SQUIRE PATTON BOGGS

US AI law: 2026 Midyear state update

In this second of a three-part series on US data law updates, we cover state laws related to development and deployment of artificial intelligence (AI) systems. In Part I, we focused on the trend of more restrictive state consumer privacy laws. In this Part II, we review how state AI laws are focused on the most potentially harmful uses of AI systems. While state legislatures enacted a steady stream of new and amended consumer privacy laws during Q1 and Q2, legislative activity on AI and AI-related laws accelerated during May through August. This article focuses on some of the more significant developments during this period.

State AI laws in force January 1, 2026

The California legislature continues to lead the states in introducing and enacting AI related laws.

Several new harm-focused AI laws entered into force on January 1, 2026, including:

- The California Companion Chatbots Act, California Artificial Intelligence Training Data Transparency Act and California Transparency in Frontier AI Act (TFAIA), each of which are discussed below
- An amendment to the California AI Transparency Act (Cal. Bus. & Prof. Code § 22757, et seq) extended its in-force date from January 1, 2026, to August 2, 2026 (also discussed below)
- California Artificial Intelligence Defense (subject to some exclusions, in an action against a defendant who developed, modified or used AI that is alleged to have caused a harm to the plaintiff, it shall not be a defense and the defendant may not assert, that the AI autonomously caused the harm to the plaintiff)
- California Health Advice from AI (AI technology providers must comply with pre-existing prohibitions on the use of any terms, letters or phrases to indicate, or imply (i) possession of a license or certificate to practice a healthcare profession without one or (ii) when true, the services being offered are being provided by a licensed or certified health care professional)
- Cal. Civ. Code § 1714.46 (in an action against a defendant who developed, modified, or used AI that is alleged to have caused a harm to the plaintiff, it shall not be a defense and the defendant may not assert, that the AI autonomously caused the harm to the plaintiff)
- California Real Estate Digitally Altered Images Disclosures (requires a real estate broker or salesperson, or person acting on their behalf, who includes a digitally altered image in an advertisement or other promotional material for the sale of real property to include a statement disclosing that the image was altered and access (link, QR code, etc.) to the original, unaltered image)

The Texas Responsible AI Governance Act (TRAIGA) also went into force on January 1, 2026. The TRAIGA applies to the development or deployment of an AI system by private-sector entities that conduct business in Texas, that produce a product or service used by Texas consumers or that develop or deploy an AI system in Texas. The TRAIGA is not, however, a true general AI law (like the EU AI Act).

Concerns about the effects of overly broad state AI laws on innovation started in 2024, when the first general state AI law – "Concerning Consumer Protections in Interactions with Artificial Intelligence Systems" (CO Rev Stat §§ 6-1-1701 — 6-1-1707) (Colorado AI Act) —was enacted (read our 2024 coverage here). Concurrent with signing the Colorado AI Act, Governor Jared Polis (D) expressed "reservations" to Colorado's legislature that the new law would hamper innovation in Colorado. As discussed below, the Colorado AI Act was replaced with a law with a narrower approach focusing on consequential automated decision-making.

The original draft of TRAIGA, introduced in December 2024, was like the original Colorado AI Act. A month later, Executive Order 14179 (Removing Barriers to American Leadership in Artificial Intelligence, January 23, 2025) was issued and prioritized deregulation and the promotion of AI innovation as a means of maintaining US global dominance.

When the Texas legislature enacted the TRAIGA in June 2025, the parts of TRAIGA that apply to private sector deployment of AI were focused on the most harmful uses of AI. In its final form, the TRAIGA prohibits an AI system that is developed or deployed:

- To intentionally encourage any person to physically harm themselves or others or to engage in criminal activity (§ 552.052)
- With the sole intent of infringing, restricting or impairing a person's federal Constitutional rights (§ 552.055(a))
- With the intent of unlawful discrimination against a protected class under federal or state law (§ 552.056(b))
- With the sole intent of producing, assisting or aiding in producing, or distributing child pornography or unlawful deepfake videos or images (§ 552.057(1))
- To intentionally engage in explicit text-based conversations while impersonating a child under the age of 18 (§ 552.057(2))

The TRAIGA does not offer a private right of action but has stiff penalties: not less than US$10,000 per curable violation up to US$200,000 per day for a continuing violation. The TRAIGA also offers a rebuttable presumption that an entity subject to TRAIGA used "reasonable care" to comply (§ A552.105(c)). The TRAIGA also protects a defendant from liability for an AI system when a third-party uses the AI system for a prohibited purpose under TRAIGA. (§ A552.105(e)). That is, the intent in developing and distributing an AI system, not how the AI system is used or misused, is determinative.

Other states also enacted targeted AI laws that went into force on January 1, 2026, including for AI likenesses (e.g., Montana's Property Right in Use of Names, Voices and Visual Likenesses), civil rights and employment (e.g., Amendment to Illinois' Human Rights Act and Consumer Protection Law), healthcare (e.g., Oregon's HB 2748, which prohibits use of medical professional titles in the name/description of an AI system) and political advertising (e.g., Nevada AI Political Advertising Law).

State AI laws enacted or amended in 2026

2026 started slowly for new AI legislation, but picked up steam over the summer. Even the broadest state legislation now under consideration has avoided the EU-style comprehensive regulation that state legislatures were considering in 2024.



New and amended provenance data and transparency laws

During Q1, Utah enacted the Utah Digital Content Provenance Standards Act, which is in force as of January 1, 2027, and Washington enacted its AI Provenance Law, which is in force as of February 1, 2027. These laws establish transparency mandates for developers and platforms to help consumers identify AI generated content, especially deepfakes, through both cryptographic metadata and consumer visual cues.

During Q2, the Connecticut Artificial Intelligence Responsibility and Transparency (CART) Act was signed into law. Section 15 of the CART Act includes transparency obligations on covered providers that generate "synthetic digital content," effective October 1, 2026. (The CART Act's other provisions are discussed below). On September 2, 2026, an amendment (SB1000) to the California AI Transparency Act (CAITA) (Cal. Bus. & Prof. Code § 22757, et seq.), which is the first state provenance data and transparency law, was delivered to Governor Gavin Newsom for signature. The CAITA faced significant opposition from California businesses because of its many technical and implementation challenges, but had broad bipartisan support in the legislature. If SB1000 becomes law (the governor has until the end of September to sign or veto), it will "take effect immediately as an urgency statute" and, among other changes, will replace the CAITA's AI detection tool requirement with a "disclosure verification tool," eliminate the requirement that a covered provider provide users the option to include a manifest disclosure in AI-generated content, and require latent disclosures to indicate whether a generative AI system created or altered the content.

Colorado and Connecticut regulate AI developers and deployers, though not quite comprehensively

After Colorado's legislature enacted a five month delay of the in-force date for the Colorado AI Act in August 2025, xAI filed suit in federal court (Case No. 1:26-cv-0151 (D. Colo, April 9 , 2026) seeking an injunction against the Colorado AI Act on First Amendment, Dormant Commerce Clause, due process, and equal protection grounds (read more here). On April 27, 2026, the magistrate judge assigned to the xAI case granted a Joint Motion to Vacate Scheduling Conference and Suspend Case Deadlines and Stipulation to Temporarily Stay Enforcement, preventing enforcement of the Colorado AI Act.

A few days later, the "Automated Decision-Making Technology in Consequential Decisions" Act (SB26-189) (Colorado ADMT Act), which replaced and superseded the CO AI Act, was introduced and subsequently enacted by the Colorado legislature and signed by Governor Polis on May 14, 2026 – almost two years to the date after the predecessor Colorado AI Act was enacted. The Colorado ADMT Act abandoned the general duties of care for developers and deployers of AI systems, and set more narrow obligations on use of Automated Decision-Making Technology (ADMT), as explained below. The regulations issued under the Colorado ADMT Act, which are in draft form as of the date of this post, become effective on January 1, 2027.

A few weeks later, on May 27, 2026, Connecticut Governor Ned Lamont (D) signed the CART Act, which has four main parts:

- Whistleblower protections for "covered employee" of large "frontier developer" (Section 2) – in force on October 1, 2026
- Companion chatbot requirements (Sections 4-6) – in force on January 1, 2027 (discussed below)
- Automated employment-related decision technology (Sections 7-14) – in force October 1, 2026; and
- Transparency obligations on "covered providers" that generate "synthetic digital content" (Section 15) in force October 1, 2026 (discussed above).

Both the Colorado ADMT Act and the CART Act apply to developers (generally, an organization that develops or intentionally and substantially modifies in-scope technology for state residents) and the deployers of in-scope technology. Both include notice and transparency obligations, and neither require risk assessments. The key differences are:

- **Technology** – The CART Act has a narrower scope of covered technology and use compared to the Colorado ADMT Act but addresses more topics. The CART Act's regulation of automated decision-making is limited to employment decisions whereas the Colorado ADMT Act covers consequential decisions in covered domains that include but are not limited to employment.
- **Post adverse outcome notice and consumer rights** – The Colorado ADMT Act requires deployers to provide notice after an adverse outcome including the consumers rights to meaningful human review and reconsideration, and to access and correct personal data used in the consequential decision. The CART Act does not and focuses on transparency.

	CO ADMT Act	CART Act
In-Scope AI Technology	Covered ADMT means a technology that processes personal data and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores or other information that is used to make, guide or assist a decision, judgment or determination concerning an individual (ADMT) used to materially influence a consequential decision. "Materially influence" means (i) an ADMT output is a *non-de minimis* factor that is used in making a "consequential decision"; and (ii) an ADMT output affects the outcome of a consequential decision, including by meaningfully altering how a consequential decision is made "Consequential decision" means a (i) a decision, determination or action made about a consumer that relates to the provision of or a consumer's access to, eligibility for, selection for or compensation for a "covered domain" or (ii) a decision, determination, or action about a consumer that relates to a differentiated price, cost sharing, compensation or other material terms in a manner that is reasonably likely to materially limit, delay, effectively deny or otherwise fundamentally alter the consumer's access, eligibility or opportunity for a covered domain	Automated Employment-related Decision Technology (AEDT) is "any technology that processes personal data and uses computation to generate any output, including any prediction, recommendation, classification, ranking, score or other information, that is a "substantial factor" used to make or materially influence [not defined] an employment-related decision." "Substantial factor" means a factor, a constraint, ranking, score, recommendation or classification, that meaningfully alters the outcome of an employment-related decision "Employment-related decision" means a decision, made based on any individual's personal data, to hire, promote, discipline or discharge such individual, to renew such individual's employment, to select such individual for any training or apprenticeship or with respect to such individual's tenure or terms, privileges or conditions of employment

The CO ADMT Act and the CART Act overlap with those states' consumer privacy laws (Colorado Privacy Act and Connecticut's Consumer Data Privacy And Online Monitoring law, respectively) with respect to processing of personal data.

Companion chatbot laws

2026 started with three states (California, New Hampshire, and New York) regulating so-called companion chatbots:

Law	In force date
California: Companion Chatbots Act	January 1, 2026
New Hampshire: Enforcement Action for Solicitation of Children Through Responsive Generative Communication	January 1, 2026
New York: AI Companion Models Law	November 5, 2025

Now, the count is up to 12. Chatbot laws were enacted in Colorado, Connecticut, Georgia, Hawaii, Idaho, Iowa, Nebraska, Oregon and Washington during 2026. All but one (Hawaii) of these nine new chatbot laws are in force during 2027.

Law	Enacted	In force date
Colorado: Chatbot Safety Act	May 29, 2026	January 1, 2027
Connecticut: AI Responsibility and Transparency Act (Sections 4–6: "AI Companions")	May 27, 2026	January 1, 2027
Georgia: AI Companion Chatbots Law	May 11, 2026	July 1, 2027
Hawaii: AI Disclosure and Safety Act	July 13, 2026	July 14, 2026*
Idaho: Conversational AI Safety Act	March 31, 2026	July 1, 2027
Iowa: Chatbot Law	May 2, 2026	July 1, 2027
Nebraska: Conversational AI Safety Act	April 14, 2026	July 1, 2027
Oregon: AI Companion Law	March 31, 2026	January 1, 2027
Washington: AI Companion Law	March 24, 2026	January 1, 2027

* Signed on July 13, 2026, and enforceable upon the governor's signature.

A companion chatbot, also known as an AI companion or conversational AI service (Colorado), is a publicly available AI system with a natural language interface that simulates human conversation, such as by asking unprompted or unsolicited questions that go beyond a direct response to a user prompt, and can sustain an ongoing dialogue with a user across multiple interactions. A key exclusion from "companion chatbot" that is relevant for many businesses is a chat bot used only for customer service, a business' operational purposes, productivity and analysis related to source information, internal research or technical assistance.

Some of the common requirements among the companion chatbot laws are:

- **Initial and recurring notices** – Most of the chatbot laws generally require that a companion chatbot operator provide notices to users when a reasonable person interacting with the chatbot would believe that the person is interacting with a human. (California and Utah have laws requiring similar disclosures for certain bots.) Generally, a companion chatbot operator must provide notice to the user :
  - At the beginning of each interaction or, as a persistent disclosure visible to the user (e.g., Colorado, Connecticut and Iowa)
  - At periodic intervals during continuing AI companion interactions reminding the user that the user is not communicating with a human (e.g., at least every **three hours** in New York's law)

  Some states require notices only for minor users, such as the companion chatbot laws of Hawaii (initial and hourly recurring notice) and Idaho, Oregon, California and Nebraska (initial notice and recurring notices every three hours)
- **Protocols and disclosures** – Most of the laws require that operators have and publish details on safety protocols for content that includes suicidal ideation or self-harm, such as referring a user to a suicide hotline or crisis text line, if the user expresses suicidal ideation, suicide or self-harm. Several of the laws require operators to develop reasonable measures to prevent the companion chatbot from producing sexually explicit content material for minors. Some laws require that operators offer tools for users or guardians to manage privacy and account settings, not provide points or similar rewards at unpredictable intervals with the intent to encourage increased engagement, and/or estimate the age of account holders or users.

The Colorado Department of Law issued the proposed Automated Decision-Making Technology & Conversational AI Service Rules (open for public comment until October 26, 2026) that address age assurance methods, notices and protections for minors (among others).

Federal bills regulating companion chatbots, including the People-First Chatbot Act and Children's Health, Advancement, Trust, Boundaries and Oversight in Technology Act, were introduced during 2026 but, so far, none of them made it over the legislative finish line.

On September 10, Governor Newsom signed a package of child/minor protection bills, including SB 1119 (Adam's Law), which amended California's companion chatbot law to strengthen protections for minors. These amendments ranged from usage time nudges to hard limits, from self-harm protocols to active response mechanisms, from sexual content prohibitions to a ban on emotional grooming. The amendments also added a requirement that a risk assessment must be checked by an independent auditor that will report its findings to the attorney general and expanded the private right of action. The amendments come in force on July 1, 2027. SB-867, a four-year moratorium on selling toys that include companion chatbots, was also signed as part of that package. We will cover these and the other bills in that package of legislation (including an update of the CA Age-Appropriate Design Code Act) in the next part of this series on children's and minors' privacy and safety legislation.

Frontier models and safety and security

The California Transparency in Frontier AI Act (TFAIA) went into effect on January 1, 2026. The New York Responsible AI Safety and Education (RAISE) Act, amendment enacted on March 27, 2026, and the Illinois AI Safety Measures Act (IAISMA), enacted on July 6, 2026, will go into effect on January 1, 2027.

These three laws regulate a frontier model, which is similarly defined across the trio as an AI model trained using greater than 10^26 computational operations (e.g., integer or floating-point operations). The two tiers of developers used in these laws are (i) a frontier developer, meaning a legal or natural person, including affiliates, who has trained or initiated the training of, a frontier model, and (ii) a large frontier developer, meaning a frontier developer, including affiliates, with a gross revenue of over US$500 million in the preceding calendar year.

In general, a frontier developer must:

- Publish a report on its website with information about the frontier model
- Report any critical safety incident within seventy-two (72) hours of discovery (and within 24 hours to an appropriate authority in certain circumstances) (TFAIA – 15 days)
- Refrain from making materially false or misleading statements regarding catastrophic risks and how risks are managed

A large frontier developer also must:

- Publish and follow an AI safety and oversight framework
- Submit a summary of catastrophic risk assessments
- Provide additional detail in its online report

The TFAIA and the IAISMA include whistleblower protections for covered employees who report catastrophic risks or violations. Frontier developers are required to notify employees of their rights and maintain anonymous internal reporting channels. (The RAISE Act does not have these specific requirements.)

A key difference is the IAISMA's third-party audit requirement, which is in force one year after the effective date on January 1, 2028 (or 90 days after a developer first qualifies as a large frontier developer). A large frontier developer subject to IAISMA must conduct an annual independent audit (by third-party with "demonstrated competence") of compliance with the IAISMA's requirements based on generally accepted auditing standards and best practices, retain it for five years and publish a high-level summary on the developer's website.

Training data transparency

California Artificial Intelligence Training Data Transparency Act – While laws regulating frontier models require disclosures about how their models were developed, only California has a law specific to training data disclosures. The California Artificial Intelligence Training Data Transparency Act (AITDTA) applies to developers of generative AI, which are AI systems that "can generate derived synthetic content, such as text, images, video and audio, that emulates the structure and characteristics of the AI's training data."

Calfornia's AITDTA requires any developer that creates, codes or produces generative AI, which was released or "substantially modified" on or after January 1, 2022, and is available to California residents, to publicly post documentation about the developer's training data, including source/owners of training data, whether the developer purchased or licensed the data, whether training data is protected by copyright, trademark, or patent or is entirely in the public domain.

For AITDTA purposes, "substantially modifies" or "substantial modification" means a new version, new release or other update to a generative AI system or service that materially changes its functionality or performance, including the results of retraining or fine tuning.

The AITDTA was met with significant opposition from the tech community. Developer expressed concern about what qualifies as a substantial modification for AITDTA purposes. xAI filed a complaint for a preliminary injunction in December 2025, claiming that the AITDTA requires developers to disclose their trade secrets, is unconstitutionality vague and violates the First Amendment. US District Judge Jesus Bernal denied the xAI's request for an injunction on March 4, 2026.

Anthropic's settlement of copyright claims – In July, a federal court approved a settlement between a class of book authors and Anthropic whereby Anthropic will pay US$1.5 Billion (roughly US$3000 for each of the 500,000 books at issue) to fund compensation to authors for books that Anthropic obtained from websites that made infringing copies of the books available.

This follows an earlier ruling where the court held that use of books to train AI could be a transformative fair use, but in doing so the copying of works obtained from websites that published books without a license to build a research library was not subject to fair use. The court thus concentrated on the copying and storage, and noted that the training purpose did not necessitate the unauthorized access to the works in the first place and that the library was retained subsequent to the works use in training. On the other hand, for physical books that were purchased by Anthropic, copying to a digital format, storage of the digital copes and use to train AI, were all sufficiently transformative and otherwise met the elements of the fair use defense. While the court's decision is in part a win for those advancing fair use for AI training, that does not necessarily extend to the way the material is obtained, prepared and maintained. Furthermore, other courts may well be less convinced about the fair use of AI training even where the works are acquired in a non-infringing manner, but are then reformatted and repurposed. High profile cases brought by copyright owners continue to be litigated and the issue of the scope of fair use for AI training is likely eventually headed to the Supreme Court. In the meantime, the trend seems to be toward licensing copyrighted works for training data sets. The Trump administration is on record supporting a finding of fair use in pending legislation.

Other state AI laws enacted or in force so far in 2026 have a narrower focus relate to healthcare, education, employment, AI likenesses and political advertising. We expect that the AI related legislative activity will be equally active during the rest of 2026, but the likelihood of a general AI law at the state level remains low. Likewise, Congress has yet to advance a general AI law. The Trump administration continues to support pre-emption, but, more recently, the administration's AI policy has focused on national security concerns – in part because of the growing cyber capabilities of frontier models. We will cover the shifts in federal AI policy in a separate post, and will continue to update our readers on new legislative developments as they arise.

For more information on the topics covered in this post, contact the authors. Visit our AI Hub to keep up with the latest on AI law and policy.

Contacts



Alan Friel
Partner, Los Angeles | Atlanta
T +1 213 689 6518
alan.friel@squirepb.com



Julia Jacobson
Partner, New York
T +1 212 872 9832
julia.jacobson@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

© Squire Patton Boggs. All Rights Reserved 2026.