CLIENT ALERT | June 23, 2025

Texas Signs Responsible AI Governance Act Into Law

After undergoing substantial changes in the Texas legislature, a scaled-down TRAIGA will go into effect in 2026.

Key Points:

- The Act prohibits the development and deployment of AI systems for certain purposes, including behavioral manipulation, discrimination, creation or distribution of child pornography or unlawful deepfakes, and infringement of constitutional rights.
- The Act also establishes a regulatory sandbox program for developers and creates the Texas Artificial Intelligence Advisory Council.
- The Act will go into effect on January 1, 2026.

On June 22, 2025, Texas Governor Greg Abbott signed the Texas Responsible AI Governance Act (TRAIGA or the Act) into law, marking the final chapter of a bill that received national attention and underwent major changes throughout the legislative process.

As introduced in December 2024, the original draft of TRAIGA proposed a sweeping regulatory scheme modeled after the Colorado AI Act and the EU AI Act, focusing on "high-risk" artificial intelligence (AI) systems and imposing substantial requirements and liability for developers and deployers in the private sector. However, in March 2025, Texas legislators introduced an amended version that significantly scaled back the bill's scope. Many of the original draft's most onerous requirements — such as the duty to protect consumers from foreseeable harm, conduct impact assessments, and disclose the details of high-risk AI systems to consumers — were either deleted entirely or limited to apply solely to governmental entities.[1]

Still, the enacted version of TRAIGA includes a number of provisions that could impact companies that operate in Texas. Most notably, the Act imposes categorical restrictions on the development and deployment of AI systems for certain purposes, including behavioral manipulation, discrimination, the creation or distribution of child pornography and unlawful deepfakes, and infringement of constitutional rights. The Act also creates a regulatory sandbox program that will allow participants to develop and test AI systems in a relaxed regulatory environment. Furthermore, it establishes an AI advisory council tasked with assisting the state legislature in identifying effective AI policy and law, making recommendations to state agencies regarding their use of AI systems, and advising on improvements to the regulatory sandbox program, among other responsibilities.

This Client Alert will touch on the full scope of TRAIGA, with a particular focus on the Act's implications for private-sector developers and deployers of AI systems that do business in Texas.

TRAIGA's Substantive Provisions

Prohibited AI Practices

TRAIGA prohibits the development or deployment of any AI system[2] for certain purposes, including by private-sector entities that conduct business in Texas, produce a product or service used by Texas residents, or develop or deploy an AI system in Texas. These prohibitions include:[3]

1. **Manipulation of Human Behavior:** AI systems cannot be developed or deployed to intentionally encourage any person to physically harm themselves or others or to engage in criminal activity.

2. **Constitutional Protection:** AI systems cannot be developed or deployed with the sole intent of infringing, restricting, or impairing a person's federal Constitutional rights.

3. **Unlawful Discrimination:**[4] AI systems cannot be developed or deployed with the intent of unlawfully discriminating against a protected class under federal or state law. Notably, TRAIGA specifies that a "disparate impact" alone is not sufficient to demonstrate an intent to discriminate under this provision; therefore, merely showing that an AI system negatively impacts a protected class would not, by itself, establish a violation.

4. **Sexually Explicit Content:** AI systems may not be developed or distributed with the sole intent of producing, assisting or aiding in producing, or distributing child pornography or unlawful deepfake videos or images. Intentionally developing or distributing an AI system that engages in explicit text-based conversations while impersonating a child under the age of 18 is also prohibited.

The Act states that these prohibitions should be "broadly construed and applied" to promote TRAIGA's underlying purposes, which include facilitating responsible development of AI and protecting the public from foreseeable risks associated with AI.

Enforcement and Penalties

TRAIGA vests enforcement authority solely in the Texas Attorney General (AG). Under the Act, the AG must develop a reporting mechanism on its website to facilitate consumer complaints of potential violations, similar to the online mechanism created in conjunction with the Texas Data Privacy and Security Act. After receiving a consumer complaint, the AG may issue a civil investigative demand to parties suspected of violating TRAIGA, in which the AG can request extensive information, including a high-level description of the AI system's purpose and intended use, a description of the types of data used to program or train the AI system, a high-level description of the data processed as inputs as well as outputs produced by the AI system, any metrics used to evaluate the performance and known limitations of the AI system, and a description of post-deployment monitoring and user safeguards.

After receiving a notice of violation from the AG, a party has 60 days to cure any violation and provide supporting documentation to the AG explaining how the alleged violations were cured. The AG may bring an enforcement action to enjoin uncured violations only after the cure period has ended. The AG may also seek civil penalties for uncured violations, which range in amount depending on the type of violation at issue:

- Violations that are determined by a court to be curable and breaches of a written "cure" statement to the AG are each subject to fines of $10,000 to $12,000 per violation/breach
- Violations that a court deems uncurable are subject to fines of $80,000 to $200,000 per violation
- Continuing violations are subject to fines of up to $40,000 per day the violation continues

The Act also gives state agencies the authority to sanction a party that is licensed by such agency, if that party is found liable for TRAIGA violations and the AG recommends additional enforcement by the applicable agency. Potential sanctions can include suspending or revoking the party's license and monetary penalties of up to $100,000.

The Act creates several affirmative defenses to liability for parties that discover their own violation either through (i) feedback that the party has received from a developer, deployer, or other person; (ii) testing procedures such as red-teaming or adversarial testing; (iii) following state agency guidelines; or (iv) an internal review process, provided that the party is otherwise in compliance with a nationally recognized AI risk management framework, such as NIST's AI Risk Management Framework.

The Act also clarifies that a developer or deployer cannot be held liable simply because an end user or other third party uses an AI system for a prohibited purpose. In other words, the Act's plain language suggests that the key question in determining liability under TRAIGA will be a developer's or deployer's intent in creating and distributing an AI system — and not the way end users actually use that system.

Regulatory Sandbox Program

TRAIGA introduces a regulatory sandbox program administered by the Department of Information Resources (DIR) that is designed to support the testing and development of AI systems under relaxed regulatory constraints.

Interested parties must submit an application that includes a detailed description of the AI system that will be tested under the program; a benefit assessment addressing impacts on consumers, privacy, and public safety; mitigation plans in case of adverse consequences during the testing phase; and proof of compliance with federal AI laws and regulations. If accepted, program participants get 36 months to test and develop their AI systems under the program, during which time the AG cannot file charges and state agencies cannot pursue punitive action for violations of state laws or regulations waived under the Act.

Participants must submit quarterly reports to DIR detailing system performance metrics, updates on how the system mitigates risk, and feedback from consumers and stakeholders. DIR will use information gathered from the program to submit annual reports to the Texas legislature and make recommendations for future legislation and regulatory reform.

Texas Artificial Intelligence Council

Finally, TRAIGA establishes the Texas Artificial Intelligence Advisory Council (Council), comprising seven qualified members appointed by the governor, lieutenant governor, and speaker of the house. The Council is charged with conducting AI training programs for state agencies and local governments, and may issue reports on AI-related topics such as data privacy and security, AI ethics, and legal risks and compliance, with the goal of helping to guide the Texas legislature on effective policy. However, the Council is expressly prohibited from promulgating any binding rules or regulations itself.

Practical Takeaways for Developers and Deployers

Developers and deployers that operate in Texas have time to ensure compliance before TRAIGA goes into effect on January 1, 2026.

Companies can start by evaluating whether they have developed or deployed (or intend to develop or deploy) an AI system that could implicate one of TRAIGA's prohibited uses. The Act's plain language suggests that a party may be liable only if it *intentionally* develops or deploys an AI system for the purpose of engaging in a prohibited practice. But the Act also instructs that it should be broadly construed and applied so as to protect consumers from AI-related risks. Moreover, the AG has seemingly made AI an enforcement priority and has filed several high-profile lawsuits against AI companies within the last few years. As such, companies that develop or deploy AI systems that are capable of engaging in prohibited practices — even if that is not the system's intended purpose — could face risk under TRAIGA.

The Act also encourages developers and deployers to be proactive in preventing potential issues by limiting liability for parties that identify and cure their own violations. Developers and deployers of AI systems that are capable of engaging in prohibited practices should consider establishing robust internal processes designed to identify potential violations — including implementing NIST's AI Risk Management Framework — and should work closely with counsel to ensure that those processes fall within the scope of the Act's affirmative defenses.

Contacts

Sy Damle
sy.damle@lw.com
+1.202.637.3332
+1.212.906.1659
Washington, D.C. / New York

Andy Gass
andrew.gass@lw.com
+1.415.395.8806
San Francisco

Ghaith Mahmood
ghaith.mahmood@lw.com
+1.213.891.8375
Los Angeles

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Robert Brown
robert.brown@lw.com
+1.713.546.7454
Houston / Austin

Endnotes

[1] The Act defines "governmental entity" as "any department, commission, board, office, authority, or other administrative unit of this state or of any political subdivision of this state, that exercises governmental functions under the authority of the laws of this state," (excluding hospital districts and institutions of higher education).

[2] The Act defines "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."

[3] In addition to the prohibitions described in this Client Alert, TRAIGA also prohibits the use or deployment of AI systems for social scoring and using biometric data to identify a specific individual, but limits the applicability of those provisions solely to governmental entities.

[4] A federally insured financial institution is deemed to be in compliance with this provision if the institution complies with all federal and state banking laws and regulations. Likewise, the provision does not apply to insurance companies for purposes of providing insurance services if the company is subject to statutes regulating unfair discrimination, unfair methods of competition, or unfair or deceptive acts or practices related to the business of insurance.