Unique Aspects Of Texas' Approach To AI Regulation

By **Karin McGinnis and Jules Carter** (November 21, 2025)

Karin McGinnis

Jules Carter

Effective Jan. 1, 2026, the Texas Responsible Artificial Intelligence Governance Act takes a unique approach to AI regulation — pulling threads from the European Union's Artificial Intelligence Act, the Colorado AI Act, and national innovation policy, while weaving in Texas-specific priorities.

A Targeted Approach to AI Governance

While many jurisdictions move toward comprehensive, often risk-based, AI regulatory frameworks, Texas has opted for a more targeted approach with fewer obligations on commercial entities.

The Texas Responsible AI Governance Act introduces foundational rules for the development and use of AI technologies — particularly by government actors and in consumer-facing contexts — while leaving significant room for commercial innovation with minimal private-sector burdens.

This law blends select provisions from the EU AI Act (e.g., prohibited uses and a testing sandbox), Colorado's AI Act (e.g., transparency obligations and a dual focus on developers and deployers), and elements of federal policy, such as President Donald Trump's executive order aimed at removing barriers to American AI innovation.[1]

Key Distinctions From Other AI Laws

No Risk-Based Framework

The Texas Responsible AI Governance Act does not categorize AI systems by risk level. Unlike the EU AI Act or Colorado's AI Act, Texas does not define or regulate high-risk AI, nor does it generally link regulation to the provision or denial of key opportunities or services such as employment, housing, lending or healthcare.

Intent-Based Discrimination Standard

The Texas Responsible AI Governance Act prohibits intentional discrimination using AI systems, but disparate impact alone is not sufficient to show unlawful behavior. This marks a divergence from Colorado's law. It also aligns with the Trump administration's disfavor of the disparate impact theory of liability.[2]

Narrow Transparency Requirements

Notice obligations are limited to government agencies and healthcare providers using AI in relation to service or treatment. Unlike broader AI laws, most private businesses have no transparency requirements under this act.

Scope and Applicability

Unlike the EU AI Act and the Colorado AI Act, Texas' AI Act does not apply to employment or commercial contexts. As a result, businesses do not need to provide notices or meet specific transparency or nondiscrimination requirements with respect to individuals acting in an employment or business-to-business context.

The act applies to both developers and deployers, although both terms are defined self-referentially and, notably, neither "develop" nor "deploy" is defined.[3] This may raise potential interpretive issues and leave some ambiguity for compliance and enforcement.

The act also limits its more burdensome obligations to state government entities, healthcare providers and developers who want to participate in the sandbox.[4] As a result, most private sector organizations remain largely unencumbered by many of the act's more prescriptive rules.

Focus on Biometric Identifiers

The act makes several important amendments to Texas' existing biometric data laws, a long-standing focus of the state.

Section 503.001 of the Texas Business and Commerce Code requires informed consent to capture, store or use biometric identifiers for commercial purposes, but the act clarifies that the existence of a biometric identifier on the internet or other publicly available source does not constitute consent to use the information unless it was made publicly available by the individual.[5]

In addition, as amended by the act, the consent requirement does not apply to, among other things, the use of biometric data to (1) develop or train AI systems that are not used or deployed for the purpose of uniquely identifying individuals; or (2) to develop or deploy AI systems for preserving the integrity or security of a system or for the purpose of preventing or detecting fraud, harassment, identity theft, or other malicious, deceptive, or illegal activities, or investigating, reporting or prosecuting a person responsible for such activities.[6]

The act also prohibits government entities from using AI technology to identify individuals based on biometric data or gathering media or images from the internet or other publicly available sources without the individual's consent if the gathering would infringe on any individual right.[7]

Expressly Prohibited AI Uses

Consistent with the EU AI Act's prohibited uses framework, the Texas act bans the use of AI to engage in or aid specific practices, including:

- Social scoring by government entities that leads to adverse treatment or rights infringements;[8]

- Generation or distribution of child sexual abuse material, including deepfake generation and explicit text-based outputs;[9]

- Developing or deploying an AI system with the intent for the system to infringe, restrict or otherwise impair an individual's rights guaranteed under the U.S. Constitution;[10] and

- Manipulation of human behavior to incite or encourage a person to commit physical self-harm, harm to another person, or engage in criminal activity.[11]

Bias and Discrimination

One key issue that has emerged at the forefront of the AI landscape is algorithmic bias, which arises when biases originating from the assumptions of human developers or the characteristics of a training data set become embedded within an algorithmic model.[12]

The major concern is that if such a model is relied upon in a decision-making process, it may contribute to unfair or discriminatory outcomes that reproduce or exacerbate existing inequalities at scale.

Texas takes a somewhat unique approach to addressing the issue of algorithmic bias, focusing on the mental state of developers and deployers. The Texas Responsible AI Governance Act prohibits covered persons from developing or deploying AI systems with the intent to unlawfully discriminate against protected classes in violation of state or federal law.[13]

Notably, demonstrating that the AI system has a disparate impact on a protected class is not alone sufficient to establish prohibited discrimination.[14]

Insurance entities are exempt from the discrimination prohibitions so long as they are already subject to insurance laws and regulations prohibiting unfair discrimination, competition or acts in the business of providing insurance.[15]

Federally insured financial institutions also will be considered to be in compliance with the act if they comply with all federal and state banking laws and regulations.[16] This approach narrows the scope of potential liability compared to broader anti-bias rules in other jurisdictions.[17]

Disclosures and Documentation

Notice to consumers is required only for government agencies and healthcare services.[18]

Specifically, a governmental agency that makes available an AI system designed to interact with consumers must make a clear and conspicuous disclosure to consumers, before or at the time of the interaction, that the consumer is interacting with an AI system, even if the interaction would be obvious.[19]

A provider of healthcare services or treatment for humans by a licensed, registered or certified provider must clearly disclose to the recipient of a service or treatment that the recipient is interacting with an AI system on or before the date on which the service or treatment is first provided or, in the case of an emergency, as soon as reasonably possible.[20]

Outside of these requirements and the requirements for participants in the regulatory sandbox, obligations for documentation and impact assessments are sparse, particularly when compared to other AI laws such as the Colorado AI Act, the EU AI Act, the New York City local law regarding automated employment decision-making tools, and other state comprehensive privacy laws regarding automated decision-making.[21]

Note, however, that the Texas act gives the attorney general the authority to request that a developer or deployer produce information related to the development, testing and monitoring of an AI system as part of an investigation.[22] Therefore, documentation and assessments remain an important part of good governance, even in Texas.

Innovation and Oversight

The Texas Responsible AI Governance Act establishes a regulatory sandbox program to support experimentation and testing of AI systems.[23] This innovation-forward feature echoes regulatory sandboxes in both the EU and the U.S., aiming to balance safety with economic development.[24]

The act sets forth the requirements for applying for and participating in the sandbox program, including: requirements for disclosure of a system's intended use; potential effects on consumers, relevant privacy and public safety risks; plans for mitigating any adverse consequences that may occur during testing; proof of compliance with applicable federal AI laws and regulations, as well as periodic reporting on metrics, risk mitigation; and stakeholder feedback on the AI system.[25]

Program participants enjoy a safe harbor from attorney general charges under the act during participation, but a participant can be removed from the program on a finding that the AI system "poses an undue risk to public safety or welfare ... violates any federal law or regulation ... [or] violates any state law or regulation not waived under the program."[26]

Participation is limited to 36 months, subject to extensions for good cause.[27]

The Texas Department of Information Resources is tasked with submitting an annual report that, among other things, discusses the overall performance and effect of the AI systems tested in the sandbox program and makes recommendations on changes to laws or regulations.[28]

To support ongoing policymaking and public understanding of AI, the act also establishes the Texas AI Advisory Council to advise the legislature on AI-related issues and authorizes programs to study the societal effect of AI technologies.[29]

Enforcement and Penalties

The Texas attorney general and state agencies have exclusive authority to enforce the act, as it creates no private right of action.[30]

Notable features of the enforcement mechanism include the following.

Online Complaint Mechanism

The act tasks the attorney general with creating and maintaining an online complaint mechanism on its website so that consumers can submit complaints.[31]

Investigative Demands

Although the Texas Responsible AI Governance Act does not have robust reporting, documentation and impact assessment requirements for developers and deployers outside of the sandbox program, the attorney general can issue an investigative demand to an organization that is the subject of a complaint.

The demand can require:

> a high-level description of the purpose, intended use, deployment context and associated benefits of the [AI] system ... a description of the type of data used to program or train the [AI] system ... a high-level description of the categories of data processed as inputs for the [AI] system ... a high-level description of the outputs produced by the [AI] system ... any metrics the person uses to evaluate the performance of the [AI] system ... any known limitations of the [AI] system ... a high-level description of the post-deployment monitoring and user safeguards ... [and] any other relevant documentation reasonably necessary for the attorney general to conduct an investigation.[32]

Notice-and-Cure Requirement

The act requires that those found to have violated any of its provisions must receive written notice and a 60-day period to cure the identified violations. This requirement appears to apply even in cases involving serious misconduct like discrimination or the creation of child sexual abuse material.[33]

Civil Penalties Only

The act allows for monetary fines, injunctions and reimbursement of court and investigation costs, but not criminal penalties.[34]

Safe Harbors

The act provides that a person will not be held liable if a prohibited use was committed by another party using a compliant system, and it establishes a presumption of reasonable care for entities complying with certain internationally recognized risk management frameworks, such as the National Institute of Standards and Technology's AI Risk Management Framework.[35]

Final Thoughts

The Texas Responsible AI Governance Act signals a distinctively Texan approach to regulating AI — limited in scope and innovation-friendly, and largely aligned with related federal policy trends.

While government use of AI will be subject to increased scrutiny under the act, private sector actors will find relatively few immediate compliance burdens, particularly outside of healthcare contexts.

With the effective date of the Colorado AI Act pushed out to June 30, 2026, Texas' law will be the sole comprehensive AI law in the U.S.

Nonetheless, developers and deployers operating in Texas should:

- Monitor ongoing developments as regulatory definitions and requirements become clearer, especially considering the current ambiguities and the early-stage nature of the sandbox framework;

- Recognize that this law introduces additional complexity to the already varied U.S. regulatory environment, which affects organizations using AI across multiple states; and

- Engage in careful, jurisdiction-specific compliance planning to address the unique requirements and challenges in Texas and other states.

Karin M. McGinnis is a co-head of privacy and data security and a member of employment and labor and litigation, and Jules W. Carter is an associate at Moore & Van Allen PLLC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., 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.

[1] Removing Barriers to American Leadership in Artificial Intelligence, Exec. Order No. 14179, 90 Fed. Reg. 8741 (January 23, 2025).

[2] See Restoring Equality of Opportunity and Meritocracy, Exec. Order No. 14281, 90 Fed. Reg. 17537 (April 23, 2025).

[3] TX H.B. 149, sec. 4, § 552.001.

[4] See, e.g., TX H.B. 149, sec. 4, §§ 552.051(b) & (f); § 553.051-553.054, 553.101-553.103.

[5] TX H.B. 149, sec. 2, § 503.001(b-1).

[6] Id. at §§ 503.001(e).

[7] TX H.B. 149, sec. 4, § 552.054(b).

[8] Id. at § 552.053.

[9] Id. at § 552.057.

[10] Id. at § 552.055.

[11] Id. at § 552.052

[12] See, e.g., U.S. Dep't of the Treasury, A Financial System the Creates Economic Opportunities: Nonbank Financials, Fintech and Innovation, at 103 (July 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-thatCreates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf. (citing Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (2016)).

[13] TX H.B. 149, sec. 4, § 552.056(b); § 552.056(a)(3) ("'Protected class' means a group or class of persons with a characteristic, quality, belief, or status protected from discrimination by state or federal civil rights laws, and includes race, color, national origin, sex, age, religion, or disability.").

[14] Id. at § 552.056(c).

[15] Id. at § 552.056(d).

[16] Id. at § 552.056(e).

[17] See, e.g., Colo. Rev. Stat. § 6-1-1701(1) (defining "algorithmic discrimination" to include "any condition in which the use of an artificial intelligence system results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of this state or federal law.").

[18] TX H.B. 149, sec. 4, § 552.051.

[19] Id. at § 552.051(b).

[20] Id. at § 552.051(f).

[21] See Colo. Rev. Stat. § 6-1-170; 2024 O.J. L 2024/1689; New York City, NY, Automated Employment Decision Tools (AEDT), Local Law 144 (2021).

[22] TX H.B. 149, sec. 4, § 552.103(b)(8).

[23] Id. at § 553 subchapters A, B and C.

[24] Id. at § 553.051(b).

[25] Id. at § 553.052(b).

[26] Id. at § 553.101.

[27] Id. at § 553.053.

[28] Id. at § 553.103.

[29] Id. at § 554.001.

[30] Id. at § 552.101.

[31] Id. at § 552.102.

[32] Id. at § 552.103.

[33] Id. at § 552.104.

[34] Id. at § 552.105.

[35] Id. at § 552.105(e).