


AI Law and Policy

Legal Considerations Involving Artificial Intelligence

Texas Considers Comprehensive AI Bill



By Carolyn Metnick & Michael Sutton on December 30, 2024

 Listen to this post

Texas is joining a growing number of states in considering comprehensive laws regulating use of AI. In particular, the Texas Legislature is scheduled to consider the **draft** “Texas Responsible AI Governance Act” (the “Act”), which seeks to regulate development and deployment of artificial intelligence systems in Texas. Critically, as most states continue to grapple with the emergence of AI, the Act could serve as a model for other states and could prove tremendously impactful.

Applicability

The bulk of the Act is focused on “high-risk artificial intelligence systems”, which include

artificial intelligence systems that, when deployed, make or are otherwise a contributing factor in making, a consequential decision.**[1]** The Act specifically excludes a number of systems, such as technology intended to detect decision-making patterns, anti-malware and anti-virus programs, and calculators, among others.**[2]**

Separately, the Act also imposes specific obligations depending on the role of a party, including:

- A “deployer”, who is a party doing business in Texas that deploys a high-risk artificial intelligence system.**[3]**
- A “developer”, who is a party doing business in Texas that develops a high-risk artificial intelligence system or who substantially or intentionally modifies such a system.**[4]**

Determining a party’s role is key to assessing its obligations under the Act.

Duties of Developers

The Act requires that developers of a high-risk artificial intelligence system use reasonable care to protect consumers from known or reasonably foreseeable risks.**[5]** In addition, the Act requires that developers, prior to providing a high-risk artificial intelligence system to a deployer, provide deployers with a written “High-Risk Report”**[6]** which must include:

1. A description of how the high-risk artificial intelligence system should be used and not used, as well as how the system should be monitored when the system is used to make (or is a substantial factor in making) a “consequential decision.”**[7]**
- A description of any known limitations of the system, the metrics used to measure performance of the system, as well as how the system performs under those metrics.**[8]**
 - A description of any known or reasonably foreseeable risks of algorithmic discrimination, unlawful use/disclosure of personal data, or deceptive manipulation or coercion of human behavior which is likely to occur.**[9]**
 - A description of the types of data to be used to program or train systems.**[10]**

- A summary of the data governance measures which were implemented to cover the training datasets as well as their collection, the measures used to examine the suitability of the data sources, possibly discriminatory biases, and measures to be taken to mitigate such risks.[11]

Prior to deployment of a high-risk artificial intelligence system, developers are required to adopt and implement a formal risk identification and management policy that must satisfy a number of prescribed standards.[12] Further, developers are required to maintain detailed records of any generative artificial intelligence training datasets used to develop a generative artificial intelligence system or service.[13]

Duties of Distributors

The Act requires that deployers of high-risk artificial intelligence systems use reasonable care to protect consumers from known or reasonably foreseeable risks arising from algorithmic discrimination.[14] In addition, if a deployer considers or has reason to consider that a system is not in compliance with the foregoing duty, the Act requires that the deployer suspend use of the system and notify the developer of the corresponding system of such concerns.[15] Further, deployers of high-risk artificial intelligence systems are required to assign human oversight with respect to consequential decisions made by such systems.[16] In the event a deployer learns that a deployed high-risk artificial intelligence system has caused or is likely to cause algorithmic discrimination or an inappropriate or discriminatory consequential decision, such deployer must notify the Artificial Intelligence Council,[17] the Texas Attorney General, or the director of the state agency that regulates the deployer's industry no later than ten (10) days after the date the deployer learns of such issues.[18]

Separately, the Act also obligates deployers of high-risk artificial intelligence systems to complete an impact assessment on a semi-annual basis and within ninety (90) days after any intentional or substantial modification of the system.[19] The Act outlines a number of items which must be addressed in the assessment, including among others an analysis of whether the system poses any known or reasonably foreseeable risks of algorithmic discrimination as well as a description of the steps taken to mitigate such risks.[20] In addition, after an intentional or substantial modification to a high-risk artificial intelligence system occurs, the deployer must disclose the extent to which the system was used in a

manner that was consistent with or otherwise varied from the developer's intended use of the system.[21]

Further, the Act requires developers to review the deployment of high-risk artificial intelligence systems on an annual basis to ensure that the system is not causing algorithmic discrimination.[22]

Digital Service Providers and Social Media Platforms

The Act also provides that digital services providers[23] and social media platforms[24] must use commercially reasonable efforts to prevent advertisers on the service or platform from deploying high-risk artificial intelligence systems that could expose users to algorithmic discrimination.[25]

Specific Prohibited Activities

The Act includes several limitations on specific activities, such as:

- **Manipulating Human Behavior** – The Act prohibits use of an artificial intelligence system that uses subliminal or deceptive techniques with the objective or effect of materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision.[26]
- **Social Scoring** – The Act prohibits use of an artificial intelligence system developed or deployed for the evaluation or classification of natural persons or groups of natural persons based on their social behavior or predicted personal characteristics, with the intent to determine a social score or a similar estimation/valuation.[27]
- **Biometric Identifiers** – The Act prohibits use of an artificial intelligence system which is developed or deployed with the purpose or capability of gathering or otherwise collecting biometric identifiers of individuals.[28] In addition, the Act prohibits use of a system which infers or interprets sensitive personal attributes of a person or group of persons using biometric identifiers, except for the labeling or filtering of lawfully acquired biometric identifier data.[29]
- **Protected Characteristics** – The Act prohibits use of an artificial intelligence system that utilizes characteristics of a person based on their race, color, disability, religion,

sex, national origin, age, or a special social or economic situation with the objective (or effect) of materially distorting the behavior of that person in a manner that causes or is reasonably likely to cause that person or another person significant harm.[30]

- **Emotional Inferences** – The Act prohibits use of an artificial intelligence system that infers, or is capable of inferring, the emotions of a natural person without the express consent of such person.[31]

Consumer Rights

A deployer or developer who deploys, offers, sells, leases, licenses, gives, or otherwise makes available a high-risk artificial intelligence system that interacts with consumers must disclose to consumers (before or at the time of interaction) the following:

1. That the consumer is interacting with an artificial intelligence system;
2. The purpose of the system;
3. That the system may or will make a consequential decision affecting the consumer;
4. The nature of any consequential decision in which the system is or may be a contributing factor;
5. The factors to be used in making any consequential decisions;
6. The contact information of the pertinent deployer;
7. A description of any human components of the system;
8. A description of any automated components of the system;
9. A description of how human and automated components are used to inform a consequential decision; and
10. A declaration of the consumer's rights.[32]

The foregoing disclosure must be conspicuous and presented in plain language.[33]

Separately, the Act also permits consumers to bring an action against a developer or deployer that violates the consumer's rights under the Act (including by engaging in any of the specifically prohibited activities discussed in the section immediately above).[34]

Notwithstanding the foregoing, it appears that the consumer may only seek declaratory or

injunctive relief, rather than damages, although the consumer may recover costs and reasonable and necessary attorney's fees.**[35]**

Enforcement by the Texas Attorney General

Significantly, the Act provides the Texas Attorney General with jurisdiction to investigate and enforce the Act, including through injunctions.**[36]** Further, the Act authorizes administrative fines which vary depending on the circumstances, such as fines ranging from \$40,000 to \$100,000 per violation where a developer or deployer fails to timely cure a violation of a prohibited use.**[37]**

Putting It into Practice

It will be critical that businesses operating in Texas and using artificial intelligence systems monitor the legislative progression of the Act to determine whether it will be passed into law. If the Act is ultimately enacted, businesses should begin assessing whether their current (or intended) operations are compatible with the Act's limitations and should begin conducting an impact assessment to ensure conformance. In addition, businesses should begin preparing policies, procedures, and other systems to ensure they are ready to respond to consumer requests.

If you have any questions about the Act or its impact on you or your business's use of artificial intelligence systems, please contact a member of the **Sheppard Mullin Healthcare Team**.

FOOTNOTES

[1] Section 551.001(13). The Act defines a "consequential decision" as "a decision that has a material legal, or similarly significant, effect on a consumer's access to, cost of, or terms of: (A) a criminal case assessment, a sentencing or plea agreement analysis, or a pardon, parole, probation, or release decision; (B) education enrollment or an education opportunity; (C) employment or an employment opportunity; (D) a financial service; (E) an essential government service; (F) electricity services; (G) food; (H) a health-care service; (I) housing; (J) insurance; (K) a legal service; (L) a transportation service; (M) surveillance or monitoring systems; [] (N) water[]; or (O)] elections." Section 551.001(4).

[2] Section 551.001(13).

[3] Section 551.001(8).

[4] Section 551.001(9).

[5] Section 551.003(a).

[6] Section 551.003(b).

[7] Section 551.003(b)(1).

[8] Section 551.003(b)(2).

[9] Section 551.003(b)(3).

[10] Section 551.003(b)(4).

[11] Section 551.003(b)(5).

[12] Section 551.008.

[13] Section 551.003(f).

[14] Section 551.005.

[15] Section 551.005.

[16] Section 551.005.

[17] The Artificial Intelligence Council is formed pursuant to Section 553 of the Texas Business and Commerce Code and is administratively attached to the Texas Governor's Office. Section 553.001.

[18] Section 551.011.

[19] Section 551.006(a).

[20] Section 551.006(a).

[21] Section 551.006(b).

[22] Section 551.006(d).

[23] A “social media platform” means “an Internet website or application that is open to the public, allows a user to create an account, and enables users to communicate with other users for the primary purpose of posting information, comments, messages, or images”, subject to certain exclusions such as internet service providers, electronic mail, among others. Tex. Bus. & Comm. Code § 120.001(1).

[24] A “digital service provider” means “a person who: (A) owns or operates a digital service; (B) determines the purpose of collecting and processing the personal identifying information of users of the digital service; and (C) determines the means used to collect and process the personal identifying information of users of the digital service. Tex. Bus. & Comm. Code § 509.001(2). In turn, a “digital service” includes “a website, an application, a program, or software that collects or processes personal identifying information with Internet connectivity.” Tex. Bus. & Comm. Code § 509.001(1).

[25] Section 551.010.

[26] Section 551.051.

[27] Section 551.052.

[28] Section 551.053.

[29] Section 551.054.

[30] Section 551.055.

[31] Section 551.056.

[32] Section 551.007(a).

[33] Section 551.007(c).

[34] Section 551.107(a).

[35] Section 551.107(b).

[36] Sections 551.104, 551.106.

[37] Section 551.106.

AI Law and Policy

Copyright © 2025, Sheppard, Mullin, Richter & Hampton LLP. All Rights Reserved.