The Texas Lawbook

Free Speech, Due Process and Trial by Jury

Texas Emerges as a Leading Force in State Privacy Law Enforcement

NOVEMBER 20, 2025 | BY AARON P. SIMPSON & DANIELLE DOBRUSIN

Over the past two years, Texas has emerged as a leader in the U.S. state privacy regulatory landscape. The state's attorney general, Ken Paxton, has launched a broad privacy enforcement initiative, secured notable settlements and filed lawsuits against major players across industries ranging from social media to insurance. With new privacy laws that have come into effect in 2024 and 2025 and a steady stream of enforcement activity, Texas has established itself as a state that businesses must pay close attention to when evaluating compliance obligations.

A New Era for Texas Privacy Law

Two major statutes marked a turning point in 2024 for Texas' privacy regulatory landscape. In July 2024, the Texas Data Privacy and Security Act became effective, establishing a framework similar to comprehensive consumer privacy laws in other states. Just two months later, the Securing Children Online through Parental Empowerment Act took effect, creating heightened protections for minors and imposing unique obligations on certain online platforms that allow users to create profiles, socially interact with each other and create or post content. These laws arrived against the backdrop of earlier measures, including the state's biometric privacy law and its law regulating data brokers.

In 2025, Texas has continued to expand its privacy and technology legal framework. First, in May 2025, Texas passed the Texas App Store Accountability Act, which requires app stores to verify the age category of new users, obtain parental approval for use by minors, and ensure developers can access verification data necessary to comply with the law. Then, in June 2025, the state enacted the Texas Responsible Artificial Intelligence Governance Act, which imposes requirements and restrictions regarding the development and deployment of AI systems, in addition to establishing the Texas Artificial Intelligence Council, which is has a wide-ranging mandate to help ensure AI systems in Texas are both ethical and developed in the best interests of the public.

The AI Act also introduces an innovative 36-month regulatory sandbox program that will permit approved participants to test AI systems under regulatory supervision, with temporary relief from certain licensing and compliance obligations, while still requiring safeguards such as quarterly reporting and strict prohibitions on manipulation, discrimination and unlawful content. In July 2025, the state enacted S.B. 1188, which regulates both the security and storage of electronic health record data and the use of artificial intelligence in the health care context, adding a localization requirement to keep electronic health record data in the United States.

In short, the Texas legislature has been active of late in an effort to ensure that the state's regulatory toolbox is robust and able to hold companies accountable in the privacy and AI context without stifling innovation.

Enforcement Strategy

While most states limit their privacy enforcement to the respective attorney general, Texas AG Paxton has created a team within the consumer protection division of the AG's office to enforce the state's new arsenal of privacy laws. Paxton has described the unit as one of the largest state-level privacy enforcement teams in the nation and committed to "doubling down to protect privacy rights," signaling Texas' intent to take a leading role nationally from a privacy law enforcement perspective. Paxton's privacy initiative formally launched in June 2024 and within months, his office had issued letters, filed lawsuits and secured settlements across several areas. Unlike some states that have taken a relative wait-and-see approach to new privacy laws, Texas has wasted no time in flexing its enforcement muscle.

Notably, in addition to the new statutes available to the AG, Paxton has made clear that his office will not rely solely on these privacy-specific statutes in his enforcement efforts. Texas also maintains a Deceptive Trade Practices–Consumer Protection Act, and it will remain a cornerstone of the state's privacy law enforcement toolkit. By framing certain privacy violations as "deceptive acts," Paxton has been able to expand the reach of his office's investigations and create additional avenues for sanction.

Recent High-Profile Enforcement Actions

1. Data Broker Crackdown

The state has prioritized its new Data Broker Law, which requires entities engaged in buying, selling or processing personal data to register with the Texas secretary of state. In June 2024, the attorney general's office notified more than 100 companies that they were allegedly out of compliance. The law imposes civil penalties of $100 per day, capped at $10,000 per entity per year.

2. Biometric Data Settlement

In July 2024, Texas announced the first settlement ever reached under its biometric privacy statute, the Capture or Use of Biometric Identifier Act. The $1.4 billion settlement stemmed from allegations that Meta collected biometric data through facial recognition tools without user consent. Unlike Illinois's well-known Biometric Information Privacy Act, CUBI does not allow private lawsuits, meaning enforcement authority rests solely with the state attorney general. Texas' action signaled its intent to use that authority actively.

3. Sensitive Geolocation Data Lawsuit

In January 2025, Paxton announced a lawsuit against Allstate and its analytics subsidiary Arity for allegedly collecting and selling sensitive geolocation data in violation of the TDPSA. The lawsuit claimed failures to obtain consent, provide notice or honor consumer opt-out rights, while also pointing to violations of the Data Broker Law.

4. AI-Related Investigations

In February 2025, Texas announced an investigation into Chinese-owned AI firm DeepSeek, citing potential TDPSA violations. Paxton warned that companies aligned with foreign governments would be held accountable if they violated Texans' rights or undermined U.S. innovation.

5. Google Settlement

Texas' aggressive enforcement posture was further demonstrated in May 2025, when AG Paxton announced a $1.375 billion settlement with Google over allegations that the company unlawfully collected and misused Texans' personal data.

The complaint alleged Google

continued to gather precise location information even when location services were disabled, misled users about the privacy protections of Chrome's "Incognito" mode and captured biometric identifiers in violation of state law. Paxton's office touted the settlement as the largest state-level privacy recovery in history, dwarfing both individual state settlements and multistate coalition efforts.

Constitutional Challenges

Not all of Texas's efforts have proceeded without friction. In early 2025, a federal judge issued a preliminary injunction against portions of the SCOPE Act, including provisions requiring age verification for minors. The court raised constitutional concerns, particularly around free speech and privacy. However, other parts of the law remain enforceable, such as restrictions on data collection and requirements to provide parental controls.

Companies subject to the law must therefore prepare for partial compliance obligations while the litigation unfolds.

Looking Ahead

California may have pioneered state-level privacy law development, but Texas has rapidly ascended as an equally formidable policymaker and regulator. With a robust legal framework and enforcement team, Texas is reshaping the national privacy landscape. As a result, companies are well-advised to pay close attention to developments in the Lone Star State. As 2025 unfolds, we expect Texas to remain one of the most active and aggressive states in privacy law enforcement that will set a standard of sorts for how state regulators will police data practices in the years to come.

Aaron Simpson is a partner in Hunton's Privacy and Cybersecurity practice group in the firm's New York office. As a leader on the firm's global privacy team, he advises clients on a broad range of complex global privacy, data protection and cybersecurity matters, including with respect to existing and emerging requirements in the US and EU.

Danielle Dobrusin is an associate in Hunton's Privacy and Cybersecurity practice group in the firm's New York office. She advises clients on compliance with US federal and state and international privacy and cybersecurity laws.

Oladoyin Olanrewaju, an associate at Hunton, assisted with the preparation of this article.