

Taking Stock of the Texas AG's New Focus on Privacy, Technology, and AI

Gavin George, Tim Newman¹

When one thinks of privacy and technology enforcement, Texas may not initially come to mind. But the landscape is changing thanks to a recent shift in priorities and tactics at the Texas Office of the Attorney General (the “OAG” or the “State”). Hot-button issues at the OAG have recently come to include the collection of biometric data, compliance with Texas’ new comprehensive consumer privacy law, the online safety of children, and AI washing. Companies doing business in Texas should take note of this sea change and take proactive steps to avoid ending up in the crosshairs.

Texas AG Announces New Privacy, Technology, and AI Enforcement Team

On June 4, 2024, the OAG announced a major initiative to “protect Texans’ sensitive data from illegal exploitation by Tech, AI, and Other Companies.”² As part of this initiative, the OAG established an enforcement team within its Consumer Protection Division tasked with enforcing the new Texas Data Privacy and Security Act (“TDPSA”) along with a host of other privacy and consumer protection laws already on the books in Texas. This new privacy enforcement team is already more than ten lawyers strong and is expected to grow.

To be fair, Texas had not exactly been asleep at the wheel when it comes to privacy enforcement. The State brought lawsuits under the federal Telephone Consumer Protection Act (“TCPA”) related to unsolicited faxes in the late 1990s and early 2000s,³ was one of the first states to enforce the federal Children’s Online Privacy Protection Act (“COPPA”) in 2007,⁴ and has led multi-state enforcement efforts arising from consumer data breaches.⁵ Still, the OAG’s announcement of a new team and new privacy enforcement focus signaled a distinct priority shift.

¹ Gavin George and Tim Newman are both partners at Haynes Boone. They can be reached at gavin.george@haynesboone.com and timothy.newman@haynesboone.com, respectively.

² See Press Release, Ken Paxton, Attorney General of Texas, Attorney General Ken Paxton Launches Data Privacy and Security Initiative to Protect Texans’ Sensitive Data from Illegal Exploitation by Tech, AI, and Other Companies (June 4, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive>.

³ See, e.g., *The State of Texas v. American Blastfax, Inc.*, 164 F. Supp. 2d 892 (W.D. Tex. 2001).

⁴ *Texas AG files complaint against Web sites aimed at children*, LAW.COM (Dec. 7, 2007), <https://www.law.com/nationallawjournal/almID/900005497825/>.

⁵ See Press Release, Ken Paxton, Attorney General of Texas, AG Paxton Announces \$17.5 Million Settlement with Home Depot Regarding Data Breach (Nov. 24, 2020), <https://www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-175-million-settlement-home-depot-regarding-data-breach>.

The OAG is Focused on the Collection and Use of Biometric Identifiers

Leading up to the OAG's announcement of this new enforcement focus, it had been engaged in lawsuits related to the capture and use of biometric information. In February 2022, the State sued Meta in Harrison County alleging that its Facebook "Tag Suggestions" feature violated the Texas Capture or Use of Biometric Identifier Act ("CUBI") and the Texas Deceptive Trade Practices Act (the "DTPA").⁶ This was the first lawsuit under CUBI, a statute that was codified in 2009, but sat dormant for years. Broadly speaking, CUBI prohibits the capture of biometric identifiers – retina or iris scan, fingerprint, voiceprint or record of hand or face geometry – for a commercial purpose without notice and consent from the owner.⁷ Under CUBI, organizations must protect biometric identifiers and destroy them within a reasonable time, generally within one year after the purpose for collecting the identifiers ends.⁸

In its lawsuit, the State alleged that Meta collected and made commercial use of facial geometry without notifying consumers and obtaining their informed consent.⁹ Meta vigorously defended the case for more than two years and denied any wrongdoing in the settlement, but ultimately resolved the case with a \$1.4 billion payment.¹⁰ The OAG touted the settlement as the largest ever obtained from an action by a single state and the largest privacy settlement ever secured by an attorney general.¹¹

The State is currently in litigation with Google in Midland County related to similar allegations. Filed in October 2022, the OAG's lawsuit alleges that Google's collection and use of facial geometry and voiceprints for various products without notice and consent violates CUBI and the DTPA.¹² Google is battling the lawsuit, and a trial date is to be determined.¹³ We can expect the OAG's new privacy team to be on the prowl for additional cases it might bring under CUBI.

⁶ See First Amended Petition, *The State of Texas v. Meta Platforms, Inc.*, Cause No. 22-0121 (71st Judicial Court, Harrison County May 20, 2022).

⁷ TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

⁸ *Id.*

⁹ *Meta Platforms*, *supra* note 6, at 16.

¹⁰ See Agreed Final Judgment, *The State of Texas v. Meta Platforms, Inc.*, Cause No. 22-0121 (71st Judicial District, Harrison County July 30, 2024).

¹¹ Press Release, Ken Paxton, Attorney General Ken Paxton Secures \$1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data In Largest Settlement Ever Obtained From An Action Brought By A Single State (July 30, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture>.

¹² See Original Petition, *The State of Texas v. Google, LLC*, Cause No. CV58999 (385th Judicial District, Midland County, Oct. 20, 2022).

¹³ The State has also sued Google in Victoria County alleging it violated the DTPA by not fully disclosing its data collection to Google users. See Original Petition, *The State of Texas v. Google, LLC*, Cause No. 22-01-

Both the Meta and Google lawsuits followed settlements those companies reached in connection with Illinois' Biometric Identifier Protection Act¹⁴, which is similar to CUBI. Although Texas' CUBI does not provide for a private right of action, the penalties are stiffer, allowing the OAG to potentially recover \$25,000 per violation. We may see similar follow-on actions in the future, particularly against defendants that are big tech companies, whose conduct is a particular focus of the OAG.¹⁵

The OAG is Actively Enforcing Texas' New Comprehensive Privacy Law

Alongside the OAG's new enforcement focus, Texas' new comprehensive privacy law came online in July 2024.¹⁶ The TDPSA establishes consumer rights similar to other state privacy laws and subjects businesses to new data security and consumer notification requirements. More specifically, the law gives consumers (1) the right to confirm whether a business is processing the consumer's personal data, (2) the right to opt out of data processing for targeted advertising, data sales, or profiling to inform certain decisions that affect the consumer, and (3) the right to access, correct, delete, or obtain a copy of the consumer's data in a portable or transmittable form.¹⁷ These rights cannot be waived through contract. Businesses subject to the law are also required to implement new secure processes for handling personal data and responding to consumer inquiries based on these new consumer rights.¹⁸

The TDPSA also specifies certain obligations related to a business's consumer privacy notices. The notices must be reasonably accessible and clear regarding processing and sharing of personal data and must include disclosure of:

- the categories of personal information processed;
- the purpose of processing personal data;
- the categories of personal data shared with third parties;
- the categories of third parties with whom consumer data is shared; and

88230-D (377th Judicial District, Victoria County, Jan. 24, 2022). The Thirteenth Court of Appeals recently dismissed the lawsuit for lack of personal jurisdiction, and the OAG has petitioned the Supreme Court of Texas for review. See *Google LLC v. State of Texas*, No. 13-23-00114-CV, 2025 WL 52611 (Tex. App.—Corpus Christi-Edinburg Jan. 9, 2025); Petition for Review, *The State of Texas v. Google LLC*, No. 13-23-00114-CV (Tex. Feb. 24, 2025).

¹⁴ See Order, *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD (N.D. Cal. Feb. 26, 2021); Joint Status Report, *Lindabeth Rivera and Joseph Weiss v. Google Inc.*, No. 1:16-cv-02714 (N.D. Ill. Oct. 25, 2022).

¹⁵ See *Big Tech*, KEN PAXTON, ATTORNEY GENERAL OF TEXAS, <https://www.texasattorneygeneral.gov/initiatives/big-tech> (last visited Mar. 10, 2025).

¹⁶ See TEX. BUS. & COM. CODE ANN. §§ 541.001-205 (West 2024).

¹⁷ *Id.* § 541.051 (West).

¹⁸ *Id.* § 541.055 (West).

- a description of the methods through which consumers can submit requests to exercise their consumer rights.¹⁹

If certain types of personal data are sold by the business, the notice must also state, “NOTICE: We may sell your sensitive personal data,” and if biometric data is sold, the notice must state, “NOTICE: We may sell your biometric personal data.”²⁰

With some exceptions for state agencies, higher education institutions, nonprofits, financial institutions, electric utilities and providers, and HIPAA-covered entities or business associates, the TDPSA applies to businesses that (1) conduct business in Texas or produce goods or services consumed by residents of the State of Texas, (2) process or engage in the sale of personal data, and (3) are not a small business defined by the U.S. Small Business Administration (with one exception).²¹ The TDPSA allows for civil penalties up to \$7,500 for each violation and injunctive relief, and the OAG can seek reasonable attorneys’ fees and other expenses incurred from investigating and bringing action under the law.²²

During the first two months the TDPSA was online, the OAG received hundreds of consumer complaints related to the law and quickly initiated notice and cure discussions with numerous companies. The State brought its first lawsuit under the statute in January 2025, taking Allstate and related entities to task for their alleged collection and use of driver data without notice or consent.²³ In a lawsuit filed in Montgomery County, the State alleges the defendants provided software development kits (“SDK”) to third-party app developers who included those SDKs in apps they offered to consumers.²⁴ Once installed, those apps collected driver data, including geolocation data, accelerometer data, magnetometer data, and gyroscopic data (which monitors details such as the phone’s altitude, longitude, latitude, bearing, GPS time, speed, and accuracy) and fed that data back to Allstate for the company’s use in making underwriting decisions.²⁵ According to the State, this conduct violates the TDPSA and the Texas Data Broker Act, which requires data brokers to register with the Texas Secretary of State and implement an information security

¹⁹ *Id.* § 541.102 (West).

²⁰ *Id.*

²¹ *Id.* § 541.002 (West).

²² *Id.* § 541.155 (West).

²³ See Original Petition, *The State of Texas v. the Allstate Corporation, et al.*, Cause No. 25-01-00561 (457th Judicial District, Montgomery County Jan. 13, 2025).

²⁴ *Id.* at 9.

²⁵ *Id.* at 10.

program to protect personal data.²⁶ The defendants have pushed back on the allegations, and that litigation is ongoing.²⁷

The State’s allegations against Allstate and related entities resemble those the State lodged against General Motors and OnStar in a prior August 2024 suit. In that case, also filed in Montgomery County, the OAG alleged the defendants illegally collected, used, and sold driver data, including drive date, start time, end time, vehicle speed, seatbelt status, distance driven, and other driving metrics.²⁸ And according to the State, at least two of the companies who received the data allegedly used it to calculate “Driving Scores” and sold those scores to insurance companies for underwriting decisions.²⁹ The OAG did not allege a violation of the TDPSA, which had just gone into effect the month before, but instead alleged that the defendants engaged in deceptive practices under the DTPA to secure customers’ enrollment in the data collection process and never disclosed it would sell that data to others.³⁰ The defendants have denied wrongdoing, and litigation is ongoing.³¹

One common element in the Allstate and GM lawsuits is the alleged sharing of information with insurance carriers. This appears to be another hot-button issue for the OAG, and companies operating in that data cycle should take note. We can expect the OAG to remain focused on this issue in future investigations and litigation.

The OAG is Focused on Protecting Children Online

Shortly after the TDPSA came online, Texas’ new Securing Children Online Through Parental Empowerment (“SCOPE”) Act also went into effect. The law applies generally to Digital Service Providers (“DSP”) that operate a website or application that processes personal identifying information (“PII”) via the internet and that (1) connects users so they can socially interact with other users on the digital service; (2) allows users to create a public or semi-public profile; and (3) allows users to create or post content that can be viewed by other users.³²

The SCOPE Act provides several protections to minors. Among other things, it prohibits DSPs from sharing or selling a minor’s personal information without parental consent and

²⁶ *Id.* at 1; see TEX. BUS. & COM. CODE ANN. §§ 509.005, 509.007 (West 2023).

²⁷ See Original Answer and Affirmative Defenses, *The State of Texas v. the Allstate Corporation, et al.*, Cause No. 25-01-00561 (457th Judicial District, Montgomery County Feb. 19, 2025).

²⁸ See Original Petition, *The State of Texas v. General Motors LLC and OnStar, LLC*, Cause No. 24-08-12392, at 9 (457th Judicial District, Montgomery County Aug. 13, 2024).

²⁹ *Id.* at 19.

³⁰ *Id.* at 31.

³¹ See First Amended Answer and Affirmative Defenses, *The State of Texas v. General Motors LLC and OnStar, LLC*, Cause No. 24-08-12392 (457th Judicial District, Montgomery County Jan. 22, 2025).

³² TEX. BUS. & COM. CODE ANN. § 509.002 (West 2024).

requires them to offer parental controls over minors' accounts.³³ DSPs must also register the age of each user and minimize the collection of personal data from known minors (18 and under), and they may not (1) allow a child to purchase or engage in financial transactions; (2) share, disclose, or sell a child's personal data; (3) use their services to collect a child's precise geolocation; or (4) deliver targeted advertising to a child.³⁴ Finally, DSPs must create and provide parents and guardians with tools to supervise the minor's use of the service, and they may not advertise products, services, or activities that are unlawful for minors.³⁵

More generally, DSPs must disclose how algorithms are used to provide content and the manner in which those algorithms promote, rank, and filter content.³⁶ And DSPs that knowingly publish or distribute material more than one-third of which is harmful or obscene must use a commercially reasonable age verification method, and they must verify, using a commercially reasonable method, each person seeking to perform an action on a digital service as a minor's parent or guardian.³⁷ Violations of the SCOPE Act are enforced through the DTPA, and the OAG can seek up to \$10,000 per violation and injunctive relief.³⁸

The OAG wasted little time in filing its first lawsuit under this statute. In a suit filed against TikTok in October 2024, the State alleges TikTok violated the SCOPE Act by sharing, disclosing, or selling a minor's PII without permission from the child's parent or guardian and failing to provide parents with tools to manage and control a child's privacy and account settings.³⁹ In a follow-on suit filed against the company in January, the State also alleges TikTok violated the DTPA by marketing its app as safe for minors when it is not.⁴⁰ TikTok is aggressively defending the lawsuits, which are pending in Galveston County.⁴¹

Shortly after filing against TikTok, the OAG announced an investigation of 15 other companies regarding their privacy and safety practices for minors under the SCOPE Act

³³ *Id.* §§ 509.052, 509.054 (West).

³⁴ *Id.* §§ 509.051-509.052 (West).

³⁵ *Id.* §§ 509.054-509.055 (West).

³⁶ *Id.* § 509.056 (West).

³⁷ *Id.* §§ 509.057, 509.101 (West).

³⁸ *Id.* § 509.151 (West); TEX. BUS. & COM. CODE ANN. § 17.47 (West 2019).

³⁹ See Original Petition, *The State of Texas v. TikTok Ltd., et al.*, Cause No. 24-CV-1763 (56th Judicial District, Galveston County Oct. 3, 2024).

⁴⁰ See Original Petition, *The State of Texas v. TikTok Inc., et al.*, Cause No. 25-CV-0033 (10th Judicial District, Galveston County Jan. 9, 2025).

⁴¹ See First Amended Answer, *The State of Texas v. TikTok Ltd., et al.*, Cause No. 24-CV-1763 (56th Judicial District, Galveston County Jan. 29, 2025).

and the TDPSA.⁴² It remains to be seen where these investigations will go, but we can be sure the OAG will be on the hunt for any violations of the SCOPE Act. Protection of children online has long been a priority of the OAG, even before the SCOPE Act was enacted and before this recent shift in priorities.

All that said, the constitutionality of the SCOPE Act is currently up in the air. In August 2024, before the law took effect, a federal court preliminarily enjoined enforcement of the monitoring-and-filtering requirements of the SCOPE Act (those provisions that require DSPs to monitor certain categories of content and filter it from being viewed by known minors).⁴³ The court found that “the law’s restrictions on speech fail strict scrutiny, are unconstitutionally vague, and are preempted by Section 230 of the federal Communications Decency Act.”⁴⁴

In February 2025, in a separate lawsuit, the same court preliminarily enjoined the targeted advertising restrictions (those that impose regulations on how DSPs can display advertisements to known minors) and the content monitoring and age verification requirements (those that require DSPs to reasonably verify the age of users and prohibit them from viewing obscene or harmful conduct) for similar reasons.⁴⁵ The court also reiterated its prior preliminary injunction of the monitoring-and-filtering requirements.⁴⁶

The OAG has appealed both injunctions to the Fifth Circuit Court of Appeals.⁴⁷ The ultimate enforceability of the SCOPE Act, and the OAG’s pending cases and investigations, hang in the balance until the Fifth Circuit weighs in.

The OAG is Also Focused on AI Washing

We have also seen increased activity out of the OAG related to companies’ use of artificial intelligence. In October 2024, the OAG announced a settlement with Pieces Technologies, Inc., a technology company offering a product that leveraged generative AI to summarize

⁴² Press Release, Ken Paxton, Attorney General of Texas, Attorney General Ken Paxton Launches Investigations into Character.AI, Reddit, Instagram, Discord, and Other Companies over Children’s Privacy and Safety Practices as Texas Leads the Nation in Data Privacy Enforcement (Dec. 12, 2024),

[https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigations-characterai-reddit-instagram-discord-and-](https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigations-characterai-reddit-instagram-discord-and-other#:~:text=Attorney%20General%20Ken%20Paxton%20has,the%20Texas%20Data%20Privacy%20and)

[other#:~:text=Attorney%20General%20Ken%20Paxton%20has,the%20Texas%20Data%20Privacy%20and](https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigations-characterai-reddit-instagram-discord-and-other#:~:text=Attorney%20General%20Ken%20Paxton%20has,the%20Texas%20Data%20Privacy%20and).

⁴³ *Computer & Commc’ns Indus. Ass’n v. Paxton*, 747 F. Supp. 3d 1011, 1044 (W.D. Tex. 2024).

⁴⁴ *Id.*

⁴⁵ *Students Engaged in Advancing Texas v. Paxton*, No. 1:24-CV-945-RP, 2025 WL 455463, at *19 (W.D. Tex. Feb. 7, 2025).

⁴⁶ *Id.*

⁴⁷ See Defendant’s Notice of Appeal, *Computer & Commc’ns Indus. Ass’n v. Paxton*, No. 1:24-cv-849-RP (WD. Tex. Sept. 5, 2024); Defendant’s Notice of Appeal, *Students Engaged in Advancing Texas v. Paxton*, No. 1:24-CV-945-RP19 (W.D. Tex. Feb. 11, 2025).

patient charts and draft clinical notes for healthcare facilities.⁴⁸ Although no specific allegations were made, the OAG seemed to suggest the company's statements regarding the "hallucination rate" of its product may have been false, misleading, or deceptive in violation of the DTPA.⁴⁹ These so-called "AI Washing" claims are similar to claims that the Securities and Exchange Commission and the Federal Trade Commission have brought at the federal level.⁵⁰ Pieces Technologies denied any liability, but agreed to an assurance of voluntary compliance that required clear and conspicuous disclosures in its advertising, among other things.⁵¹

In February, the OAG also announced an investigation into DeepSeek, a Chinese AI company, for suspected AI washing and violations of the TDPSA.⁵² The OAG also voiced security concerns in announcing its investigation, but has not yet filed any actions related to this investigation.⁵³ Regardless, these events signal a continued focus on companies' use of AI and claims made related to AI performance.

Change in Tools and Tactics

In addition to the OAG's shift in focus to privacy, technology, and AI matters, we have seen a shift in enforcement tactics that potentially up the ante for companies doing business in Texas. The DTPA will, without a doubt, continue to be an important enforcement tool for the OAG. The OAG's new privacy team is housed within the Consumer Protection Division, and the DTPA provides specific authority for the OAG to issue civil investigative demands. The law also broadens enforcement capabilities and available penalties for the State, even where the OAG can allege a violation of a more specific privacy law, and the DTPA is the OAG's traditional bread-and-butter enforcement tool.

But newer privacy laws give the OAG a wider arsenal to choose from, and we can expect to see more enforcement activity related to those specific laws, even if OAG actions continue

⁴⁸ See Agreed Final Order, *In the Matter of the State of Texas and Pieces Technologies, Inc.*, Cause No. DC-24-13476 (191st Judicial District, Dallas County Oct. 2, 2024).

⁴⁹ *Id.*

⁵⁰ See Press Release, Securities and Exchange Commission, SEC Charges Restaurant-Technology Company Presto Automation for Misleading Statements About AI Product (Jan. 14, 2025), <https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11352-s>; Press Release, Federal Trade Commission, FTC Announces Crackdown on Deceptive AI Claims and Schemes (Sept. 25, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>.

⁵¹ *In the Matter of Pieces Technologies, Inc.*, *supra* note 48.

⁵² Press Release, Ken Paxton, Attorney General of Texas, Attorney General Ken Paxton Announces Investigation into DeepSeek and Notifies the Chinese AI Company of its Violation of Texas State Law (Feb. 14, 2025), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-announces-investigation-deepseek-and-notifies-chinese-ai-company-its>.

⁵³ *Id.*

to include DTPA claims. In recent statements, the OAG has suggested that Texas' new direct-to-consumer genetic testing law (which governs the confidentiality of biological samples and genetic testing or analysis) or data breach disclosures under the Texas Identity Theft Enforcement Act could become additional areas of focus.

We are also seeing a change in tactics from the OAG. OAG investigations have become more public, with the OAG often issuing press releases to announce investigations before any allegations have been made in court. And in recent public statements, OAG leadership has highlighted a special litigation team within the Consumer Protection Division and touted a "litigation first" strategy, stating a preference for filing public cases and getting discovery rolling, rather than relying on the more traditional approach of gathering information through civil investigative demands that are largely private. Leadership also shared it will likely continue filing cases outside the traditional Travis County venue based on a perceived bias against cases filed by the OAG in that county. Litigation in more rural counties, which tend to be more conservative in Texas, could be less convenient venues for defendants and could result in judges or juries that are more sympathetic to the arguments of the conservative-led OAG. These tactics put a premium on reviewing privacy compliance now, and taking any necessary steps to shore up deficiencies, long before any interest arises from the State.

The Takeaway and Best Practices

One could dismiss much of the OAG's recent enforcement activity as "follow on" activity in light of similar litigation filed against many of these same defendants in other states. But there is more to the story. The OAG has become laser-focused on privacy and consumer protection, especially when big tech companies or AI are involved. It is committing significant resources to the effort, it has secured manpower, and it won't shy away from litigation, often filing suit early and in less traditional venues. The tea leaves suggest more enforcement activity is on the way. And we can expect the OAG to continue leveraging the DTPA and other laws to broaden enforcement authority and drive up potential penalties, upping the ante for defendants facing enforcement action.

For businesses that handle Texas consumer data, especially those offering online platforms or AI products and services, now is the time to review compliance with Texas law to make sure your business doesn't trip any wires. Among other things, map the consumer data your company has in its possession, and conduct a data protection assessment each time a new use of personal data is proposed to ensure that data is properly protected. Take steps to limit and protect personal data collection and processing activities, establish or update disclosure and consent requirements, revise or draft a consumer-facing privacy notice, assess and update your data governance practices, establish or update your

processes for responding to consumer requests related to their personal data, review and/or update processes for retention and deletion of data, and assess, manage, and disclose any “sales” of personal information. And businesses using AI should review public statements carefully to ensure they are accurate and transparent. Taking these steps should put companies well on their way to compliance and avoiding unnecessary run-ins with the OAG.

If the OAG does come knocking, a proactive, cooperative approach that involves early engagement with the State is often the best course. Circumstances may dictate otherwise, but respondents that engage with enforcement lawyers early to understand their concerns and proactively investigate and address those concerns, as needed, often achieve a more favorable outcome.