

AG Watch: Texas Is Entering New Privacy Enforcement Era

By **Paul Singer** (March 12, 2025)

This article is part of a regular column that features insights from former state attorney general office leaders, who share observations on that state's latest enforcement news and trends, and compliance implications.



Paul Singer

On Jan. 13, Texas Attorney General Ken Paxton sued Allstate and Arity in *State of Texas v. The Allstate Corp.*, in the District Court of Montgomery County, Texas, in the state's first action under the Texas Data Privacy and Security Act, or TDPSA, which went into effect on July 1, 2024.[1]

While it's a groundbreaking suit both because of the new law and the factual allegations, it should not be a surprise to those who have been tracking Paxton's prioritization of privacy enforcement over the past year.

In many ways, this suit is the culmination of a long-standing commitment to vigorously enforcing privacy laws in Texas, and should be seen as a sign of things to come from Texas and its sister states.

Texas Enforcement History

During the lead-up to the July 1 effective date of the TDPSA, Paxton made a number of announcements signaling his commitment to enforcing the new law.

On June 4, Paxton announced the creation of a dedicated privacy team as part of a "major data privacy and security initiative." [2] Not only was the intent to enforce the TDPSA part of this announcement, but Paxton also further made clear that this newly created unit would be responsible for enforcing Texas' Identity Theft Enforcement and Protection Act, [3] the Data Broker Act [4] the Biometric Identifier Act, [5] and the Deceptive Trade Practices Act, [6] as well as federal laws, including the Children's Online Privacy Protection Act [7] and the Health Insurance Portability and Accountability Act. [8]

The new unit worked quickly to back up these promises, first by announcing a sweeping investigation into multiple automobile manufacturers related to their collection and sale of driver data; [9] then by sending over 100 letters to companies for their "apparent failure to register as data brokers" pursuant to Texas' Data Broker Act; [10] and next by announcing the largest single-state settlement in history in July with Meta over alleged violations of Texas' biometric laws — *State of Texas v. Meta Platforms Inc.*, in the 71st District Court of Harrison County, Texas. [11]

While these actions were clearly coordinated to support the new privacy unit and serve as a warning shot to all companies of Texas' intent to take privacy enforcement seriously, Texas has long been a leader in protecting the personal information of its citizens.

Indeed, 17 years earlier, Texas became the first state to bring actions in the U.S. District Court for the Western District of Texas under the Children's Online Privacy Protection Act, suing a video game informational website in *State of Texas v. Future US Inc.*, and an online interactive social media company in *State of Texas v. The Doll Palace Corp.*, for their failure

to adequately obtain parental consent prior to collecting personal information from children under 13.[12]

At that time, Texas also had a dedicated team focused on privacy and technology consumer protection initiatives, and lawyers from that team have continued to lead investigations into the biggest privacy and data security matters that have affected consumers, including the multistate settlement with Marriott, in *State of Texas v. Marriott International Inc.*, in the 250th District Court of Travis County, Texas, over a significant data breach that spanned four years.[13]

While Texas' privacy enforcement is not new, something feels different with the recent announcements, both from the type of target — large, Fortune 100 companies — and the more aggressive nature of their actions, i.e., publicly announcing investigations and bringing suit following a more limited investigation.

Texas' recent lawsuit filed against Allstate is a prime example of this new posture and should be viewed as a clear sign of what's to come from this new privacy team.[14]

Texas v. Allstate and Arity

Stemming from the publicly announced investigation into the automobile industry, Texas announced a lawsuit against several Allstate-owned companies, collectively referred to as Allstate, alleging violations of the TDPSA, the Data Broker Act and provisions of the Texas Insurance Code prohibiting unfair and deceptive conduct.

The suit accuses Allstate of obtaining "trillions of miles" of consumer driving data without providing consumers with proper notice and control of their data. Specifically, Texas alleges that Allstate marketed a software development kit to several third-party application developers that transmitted detailed data back to Allstate, which it used to compile a large database of driving information. Information collected included location data, driving events like acceleration and deceleration, distracted driver indicators, speed and the metadata of a user's phone.

The state further alleges that Allstate specifically targeted apps that already collect information, like geolocation, in order to conceal the software development kit's collection and additional use of that information. Ultimately, the state alleges that Allstate uses its compiled database not only for its own underwriting purposes, but also to sell to other insurers.

As the lawsuit points out, however, the data collected is not necessarily coming from the app user's vehicle, or even the driver of the vehicle. For example, a consumer with a third-party app installed that includes the Allstate software development kit might be a passenger in a vehicle, which means the data collected and allegedly used by insurers is not indicative of the driving habits of the phone owner.

Despite the potential economic effect on consumers, the state alleges that the third-party apps using the software development kit do not disclose the collection and use of data, and Allstate itself further fails to clearly disclose its practices. Paxton points to Allstate's privacy policy, which he says is filled with "untrue or contradictory statements," including that it does not sell personal information for any monetary value and that the data collected is only used for analytics and profiling.

Notably, the state alleges Allstate also did not provide consumers with an easy means to opt

out of the data collection.

Texas alleges that this conduct constitutes numerous violations of the TDPSA, including that as a controller, Allstate did not provide an adequate privacy notice — in part by not providing a specific notice of the sale of data — processed data without obtaining consumers' consent, and failed to disclose its targeted advertising practices and an opt-out mechanism.

In addition, because Allstate was processing and transferring data of individuals it didn't directly collect from, the state alleges Allstate acts as a data broker without a required registration with the Texas secretary of state pursuant to the Data Broker Act.

Finally, Texas alleges that the series of practices of failing to verify consent, ignoring the lack of consent when obtaining and utilizing the data, using the data for its own purposes despite statements in its privacy policy, and marketing data as "driving behavior" data when it knew it was collecting data only from individuals' phones, all constituted violations of the Texas Insurance Code's prohibition on unfair or deceptive acts and practices.

Like many consumer protection cases, Texas seeks civil penalties, injunctive relief, restitution for consumers and the destruction of data obtained through the allegedly deceptive conduct.

Broader Implications of Texas v. Allstate and Arity

Although the litigation is in its early stages, there are several important insights that companies and privacy practitioners can take away from this case.

First, Texas is doubling down on its historical leadership in the privacy arena, and will continue this aggressive push for at least as long as Paxton's tenure as attorney general. He has clearly prioritized privacy and data security during this term, and is doing so in dramatic fashion. And Texas will continue to move quickly in investigations and not be afraid to commit itself to litigation if it cannot obtain a quick and meaningful settlement once violations are discovered.

Second, watch for low-hanging fruit. Texas' lawsuit in some ways is an outlier by pursuing a consumer protection action against a company that has no direct relationship with consumers in many instances, but that the state alleges is nevertheless obligated to verify the adequacy of third-party notices and consent. But that said, the nature of the allegations — a failure to clearly and conspicuously disclose data collection practices and obtain the requisite consent — follow core deceptive trade practice principles.

The allegations against Allstate related to the inadequacies of its privacy policy should be a reminder to all companies to evaluate their policies to ensure compliance with applicable state law, as noncompliance creates an easy target for an enforcer.

Third, privacy is not partisan. It's symbolic that the arguable two leaders in privacy legislation and litigation today are California and Texas — two states that politically rarely see eye-to-eye. To best predict which states will aggressively enforce their laws, one has to look beyond the political party and instead focus on the office and the attorney general themselves. Attorneys general tend to be transparent in their enforcement priorities and commit the resources necessary to fulfill those initiatives. Texas has demonstrated a clear commitment, and one should expect more to come from its team.

Fourth, other states will feel the pressure to follow Texas' lead. Even in the absence of a comprehensive state privacy law, states will target companies for similar practices. As noted above, many of the allegations against Allstate are core unfair or deceptive trade practice act violations. As such, an aggressive push by Texas may trigger more state action, and even the formation of more coordinated multistate actions, in order to keep up with the Lone Star State.

Finally, companies should make sure to evaluate all of the potentially applicable laws that exist in the states where they do business. While a major focus of this litigation is on the first application of the TDPSA, the fact that Texas also brought claims under the Insurance Code and Data Broker Act serve as a reminder that states like Texas will use all the tools in their toolbox in an enforcement action.

This is especially true when it comes to certain industries like insurance, which in many states is exempted from coverage under general deceptive trade practice laws.

It is imperative to make sure you know what laws apply to your business, and that you adapt your practices to stay off of the enforcement radar.

Paul Singer is a partner at Kelley Drye & Warren LLP. He was previously at the Texas attorney general's office for more than two decades, including as associate deputy attorney general for civil litigation and chief of the consumer protection division.

Kelley Drye special counsel Beth Chun and Abby Stempson, and associate Andrea deLorimier, contributed to this article.

Disclosure: Paul Singer represented the state of Texas in the Doll Palace case mentioned in the article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Tex. Bus. & Com. Code § 541.

[2] <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive>.

[3] Tex. Bus. & Com. Code § 521.

[4] Tex. Bus. & Com. Code § 509.

[5] Tex. Bus. & Com. Code § 503.

[6] Tex. Bus. & Com. Code § 17.41 et seq.

[7] 15 U.S.C. 91.

[8] 45 C.F.R. 160, 164.

[9] <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-opens-investigation-car-manufacturers-collection-and-sale-drivers-data>.

[10] <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-notifies-over-100-companies-their-apparent-failure-comply-texas-data>.

[11] State of Texas v. Meta Platforms, Inc., No. 22-0121 (71st Judicial District, Harrison County, Texas, July 30, 2024); see also <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture>.

[12] See State of Texas v. Future US, Inc., No. A07CA987LY (W.D.T.X. Dec. 5, 2007); State of Texas v. The Doll Palace Corporation et al, No. A07CA988SS, (W.D.T.X. Dec. 5, 2007); see also <https://www.wired.com/2007/12/texas-attorney/>.

[13] See State of Texas v. Marriott International, Inc., No. D-1-GN-24-008193 (250th Judicial District, Travis County, Oct. 9, 2024); see also <https://texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-35-million-settlement-following-investigation-marriotts-breach>.

[14] See State of Texas v. Allstate et. al, No. 25-01-00561 (457th Judicial District, Montgomery County, Jan. 13, 2025); <https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf>.