



House Committee on Delivery of Government Efficiency

August 19, 2026

Testimony submitted by: Kyle Trojahn, Policy Analyst, Texas Appleseed
ktrojahn@texasappleseed.org

Introduction

Chairman Capriglione, Vice Chair Bhojani, and Members of the Committee: thank you for the opportunity to offer written testimony to the House Committee on Delivery of Government Efficiency regarding Data Privacy and Security: Implementation and Effectiveness of the Texas Data Privacy and Security Act.

Texas Appleseed is a nonpartisan nonprofit focused on bringing about policies that are fair, just, and equitable for all Texans. The Fair Financial Services Project at Texas Appleseed is dedicated to advocating for consumer protections across a range of issues, including data privacy and control of our personal information in the current big data economy. We look forward to working with the Committee to support consumer protection, data privacy, and financial well-being in Texas.

I. Background: The Market in Texans' Personal Data, and What it Costs

With the Texas Data Privacy and Security Act (TDPSA) and the state data broker registration and data security law, the Texas Legislature gave Texans important privacy rights on paper.¹ The question this interim charge asks is the right one: do those rights work in practice? To help answer it, Texas Appleseed spent the past few months testing the law in the field.

Our preliminary answer is that the TDPSA includes impactful provisions, but Texans attempting to use their rights encounter friction at nearly every step. And, one of the most dangerous categories of data, precise geolocation, remains legally for sale. These preliminary findings point to a need for default data protection options and added protections for sensitive data to fulfill the important promise of the law.

Texans' personal data is bought and sold at a scale that no individual can track. As of August 13, 2026, 419 data brokers have registered with the Texas Secretary of State, and registration captures only part of the market: industry estimates count thousands of brokers operating nationally, and the universe of data controllers that collect and share personal data is larger still. Our analysis of the registry's filings found 130 registered brokers indicated that they collect geolocation information as part of the the data they process and transfer, and 38 registered brokers affirmatively describe

¹[Tex. Bus. & Com. Code ch. 541](#) (Texas Data Privacy and Security Act, H.B. 4, 88th Leg. (2023)); [Tex. Bus. & Com. Code ch. 510](#) (Data Broker Registration, S.B. 2105, 88th Leg. (2023)).

processing precise, device-level location: latitude and longitude coordinates, GPS signals, device location histories, 'dwell time' at points of interest, and movement patterns over time — with another twelve disclosing conditional or dwelling-coordinate location data.

Precise geolocation deserves particular attention because it is uniquely revealing. A running record of a phone's location shows where a person sleeps, worships, seeks medical care, drops their children at school, and can be found at any given hour. The Federal Trade Commission has found that commercially sold location data can trace individuals to sensitive places, including health clinics, places of worship, and domestic violence shelters.²

These risks are not hypothetical, and they affect all of us, regardless of party, office, or badge. In June 2025, a gunman assassinated a state legislator and her husband and gravely wounded a second legislator and his wife; investigators recovered notebooks from his vehicle listing eleven people-search data broker websites alongside the names and home addresses of more than 45 public officials.³ This month, a national investigation documented at least 50 law enforcement officers charged with or accused of misusing automated license plate reader systems, most often to surveil women; in 26 cases, officers tracked wives, girlfriends, or former partners, and a sergeant in Pasadena, Texas resigned amid an investigation into using the cameras to “track and stalk a female officer.”⁴ Domestic violence advocates have warned for years that abusers use exactly these people-search and location products to find survivors who have fled.

Older Texans are targeted through this market as well. Epsilon Data Management, a data broker headquartered in Irving, Texas, admitted in a federal deferred prosecution agreement that it sold data on more than 30 million consumers to perpetrators of elder fraud schemes, paying \$150 million in penalties and victim compensation; two of its executives were sentenced last year. Brokers in these schemes compiled and refined marketing lists of consumers profiled as easy marks, including elderly Americans and people with Alzheimer's disease, lists known in the industry as “sucker lists.”⁵

The State's own review points in the same direction. The Department of Information Resources' (DIR) December 2024 implementation report recorded 660 complaints to the Attorney General alleging violations of the TDPSA in just the first four and a half months of enforcement, a higher

² [Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations](#) (Aug. 29, 2022); see also [Press Release, Fed. Trade Comm'n, FTC to Ban Kochava and Subsidiary from Selling Sensitive Location Data](#) (May 2026).

³ [Affidavit in support of federal criminal complaint, United States v. Boelter](#) (D. Minn., filed June 2025); see [Alleged shooter found Minnesota lawmakers' addresses online, court docs say, Politico](#) (June 16, 2025).

⁴ [How Rogue Officers Turned a Nationwide Camera Network Into a Tool for Stalking, Wash. Post](#) (Aug. 2, 2026), at least 50 officers charged with or accused of misuse; 26 cases involving wives, girlfriends, or former partners); [Pasadena police sergeant resigns while under internal investigation; council member cites alleged misuse of Flock camera, KPRC 2 Houston](#) (July 10, 2026)

⁵ [Deferred Prosecution Agreement, United States v. Epsilon Data Management LLC](#) (D. Colo. Jan. 2021); [U.S. Dep't of Justice, Marketing Company Agrees to Pay \\$150 Million for Facilitating Elder Fraud Schemes](#) (Jan. 27, 2021); [U.S. Dep't of Justice, sentencing release](#) (Feb. 2025); see also [analyses of broker lists profiling vulnerable consumers, including individuals with Alzheimer's disease](#) (Nov. 2022).

volume than comparable states. The Attorney General had 29 investigations open by the time the report was published. The consumer feedback DIR gathered supports two topline recommendations from the report: provide better education to Texans about their privacy rights and how to access them and streamline the opt-out process to make it easier for people to exercise that important right.⁶ Our field research tested those same issues. The recommendations we offer are grounded in the research results. They provide policy solutions to address barriers identified both in our study and in the DIR report.

II. Our Research: Testing the TDPSA in the Field

Beyond the registry analysis described above, our findings draw primarily on a structured field study we began in June 2026. Sixteen trained participants from Texas exercised their own TDPSA rights, submitting data access requests to seven registered data brokers and three data controllers (including Flock Safety, which operates automated license plate readers across Texas). Participants filed standardized reports on the process, nearly 160 to date, covering both the experience requesting their data and the outcome of each request. Notably, two of the brokers studied, Outlogic and Venntel, are already subject to Federal Trade Commission orders restricting the sale of sensitive location data due to unlawful practices.⁷

These findings are preliminary: response windows remain open and reports are still arriving. But the patterns are already clear and consistent.

III. Preliminary Findings

1. Texas data privacy rights are hard to access. Nearly half of submission reports (47%) rated the privacy-rights information on a company's site as difficult or impossible to locate. In 52% of reports, participants could identify only one method of submitting a request despite state law requiring two methods of submitting a request. In 67%, the company's privacy notice did not clearly explain Texas consumer rights. Participants repeatedly found other states' and even European rights described while Texas went unmentioned. And roughly two-thirds of the reports related to data broker-sites found no conspicuous notice identifying the company as a Texas data broker, as Texas law requires.

2. Identity verification is operating as a barrier. Several location brokers condition data requests on information ordinary Texans cannot reasonably produce: mobile advertising IDs, IP addresses, even lists of recently visited locations. One broker refused a participant's typed advertising ID and demanded a screenshot of her phone instead. Another required downloading its app, which itself demands more data and tracking, before a request could be made; a third required creating an account. Eight percent of attempted submissions failed entirely. Among reports describing obstacles, one in four described sequential verification steps that appeared designed to discourage completion,

⁶ [Report on the Implementation of the Texas Data Privacy and Security Act, Tex. Dep't of Info. Res.](#) (Dec. 2024).

⁷ [FTC final orders prohibiting the sale of sensitive location data: In re X-Mode Social/Outlogic](#) (final order Apr. 2024); [In re Gravy Analytics & Venntel](#) (final order Jan. 2025); see also [In re InMarket Media](#) (2024).

and one in four outcome reports rated the verification demanded as more invasive than the data warranted.

3. Most requests do not produce data. Of requests that reached a conclusion, only 31% produced a data report. Thirty percent were denied outright, 19% returned “no data on you,” and the rest received no response or were blocked mid-process. Flock Safety denied nine of ten concluded requests on the ground that it is merely a “processor” for its government customers, and redirected the tenth participant to ask those government customers directly. For license-plate location data collected on public streets, no Texan in our study obtained any data. Where requests were denied, half of the denials arrived without appeal instructions, and only one company gave the participant a way to submit a complaint to the Attorney General, which the TDPSA requires when an appeal is denied.

4. What comes back shows the core problem: detailed, invasive, error-ridden files, sold onward to buyers Texans cannot see. Fifteen of the seventeen data reports received contained location information. Nine of seventeen contained identifiers the participant never provided such as unfamiliar email addresses, unexplained codes linking records across sources, and in one case between 21 and 100 device identifiers, none of which the participant could verify as her own. Participants found wrong addresses, misspelled family members, and inaccurate lifestyle inferences. Most importantly, no report identified who actually purchased the participant's data: eight of seventeen did not address the question, and six named only vague categories of recipients. Texans cannot see, and brokers do not disclose, where their data ultimately goes.

The preliminary analysis has bright spots: companies that responded to data requests did so within 45 days and without charging fees. The failures we documented are concentrated where they matter most: findability, with study participants struggling to access their privacy rights; cumbersome verification requirements; and denials. And when data is produced, it is full of invasive information. The most consistent category included in the reports was location data, present in fifteen of seventeen reports received. This finding points to a concerning conclusion: we are all being tracked through our data.

IV. Recommendations

An optimal solution for streamlining data privacy rights is to establish a one stop shop system where Texans can go to exercise their rights. With over 419 data brokers registered with the Texas Secretary of State as of August 2026 and an unknown, but vast number of data controllers, it is impossible for an individual to effectively navigate the business by business data privacy process. In addition, because the law is not specific about what happens if new data is received after a delete or opt out request, it could mean that people who want to protect their privacy rights have to engage with this daunting system multiple times per year.

Short of a centralized system where Texans can access their privacy rights, there are small improvements that can be made to Texas law that would offer substantial benefits. These recommended changes would make progress towards addressing key problems identified both in our research and in the Texas Department of Information Resources 2024 study of the Texas data privacy law.⁸

Recommendation 1: Prohibit the sale of Texans' precise geolocation data. A running record of where a person sleeps, worships, seeks medical care, or takes their children is among the most sensitive information that exists, and, as the Background above shows, it is already being used to stalk, defraud, and kill. A growing number of states now ban the sale of precise geolocation data outright, and the FTC has ordered individual brokers, including two we studied, to stop selling sensitive location data.⁹ Texas already extends heightened protection to biometric identifiers under state law;¹⁰ a person's continuous location history is at least as sensitive as a fingerprint, and it deserves at least the same treatment. We recommend amending the TDPSA to prohibit the sale of precise geolocation data.

Recommendation 2: Align Texas universal opt out language with that in other states and require web browsers to offer a universal opt-out setting. TDPSA requires businesses to honor universal opt-out signals, a one-time browser setting that tells every website not to collect or sell the user's data.¹¹ But the right is hollow for most Texans, because the dominant browsers do not offer the setting natively. Today it is activated by default only in privacy-focused browsers such as Brave and DuckDuckGo, with Firefox offering it as an option to turn on in settings. Other jurisdictions have closed this gap by requiring all browsers to include an easy-to-find opt-out preference signal setting by January 1, 2027.¹² In addition, Texas law includes unnecessary carveouts that weaken this important protection.¹³ A Texas browser statute would be genuinely low-burden, because browser developers are already building this functionality, and it should:

⁸ [Report on the Implementation of the Texas Data Privacy and Security Act, Tex. Dep't of Info. Res.](#) (Dec. 2024), (recording 660 consumer privacy complaints in the first four and a half months of enforcement and 29 open investigations).

⁹ [Md. Code Com. Law § 14-4601 et seq.](#) (Maryland Online Data Privacy Act, effective Oct. 1, 2025) (sale of sensitive data, including precise geolocation, prohibited outright); [Or. Rev. Stat. ch. 646A](#) (Oregon Consumer Privacy Act); [Virginia Consumer Data Protection Act amendments](#) (2026) (third state to ban the sale of precise geolocation data).

¹⁰ [Tex. Bus. & Com. Code ch. 503](#) (Capture or Use of Biometric Identifier Act). The Attorney General's enforcement under Texas biometric and consumer-protection law has produced the largest state privacy recoveries in the nation, [\\$1.4B for Meta](#) and [\\$1.375B for Google](#).

¹¹ [Tex. Bus. & Com. Code § 541.055\(e\)](#) (recognition of universal opt-out mechanisms, effective Jan. 1, 2025).

¹² Cal. Civ. Code § 1798.136, added by [A.B. 566, 2025–2026 Reg. Sess.](#) (Cal. 2025) (the "Opt Me Out Act," approved Oct. 8, 2025; operative Jan. 1, 2027) (requiring any business that develops or maintains a browser to include an easy-to-locate setting enabling the consumer to send an opt-out preference signal, and providing a safe harbor for browser developers where a business fails to honor the signal). The underlying technical standard, the [Global Privacy Control specification](#), already ships in several browsers today.

¹³ See [Report on the Implementation of the Texas Data Privacy and Security Act, Texas Department of Information Resources](#) (2024), at 9. According to the report, exceptions in [Sections 541.055\(e\)\(3\) and \(3\)\(4\)](#) are not included in other state privacy laws.

- apply to all browsers offered to Texans, expressly including the new generation of AI-powered browsers and agents (e.g., ChatGPT Atlas, Perplexity Comet, and AI assistants embedded in mainstream browsers), which browse and transact on users' behalf;
- require the setting to be easy for a reasonable person to locate and configure; and
- include a safe harbor for browser developers when a business fails to honor the signal.

Recommendation 3: Establish clear standards for delete and opt out requests to ensure that they capture already collected and future data and do not just apply to one point in time. Under current law, it is unclear if delete and opt out requests are enduring or simply capture the point in time of the request. As a result, data brokers and controllers could comply with an opt out request or delete request in the moment and then continue to sell and maintain individual data that is received after the date of the request. In addition, delete and opt out rights should not require onerous identification or obscure information to access. Texans would benefit by clarifying that the requests are permanent unless the individual decides to opt back into collection and sale of their data.

Our field study demonstrates why rights that rely on individual requests will always under-protect: even trained, diligent participants were turned away by verification walls, denied without explanation, and left not knowing who bought their data. In addition to the three priority recommendations, there are changes around the edges that could be made to tighten the request pipeline.

In addition to ongoing enforcement of existing law, the Legislature could: bar verification demands consumers cannot reasonably meet, such as advertising IDs, device screenshots, or forced account and app sign-ups; require every denial to include the reason, appeal instructions, and the Attorney General complaint route; require responses to name the third parties to which a consumer's data was sold;¹⁴ and clarify that surveillance operators cannot use the controller-processor distinction to leave no one obligated to respond.

But these fixes are secondary. The deeper repairs are captured in recommendations 1, 2, and 3. These recommendations provide for essential protections that work by default, without Texans having to fight for them.

V. Conclusion

The TDPSA gave Texans real data privacy rights, but those rights remain out of reach for most people. When Texans try to access their rights, they often find systems that are hard to find and navigate, verification walls that turn people away, denials with no path forward, and a market in their precise location data that individual requests and opt-outs cannot realistically stop.

¹⁴ [Cf. S.B. 361, 2025–2026 Reg. Sess.](#) (Cal. 2025) (approved Oct. 8, 2025) (expanding the disclosures data brokers must make through the state's data broker registry, including whether they collect and sell specified categories of personal information). [Tex. Bus. & Com. Code ch. 510](#) already requires registered data brokers to disclose the categories of data they process and transfer; requiring access responses to identify actual recipients builds on that existing registry framework.

Each of the recommendations above builds directly on existing Texas law. They are a low burden on data brokers and controllers, while offering Texans essential and easy-to-access privacy options.

We welcome the opportunity to share our final study results with the Committee this fall.