Updates
June 27, 2024
Texas AG Turns Up the Heat on Privacy and Data Security

The Texas Data Protection and Security Act (TDPSA) goes into effect on Monday, July 1, 2024.

Eliminating any speculation that this omnibus consumer privacy law might sit on the cupboard shelf, unenforced, the Texas attorney general announced that his office has formed a task force to enforce the TDPSA, along with Texas' several other data privacy laws. This announcement was consistent with the Texas AG office's recent enforcement of Texas' biometrics law and newly enacted Data Broker Law. Data privacy enforcement in Texas is just beginning to heat up.

What Is the Texas Data Privacy Law Landscape?

Texas may not be the first state that comes to mind when thinking about data privacy and security enforcement, but the Texas legislature has been slowly accumulating the tools necessary for a robust enforcement program.

In fact, Texas has had the oldest biometric law in the country, Capture or Use of Biometric Information (CUBI). Despite having this law on the books since 2008, the AG's office only recently started to enforce it publicly in the past two years.

Notwithstanding its strict biometrics law, Texas did not have a comprehensive omnibus consumer privacy law. That is about to change. In the summer of 2023, the Texas Legislature succeeded in a years-long effort toward enacting a data privacy law with the passage of the TDPSA (previously covered here and here). This comprehensive consumer privacy law closely mirrors Virginia and Colorado's laws, with enough minor differences to warrant attention (and potentially action) from entities already in the scope of other state or international consumer privacy laws.

That same month, the Texas legislature passed—and Governor Greg Abbott signed—the Texas Data Broker Law, which requires data brokers meeting certain thresholds and other scoping requirements to register with the

state as data brokers and provide various notices to the public. The Data Broker Law quickly took effect in stages in December 2023 and March 2024.

Given Texas AG Ken Paxton's announcement that his office is expanding and ready to enforce data privacy rights for Texans, companies that have previously given little attention to these laws can no longer afford to do so.

CUBI—Old Law, New Enforcement

Through the passage of CUBI, Tex. Bus. & Com. Code § 503.001, Texas became the first state to govern the collection, use, and retention of biometric data. CUBI imposes many similar requirements to the Illinois Biometric Information Protection Act (BIPA), a law that often garners attention because its private right of action has led to an explosion of litigation in the last decade. Like BIPA, CUBI requires (1) advance notice prior to the collection of a "biometric identifier" ("retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry") for a "commercial purpose," and (2) consent to the collection and specific uses of the biometric identifier. CUBI also imposes a tight retention period for biometric identifiers, requiring businesses to destroy biometric data within one year of the expiration of the business purpose for the data's collection (that one-year retention period applies to biometric data collected by an employer for "security purposes"—triggering at the time the employment relationship terminates). Only the Texas AG may enforce CUBI.

The Texas AG's CUBI enforcement only recently started in earnest in February 2022, when the Texas AG brought its first CUBI action against Meta Platforms, Inc. (Meta). There, the Texas AG alleged that the company's now-deprecated photo-tagging feature violated CUBI through its collection of face geometries, as well as the Texas Deceptive Trade Practices Act (DTPA). That suit followed Meta's settlement of the factually similar *In re Facebook Biometric Information Privacy Litigation* in the U.S. District Court for the Northern District of California (alleging violations of BIPA).

Later that year, the Texas AG filed another CUBI action: *State of Texas v. Google LLC,* alleging that Google LLC (Google) improperly collected, used, and stored biometric identifiers in connection with Google offerings, including Google Photos and Google Assistant. In addition to targeting the collection of face geometries, as in the *Meta* litigation, the Texas AG's suit against Google includes a CUBI claim for the collection of voiceprints.

Both actions pressed forward through 2023 and early 2024. The *Meta* action was recently stayed, pending finalization and court approval of a settlement. That stay was granted and future filings should shed light on the terms of the case's resolution. The *Google* litigation remains ongoing.

With the Texas AG's new data privacy task force assembling, companies that collect, process, and store biometric identifiers should consider the applicability of CUBI to their biometric data processing and, if in scope, review their compliance notices, consents, use cases, and retention periods for compliance.

Texas Data Broker Law—Another Tool for Enforcement

Passed last year and fully in effect as of March 2024, Tex. Bus. & Com. Code § 509 (the Data Broker Law) requires all covered data brokers to register with the Texas Secretary of State and meet specific security and notice obligations. Almost immediately after the effective date this past spring, the Texas AG began enforcing this law.

The scope of entities caught in the Data Broker Law is potentially far wider than that of similar laws adopted in other states. Whereas to qualify as a data broker in other states, a company must transfer personal data to others, in Texas, a company may be considered a data broker if it merely processes (without transferring) personal data.

Specifically, "Data Broker" is defined as an entity that derives (1) more than 50% of its revenue from processing or transferring personal data that the data broker did not collect directly from the individuals to whom the data pertains; or (2) any revenue from processing or transferring the personal data of more than 50,000 Texas residents that the data broker did not collect directly from the individuals to whom the data pertains. While the Data Broker Law uses the same definition of "Personal Data" as the TDPSA (discussed below), the Data Broker Law provides fewer exemptions with respect to specific categories of Personal Data covered by the law (for example, the Data Broker Law exempts data subject to the Gramm-Leach-Bliley Act (GLBA), but not data subject to the Health Insurance Portability and Accountability Act (HIPAA)). Requirements under the Data Broker Law include:

- **Registration.** Data Brokers must register with the Texas Secretary of State by filing a registration statement and paying a $300 fee.
- **Security.** Data Brokers must develop, implement, and maintain a comprehensive information security program, which must include several specific measures, such as employee disciplinary action, documentation of security incident responses, and technical access controls.
- **Notice.** Data Brokers that maintain an internet website or mobile application must post this to their website or application: "The entity maintaining this website is a data broker under Texas law. To conduct business in Texas, a data broker must register with the Texas Secretary of State (Texas SOS). Information about data broker registrants is available on the Texas SOS website."

The Texas AG recently announced that he issued letters to more than 100 companies as an initial measure to enforce registration of Data Brokers under the Data Broker Law. The Data Broker Law provides for daily civil penalties of no less than $100 per day for a violation, in addition to unpaid registration fees. The civil penalty assessed against the same Data Broker may not exceed $10,000 in a 12-month period. Moreover, a violation of the Data Broker Law constitutes a deceptive trade practice under the DTPA and is enforceable as such.

Texas Data Protection and Security Act—The Showstopper

Next week, on July 1, the most comprehensive data privacy law in Texas will go into effect (with an exception for the processing of consumer privacy requests by authorized agents and recognition of Global Privacy Control, obligations that go into effect January 1, 2025). The TDPSA applies to all entities that either (1) conduct business in the state of Texas or produce a product or service consumed by the residents of Texas; (2) process or engage in the sale of personal data; and (3) are not a "small business." The TDPSA refers to entities that "alone or jointly with others, determine[] the purpose and means of processing personal data" as "Controllers" and those engaged to process data on their behalf as "Processors."

While the TDPSA was modeled on Colorado and Virginia's consumer data privacy laws, there are several notable aspects of the TDPSA, including:

- **Specific notices required for the sale of sensitive or biometric data.** Controllers who engage in the sale of sensitive or biometric data must include the following specific language in their privacy notices:

"NOTICE: We may sell your sensitive personal data."

"NOTICE: We may sell your biometric personal data."

- **Exception from access requests for pseudonymized data.** Under the TDPSA, pseudonymous data that is "kept separately" and subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual may be exempt from obligations to respond to consumer requests for this data.

- **Ability to opt out of certain types of profiling.** Consumers may opt out of profiling in furtherance of a "decision that produces a legal or similarly significant effect." However, a decision can only produce a legal or similarly significant effect if the decision results in the provision or denial of financial services, housing, insurance, healthcare services, education enrollment, employment, criminal justice, or access to basic necessities.
- **Fewer obligations on loyalty programs.** Multiple consumer privacy laws, including those in California and Colorado, require certain detailed disclosures when offering financial incentives or loyalty programs. The TDPSA does not have specific disclosure requirements or valuation obligations, as required, for example, under the Colorado Privacy Act Rule 6.05.

Because the TDPSA does not authorize the Texas AG to promulgate regulations, the Texas AG's public enforcement activity and any published guidance will be critical sources of information about how the regulator interprets the TDPSA and what influence the regulations or enforcement activities in other states may have, if any. Companies should continue to monitor any related enforcement actions or publications from the AG's office to ensure compliance.

Enforcement is expected to occur. On June 4, the Texas AG's office stated that it has "launched a major data privacy and security initiative, establishing a team that is focused on aggressive enforcement of Texas privacy laws." Like California, Colorado, and Connecticut—whose enforcement bodies have been active in promulgating reports, guidance (and in some instances, regulations), and quickly launching regulatory investigations—the Texas AG's office noted that its team "is poised to become among the largest in the country focused on enforcing privacy laws."

What Comes Next—Out of the Frying Pan and Into the Fire

Texas' data privacy legal and regulatory landscape is rapidly evolving with significant new laws and enforcement initiatives coming into effect. The recent activity around the Data Broker Law, TDPSA, and CUBI represent substantial steps forward in regulating consumer privacy in Texas. With the AG's office gearing up for enforcement—specifically calling out its intended enforcement of the TDPSA, the Data Broker Law, CUBI, and other federal privacy laws, such as COPPA and HIPAA—companies doing business in Texas should be mindful of their privacy obligations and the increased likelihood of AG scrutiny.

The Texas AG closed the June press release with this warning to businesses: "As many companies seek more and more ways to exploit data they collect about consumers, I am doubling down to protect privacy rights ... With companies able to collect, aggregate, and use sensitive data on an unprecedented scale, we are strengthening our enforcement of privacy laws to protect our citizens."

Companies operating in Texas or handling data that is linked or reasonably linkable to an identified or identifiable Texas resident should stay vigilant and proactive in their compliance efforts.

Authors

Explore more in

Privacy & Security Litigation Technology Transactions & Privacy Law Advertising, Marketing & Promotions

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Trump Executive Orders on DEI Initiatives