infrastructure. Montana requires that where critical infrastructure facilities are controlled by a critical AI system (i.e., substantial factor in making consequential decisions), the deployer must develop risk management policy that considers the NIST AIRMF, ISO 4200, or another recognized risk management framework.[124] Similarly, California requires its Office of Emergency Services to prepare risk analysis of potential threats posed by generative AI to critical infrastructure.[125]

---

[119] The 2025 Federal Agency AI Use Case Inventory is available at https://github.com/ombegov/2025-Federal-Agency-AI-Use-Case-Inventory.
[120] Exec. Order No. 13960, 85 Fed. Reg. 78939 (Dec. 3, 2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.
[121] Cal. Gov. Code § 11546.45.5 (effective Jan. 1, 2024); Delaware HB 233 (effective July 17, 2024).
[122] Connecticut SB 1103 (effective July 1, 2023); Ky. Rev. Stat. §§ 42.720–42.742 (effective Dec. 1, 2025); Maryland SB 818 (effective July 1, 2024); New York S 7543B (effective Dec. 21, 2024); Tex. Ch. 2054 Gov. Code, Subch. S (effective Sept. 1 , 2025); Vermont H410 (effective July 1, 2022).
[123] Indiana SB256 (effective July 1, 2026) (foreign adversaries); Kansas SB 2313 (prohibits DeepSeek);
[124] Montana SB212 (effective Apr. 16, 2025).
[125] California SB 896 (effective Jan. 1, 2025).

Professional Service Providers:

- **Healthcare providers.** Disclosure and consent requirements are the focus on states regulating AI use for healthcare providers. For example:
    - California requires healthcare providers using generative AI in clinical patient communications to disclose the use of AI and provide instructions on how a patient may contact a human healthcare provider, except for written communications reviewed by a licensed healthcare provider.[126] California also extends prohibitions on unauthorized healthcare practice to AI technology providers.[127]
    - Texas allows healthcare providers to use AI for diagnostic purposes, conditioned on review by the healthcare provider and disclosure to the patient.[128]
    - Other states have similar requirements for mental and behavioral healthcare providers.[129]
- **Other professional services.** State licensing bodies governing professional services (legal, financial) and professional trade organizations regulate or offer guidance on the use of AI in the practice of those services.[130]

VII. CIVIL RIGHTS

Key concerns with respect to civil rights involve use of AI algorithms in decision-making processes in ways that may intentionally or unintentionally violate civil rights or inappropriately deny access to benefits. These involve concerns in criminal justice (e.g., predictive policing, facial and biometric recognition technology) and benefits or other decisions related to housing, employment, disability, credit, and workers' rights. AI systems can impair civil rights or reflect and reinforce biases against protected classes based on low-quality or biased underlying training data, prompt drafting, and model parameters. Because many AI systems lack transparency in how decisions are made, determining whether an AI system is fair may also be difficult.

AI systems may also pose difficult regulatory questions with respect to preserving rights traditionally afforded to individuals, including, for example, the interplay between the First Amendment and restrictions on AI-assisted output that may be considered speech (e.g., AI chatbots).

---

[126] Cal. Gov. Code § 1339.75 (effective Jan. 1, 2025).
[127] Cal. Bus. & Prof. Code § 4999.9 (effective Jan. 1, 2026).
[128] Texas S.B. 1188 (effective Sept. 1, 2025).
[129] Illinois HB1806 (effective Aug. 1, 2025); Nev. Rev. Stat. ch. 629 (effective July 1, 2025); Nev. Rev. Stat. ch. 391 (effective July 1, 2025) (same for school counselors).
[130] *E.g.*, American Bar Association, *Addressing Legal Challenges of AI, Report on the Impact of AI on the Practice of Law* (Dec. 2025), https://www.americanbar.org/content/dam/aba/administrative/center-for-innovation/ai-task-force/2025-ai-task-force-year2-report.pdf.

A. FEDERAL LAW

No federal legislation exists addressing AI-specific civil rights harms, but federal agencies have been active in issuing guidance on, investigating the potential for, and enforcing AI-related violations of civil rights or related federal laws, including Title VII governing employment discrimination, the Americans with Disability Act (ADA), and the Fair Credit Reporting Act (FCRA).[131] For example:

- Nine federal agencies[132] issued a joint statement announcing active monitoring of automated systems that "contribute to discrimination and otherwise violate federal law."[133]

- DHS Directive 139-08 prohibits using AI as the sole basis for DHS law enforcement actions (arrests, searches, citations, denial of benefits) and mandates governance, testing, incident reporting, and compliance requirements for AI use.[134]

- DOJ issued a Final Report on AI in criminal justice that identifies key risks and best practices for AI use in criminal justice.[135]

Shifting federal policy on AI regulation and on civil rights issues, including DEI, may change the extent to which federal agencies enforce AI-related civil rights harms.[136]

B. STATE LAW

State law addressing civil rights has primarily focused on use of AI or ADMT in consequential decisions like employment, healthcare, and access to benefits, and government use of AI, including law enforcement. Civil rights laws predominantly arise from the U.S. Constitution, state constitution, and federal and state statutes that address issues including discrimination, disability, housing rights, workers' and employment rights. Washington's civil rights laws include the Washington Law Against Discrimination ("WLAD"), which covers employment, housing and other real estate transaction, credit transactions, insurance transactions, and public accommodations that protects various classes of groups from discrimination depending on the activity involved.[137] Other legislation provides civil rights protections for

---

[131] Dep't of Justice, *Artificial Intelligence and Civil Rights*, https://www.justice.gov/archives/crt/ai (compiling DOJ guidance and enforcement actions related to civil rights).
[132] The nine agencies included: Consumer Financial Protection Bureau (CFPB), DOJ, Equal Employment Opportunity Commission (EEOC), FTC, Department of Education (DOE), Department of Health and Human Services (DHHS), Department of Homeland Security (DHS), Housing and Urban Development (HUD), and Department of Labor (DOL).
[133] Rohit Chopra, Director of the CFPB, *et al.*, *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems* (Apr. 4, 2024), https://www.justice.gov/archives/crt/media/1346821/dl?inline.
[134] Dep't of Homeland Security, Dir. 139-08 (Jan. 15, 2025) (titled "Artificial Intelligence Use and Acquisition").
[135] Dep't of Justice, Final Report, Artificial Intelligence and Criminal Justice (Dec. 3, 204), https://www.justice.gov/olp/media/1381796/dl.
[136] *See* Exec. Order 14319, 90 Fed. Reg. 35389 (July 23, 2025) (titled "Preventing Woke AI in the Federal Government"), https://www.federalregister.gov/documents/2025/07/28/2025-14217/preventing-woke-ai-in-the-federal-government.
[137] Ch. 49.60 RCW.

pregnant employees,[138] civil rights protections for job applicants who have been involved in the criminal legal system,[139] and provides equal opportunity for protected classes to vote.[140] Various agencies enforce these laws. For example, the Washington State Human Rights Commission and the Attorney General's Office administer and enforce WLAD, and the Washington State Department of Labor & Industries enforces workplace rights.

Washington has enacted legislation specific to use of AI in healthcare prior authorization, prohibiting using AI as the sole means of determining whether to deny, delay, or modify healthcare services and requiring human review.[141]

ADMT

- Many states have enacted cross-sectoral legislation regulating ADMT use that involves using consumer's personal data in significant decisions impacting the consumer, including financial or lending services, housing, education, employment, and healthcare decisions.
    - Most of these states approach ADMT regulation from a data privacy perspective, *supra* at V.B.2, and provide consumers opt-out, access, delete, and similar rights and require data protection assessments, with civil penalties but no private right of action.[142]
    - **Colorado** broadly requires **developers** and **deployers** of AI systems making consequential decisions (e.g., access to benefits like healthcare, employment, lending, housing) take reasonable care to protect consumers from algorithmic discrimination.[143] Requirements include: **developers** have documentation requirements relating to model characteristics and risk management measures and transparency obligations to deployers; **deployers** have disclosure obligations, must provide consumers right to correct or access information and appeal adverse decisions; and must implement a risk management program, impact assessments, and address transparency obligations to consumers.

[138] RCW 43.10.005.
[139] 49.94 RCW.
[140] 29A.92 RCW.
[141] Washington SB 5395 (effective June 11, 2026).
[142] *E.g.*, Col. Rev. Stat. § 6-1-1301 et seq. (July 1, 2023); Conn. Gen. Stat. § 42-515 et seq. (effective July 1, 2023); Del. Code tit. 6, § 12D-101 et seq.; Florida SB 262 (effective July 1, 2024); Ind. Code § 24-15-1 (effective Jan. 1, 2026); Ky. Rev. Stat. § 367.3611 et seq. (effective Jan. 1, 2026); Md. Code Ann. § 14-4601 et seq. (effective Oct. 1, 2025); Minn. Stat. § 325O et seq. (effective July 31, 2025); Mont. Code. Ann. § 30-14-2801 et seq. (effective Oct. 1, 2024); Nebraska LB 1074 (effective Jan. 1, 2026); N.H. Rev. Stat. § 507-H:8 (effective Jan. 1, 2025); N.J. Rev. Stat. § 56:8-166.4 et seq. (effective Jan. 15, 2025); Oregon SB 619 (July 1, 2024); R.I. Gen. Law § 6-48.1-1 et seq. (effective Jan. 1, 2026); Tenn. Code Ann. § 47-18-3301 (effective July 1, 2025); Tex. Bus. & Com. Code § 541.051(b)(5)(C) (effective July 1, 2024); Va. Code Ann. § 59.1-577A(A)(5) (Jan. 1, 2023).
[143] Co. Rev. Stat. § 6-1-1701 et seq. (June 30, 2026).

- In California:
  - **developers** and **deployers** are required to conduct a risk protection assessment when making significant decisions or training ADMT,
  - **distributors** to businesses using the ADMT are required to provide information necessary for the business to conduct the risk assessment, and
  - **deployers** must disclose ADMT use, disclose information regarding the ADMT, and provide a right to opt out.[144]
  - California provides civil penalties and a private right of action for data breaches.
- **Washington** has not enacted legislation specifically regulating AI usage in making consequential decisions, and two bills introduced this year that were similar to the Colorado AI Act were adjourned in session.[145]

- Texas prohibits development or deployment of AI systems with the intention of harmfully manipulating human behavior, intentionally discriminating against individuals, or intentionally infringing on their rights.[146]

Government:

- **Washington** requires government agencies using AI systems to interact with consumers to disclose to each consumer that they are interacting with an AI system,[147] and prohibits state agencies from using facial recognition systems without certain reporting or deployment requirements.[148] Washington has not enacted broad legislation regulating use of AI within the government.

- Several states, *supra* at VI.C.2., require inventory of high-risk AI used in government operations that detail functions, benefits, data usage, and risk mitigation strategies, including risk of unlawful discrimination.

- **Montana** expressly prohibits government entities from using AI to harm or discriminate against people or to surveil public spaces (with exceptions).[149] Government entities must disclose certain AI use, and AI-assisted decisions impacting rights and privileges must be reviewed by a human.

- Several states prohibit state agencies using real-time and remote biometric identification systems (like facial recognition technology (FRT)) for surveillance, except with a

[144] California 11 CCR § 7001 et seq. (effective Jan. 1, 2027).
[145] Washington HB 2157; Washington SB 6120.
[146] Texas HB 149 (effective Jan. 1, 2026) (TRAIGA).
[147] Washington HB 1170 (effective Feb. 1, 2027).
[148] Washington Chapter 43.386 RCW.
[149] Montana HB 178 (effective Oct. 1, 2025).

warrant,[150] and prohibit deceptive, discriminatory, or harmful AI uses.[151] Agencies must ensure AI-assisted decisions are reviewed by a human and must provide disclosures of AI use.

- **Texas** requires disclosure of government AI use with consumers, prohibits any form of AI-based social scoring system or biometric surveillance that could infringe rights.[152]

Law enforcement and criminal justice

- **Washington** has enacted legislation setting forth requirements for the use of facial recognition services, including reporting requirements, testing requirements, human review, and prohibiting use of facial recognition based on protected characteristics.[153] Localities and local law enforcement have issued independent regulations concerning the use of AI in law enforcement.[154]

- **California** requires law enforcement agencies preparing AI-generated official reports to disclose and to retain an audit trail.[155] Vendors receiving information provided by law enforcement may not use AI in processing that information except for law enforcement purposes or by court order.

- **Utah** requires law enforcement agencies to have policies concerning use of generative AI and requires reports and records to disclose if generative AI was used and to contain a certification of review for accuracy.[156]

- **Virginia** requires that criminal justice decisions, including pre-trial detention, release, sentencing, and parole, be made by a human decision-maker even if AI is used for recommendations or predictions.[157]

Employment and Workers' Rights

- **Washington** has not enacted legislation specifically regulating employment and workers' rights, and two recently introduced bills involving notifying employees before using AI tools to assist in performance evaluations[158] and restricting employee monitoring and employer use of ADMT were unsuccessful.[159]

---

[150] *E.g.*, Washington Chapter 43.386 RCW.
[151] New Hampshire HB 1688 (July 1, 2024).
[152] Texas HB 149 (effective Jan. 1, 2026) (TRAIGA).
[153] Washington SB 6280 (effective July 1, 2021).
[154] *See, e.g.*, Email from King County (WA) Prosecuting Attorney's Office re Axon Draft One (2024), https://pceinc.org/wp-content/uploads/2025/01/20240920-Email-to-Police-Chiefs-re-Axon-Draft-One-King-County-Prosecuting-Attorney-Dan-Clark.pdf.
[155] Cal. Pen. Code § 13663 (effective Jan. 1, 2026).
[156] Utah Code § 53-25-601 to 602 (effective May 7, 2025).
[157] Va. Code § 19.2-11.14 (effective June 6, 2025).
[158] Washington SHB 2144 (2026).
[159] Washington SHB 1672 (2025).

- **General.** States have enacted employment legislation that declares failure to disclose use of AI in an employment decisions a civil rights violation and prohibits use of AI that has the effect of discrimination.[160]

    - State regulatory bodies have issued regulations clarifying that existing antidiscrimination laws apply in the AI context,[161] prohibit uses of ADMT that discriminate against protected classes, and require records maintenance and data.[162]

    - In New York City, employers are restricted to AI employment decision tools that have been subject to a recent bias audit that is publicly available, requires disclosures to job candidates and allows candidates to opt out.[163]

- **Government employment.** New York has enacted specific legislation for government employment that requires disclosures of AI used in employment decisions,[164] and prevents AI-use from resulting in adverse decisions that result in job loss or transfer, or impair collective bargaining agreements, work hours, wages or benefits.[165]

- **Video interviews.** Illinois requires employers using AI to analyze video interviews to disclose to applicants, explain how the AI works, and get the applicant's consent.[166]

Healthcare and Insurance:

- **Washington** has enacted legislation specific to the use of AI in healthcare prior authorization, prohibiting using AI as the sole means of determining whether to deny, delay, or modify healthcare services and requiring human review.[167]

- **California** requires healthcare service plans and disability insurers using AI for utilization reviews to ensure compliance with requirements involving the information used, discrimination, and fair and equitable application.[168]

- **Texas** prohibits utilization review agents from using AI to make, wholly or partly, an adverse determination.[169]

- **Maryland** requires insurers, healthcare service plans, and any other providers of health benefit plans:

---

[160] Illinois HB 3773 (Jan. 1, 2026).
[161] *E.g.*, N.J. Admin. Code 13:16.
[162] *E.g.*, Cal. Code Reg., tit. 2 § 11008 et seq.
[163] N.Y.C. Local Law 144 (effective Jan. 1, 2023).
[164] New York A433 (effective July 1, 2025).
[165] New York S8831 (effective Feb. 13, 2026).
[166] 820 Ill. Comp. Stat 42 (effective Jan. 1, 2020) (Artificial Intelligence Video Interview Act).
[167] Washington SB 5395 (effective June 11, 2026).
[168] Cal. SB 1120 (effective Jan. 1, 2025).
[169] Texas SB 815 (effective Sept. 1, 2025).

- provide quarterly reports on governance information including number of adverse decisions and use of AI;
- develop policies and procedures governing use, and oversight;
- regularly review and revise performance, use and outcomes of AI;
- make AI systems open for inspection or audit;
- ensure AI bases determinations on patient-specific clinical information and not a group dataset;
- have human oversight in decision determinations; and
- ensure AI does not result in discrimination and is fair and equitable.[170]

- **Colorado** prohibits insurance providers from using AI that unfairly discriminates and requires the insurance commissioner to adopt rules requiring insurers to demonstrate their use of AI does not result in unfair discrimination.[171]
- **Indiana** prohibits insurers from using AI as the sole basis for health claim determinations and requires insurers to disclose when AI is used to make an adverse prior authorization or claim determination.[172]
- **Virginia** has mandated regulations requiring hospitals and nursing facilities to ensure permissible access to and use of virtual assistants.[173]

VIII. INTELLECTUAL PROPERTY AND OWNERSHIP

Intellectual property (IP) is primarily governed by federal law, with state law serving as a gap filler in areas including trade secrets, right of publicity and name and image likeness (NIL). At the federal level, IP includes four main forms of legal protection: patents, copyrights, trademarks, and trade secrets.

Patents are IP in inventions, which means "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." Patents must be granted by the U.S. Patent and Trademark Office (USPTO).

Copyrights are IP granted to creators of content ("original works of authorship") and provides creators exclusive rights to their creative work, including the right to reproduce, perform or display it, distribute it, and prepare derivative works. A copyright holder does not need to apply to the government to obtain a copyright, which is formed once the work is created

[170] Md. Code Ann., Ins. §§ 15-10-A-06, 15-10B-05.1 (effective Oct. 1, 2025).
[171] Co. Rev. Stat 10-3-1104.9 (effective July 6, 2021).
[172] Indiana HB 1271 (effective July 1, 2026).
[173] Va Code Ann. § 32.1-127 (effective July 1, 2021).

and fixed in a tangible form. Copyrights have two primary limitations. "Fair use" permits certain socially valuable or protected uses that would otherwise be copyright infringement (e.g., using copyrighted works in a parody). "Transformative" use is use that has a different purpose or alters the original work with new expression or meaning.

Trademarks are IP in a "word, name, symbol, or device" that identifies a particular business's goods or services. Trademarks must be registered with the USPTO, but there are some protections for unregistered trademarks. Trademark law seeks to protect consumers from businesses misrepresenting the source of goods or services and, as with all other IP, encourage brands to invest in the quality of their goods and services.

AI-specific federal law regarding intellectual property has been regulated by the USPTO[174] and the US Copyright Office[175] through guidance and decisions, with private litigation developing AI-specific application of intellectual property laws. Key issues in applying intellectual property laws to AI include to what extent generative AI constitutes human authorship, whether training AI models is fair use, AI use in music, and ownership. There has been significant private litigation to determine whether IP was valid, or infringed upon, particularly in the use of IP in training materials or in the USPTO or Copyright Office's refusal to grant IP status.[176]

State law on AI in intellectual property has been limited, and enacted laws relate primarily to NIL issues, particularly in states with large entertainment industries supporting new legislation. States provide both civil penalties and private rights of action, as well as relief from unenforceable contract provisions.

Ownership:

- **Washington** has not enacted legislation setting rules for AI ownership.
- **Arkansas** has enacted a statute that sets default rules for AI ownership:[177]
    - The person who provides input or directive to a generative AI tool is the owner of the content generated, unless the content infringes upon existing IP.

---

[174] Dep't of Commerce, Patent & Trademark Office, Revised Inventorship Guidance for AI-Assisted Innovation, Docket No. PTO-P-2025-0014 (Nov. 28, 2025), https://public-inspection.federalregister.gov/2025-21457.pdf?utm_campaign=subscriptioncenter&utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=.

[175] U.S. Copyright Office, Copyright and Artificial Intelligence, Part 1: Digital Replicas (July 2024), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf; U.S> U.S. Copyright Office, Copyright and Artificial Intelligence, Part 2: Copyrightability (Jan. 2025), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf; U.S. Copyright Office, Copyright and Artificial Intelligence, Part 3: Generative AI Training (Pre-Publication Version) (May 2025), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf.

[176] *E.g.*, *Thaler v. Perlmutter*, 687 F. Supp. 3d 140, 146 (D.D.C. 2023); *In Re OpenAI, Inc., Copyright Infringement Litig.*, No. 25-MD-3143, 2025 WL 3003339 (S.D.N.Y. Oct. 27, 2025); *Disney v. Midjourney*, No. 2:25-CV-05275 (C.D. Cal.)

[177] Ark. Code § 18-4-101 (effective Apr. 21, 2025).

- The person who provides data or input to train a generative AI tool is the owner of the trained model, unless the data was unlawfully acquired or the person transferred ownership by agreement.

- A person's employer owns generated content or trained model where person is directed to use the AI tool for the purpose of training or generating content as part of their employment duties.

Name and Image Likeness (NIL):

- **Washington** has enacted legislation providing that individuals have a property right in their NIL, and providing criminal and civil remedies for forged NIL, including through the use of generative AI.[178]

- **Property right.**

    - **Tennessee's** Ensuring Likeness, Voice, and Image Security (ELVIS) Act, was an early mover, providing that every individual has a property right in their NIL, and establishing a civil cause of action for uses of AI that infringes on the NIL.[179] Other states have since enacted similar laws.[180]

- **Privacy right.** Other states approach NIL AI use as primarily a privacy issue and have enacted legislation that extends similar privacy protections to AI generated uses of NIL.[181]

- **Contracts.** Several states with key entertainment industries have made professional services contracts unenforceable where they allow for use of a digital replica in place of work a performer would have done in person, where the person is not represented by counsel or a union or the provision is not reasonably specific as to the intended uses of the replica.[182]

    - **New York** requires clear, separate written consent from models to use their digital replica, detailing scope, purpose, rate of pay, and duration.[183]

- **Deceased performers.** Several states prohibit using a deceased performer's digital replica without consent.[184]

---

[178] Washington SB 5886 (effective June 11, 2026); Washington HB 1205 (effective July 27, 2025).
[179] Tenn. Code Ann. § 47-25-1101 (effective July 1, 2024).
[180] Illinois HB 4875 (effective Aug. 9, 2024); Mt. Code Ann. § 30-14-1 (effective Jan. 1, 2026);
[181] N.Y. Civ. Rights Law § 50 et seq. (Apr. 20, 2024); Utah Code § 45-3-2 et seq. (effective May 7, 2025).
[182] California AB 2602 (effective Jan. 1, 2025); Illinois HB 4762 (effective Aug. 9, 2024); New York Gen. Ob. Ch. 24-A, Art. 5, Tit. 3 (effective Jan. 1, 2025)
[183] New York S 9832 (effective June 19, 2025).
[184] California AB 1836 (effective Jan. 1, 2025); New York S8391 (effective Dec. 11, 2025).