# New Texas AI Law Affects Collection and Use of Biometric Identifiers

Jul 15, 2025

**Categories:**

Publications
Technology Blog

**Authors:**

Mason C. Clutter
Lauren E. Cole

On June 22, 2025, Texas Governor Greg Abbot signed into law the Texas Responsible Artificial Intelligence Governance Act (TRAIGA). Texas joins California, Utah, and Colorado in specifically regulating artificial intelligence (AI). Much has been written about the law's likely impact on private-sector AI developers and deployers, as well as the responsible use mandates for Texas government entities and updates to the Texas consumer privacy law, which Frost Brown Todd is monitoring closely. Not as much has been discussed, however, about the changes TRAIGA made to the Capture or Use of Biometric Identifier Act (CUBI), which has been a cornerstone in regulating the collection and use of biometric identifiers for commercial purposes in Texas since 2009.

TRAIGA (1) makes clear that CUBI applies to AI models or systems, (2) clarifies that consent has not been given by an individual for the use of their biometric identifiers simply by appearing in public images on the internet that the individual did not post, and (3) creates exceptions for businesses that are developing AI systems that (a) are *not* used to identify individuals or (b) are used for security purposes. It is important that affected companies understand both laws to avoid potentially significant fines ranging from $2,000 to $200,000.

## Who Is Covered, and What Are Biometric Identifiers?

TRAIGA applies "to a person [including a business] who: (1) promotes, advertises, or conducts business in [Texas]; (2) produces a product or service used by residents of [Texas]; or (3) develops or deploys an artificial intelligence system in Texas." CUBI, on the other hand, applies to all persons, including businesses acting with a "commercial purpose." Commercial purpose is not defined; therefore, a broad interpretation for any business purpose is a conservative reading.

Texas defines "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Under CUBI, companies intending to capture an individual's biometric identifier for a commercial purpose must notify the individual and obtain their consent prior to capture. In addition to notice and consent requirements, CUBI imposes requirements regarding retention and destruction of biometric identifiers, prohibits the sale, lease, or disclosure of biometric identifiers subject to a few limited exceptions, and imposes data security

requirements.

## CUBI's New AI-Related Guidelines

TRAIGA clarifies consent regarding biometric identifiers found online and introduces limited exceptions for the use of biometric identifiers in AI systems, consistent with TRAIGA's responsible use requirements. Other key provisions are examined below.

### *Consent*

TRAIGA specifies that an individual's appearance in images or media that are available on the internet or from a publicly accessible source does not constitute notice or consent unless the individual personally uploaded images or media containing a biometric identifier. This means that posts by anyone, or anything, other than the individual whose biometric identifier appears in the media, do not satisfy consent requirements under CUBI for the use of that individual's biometric identifiers. For example, scraping social media pages for photographs to use to develop records of face geometry for facial recognition purposes, without first obtaining the consent of the photographed individuals if they did not post the photograph themselves, may be prohibited under the law if such use is for a "commercial purpose."

### *Application to AI*

As noted, TRAIGA makes clear that CUBI's requirements apply to the use of biometric identifiers in AI systems, subject to a few exceptions. Specifically, CUBI does not apply to the training, processing, or storage of biometric identifiers involved in AI systems that are not used or deployed "for the purpose of uniquely identifying a specific individual." Further, CUBI does not apply to the development or deployment of an AI system for the purposes of (1) "preventing, protecting against, or responding to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any other illegal activity"; (2) preserving the security or integrity of a system; or (3) "investigating, reporting, or prosecuting" acts identified in number (1) or other illegal activity. All other uses of a biometric identifier captured for the purpose of training an AI system and subsequently used for a commercial purpose are governed by CUBI. Civil penalties of CUBI remain up to $25,000 for each violation, which can only be brought by the Texas Attorney General.

Accordingly, unless you are collecting and using biometric identifiers for the development or deployment of AI systems that relate to illegal activities or uses unrelated to identifying specific individuals, you are not only subject to the new Texas AI law; you are also subject to CUBI.

## Next Steps

TRAIGA represents a significant policy shift in how Texas safeguards individual biometric identifiers within the broader context of AI. Companies collecting, using, or otherwise handling biometric identifiers should implement standardized policies and ensure compliant processes are in place for notice, consent, sale, lease, disclosure, security, retention, destruction, and any use in AI systems.

At Frost Brown Todd, our attorneys work at the intersection of privacy, security, and technology, including the latest developments and requirements for AI. For further information or compliance assistance related to TRAIGA, CUBI, or other data security, privacy, or technology requirements, please contact the authors of this article or any attorney with Frost Brown Todd's Data, Digital Asset & Technology Practice Group.

***Kaitlyn Ross*, *a second-year law student at Indiana University Maurer School of Law, contributed to this article while working as a summer associate at Frost Brown Todd.***