



Testimony

House Bill 4

Testimony Before the Texas Senate State Affairs Committee

Dear Chair Hughes, Vice Chair Paxton, and Committee Members,

I am David Dunmoyer, campaign director for Better Tech for Tomorrow at the Texas Public Policy Foundation. I am testifying in support of HB 4.

The Foundation is grateful for your leadership to provide comprehensive data privacy protections and ensure Texans' personal information is more secure. Data privacy reform is the single most important technology issue for Better Tech for Tomorrow, as it will establish guardrails to promote responsible innovation while protecting personal data and recognizing it as property of the individual.

In September 2022, the Foundation published a comprehensive [research paper](#) outlining the dangers Texans face without having a comprehensive data privacy and security law, as well as policy recommendations to put Texans in the driver's seat with their personal information. To understand the need for reforms such as House Bill 4, it is important to start with the problem first.

The Problem

In the digital age, we are all spending more time online using digital devices, in turn creating increasing amounts of data. Coinciding with this increase has been a marked advancement in technologies that both harvest and commodify consumer information. Consumer data was once primarily obtained by asking users for basic information—such as their age, location, relationship status, etc. Now, the more common and less visible means of data collection is through the use of cookies. By giving tracking software to other companies that embed it into their app or website, businesses are now able to track virtually our every step, even though it is not clear to customers. And while some argue there is no problem because of the terms of service that users accept, the terms and conditions are [often crafted](#) in an opaque manner that nudges consumers toward selecting options that extract and track the largest amount of data. [In addition](#), 91% of U.S. consumers do not read the terms of service before consenting, with an even higher rate of 97% for users ages 18–34. In turn, companies have an [alarming amount](#) of Texans' data. Examples of data collected include sent and received emails; social media posts, comments, and engagement; time spent viewing content; purchasing habits; search history; personal appearance; voice; facial movements; photos stored on your phone; physical location; personally identifiable information (or PII) such as driver's license numbers, social security numbers, phone numbers, and your address; and even more granular data like [heart rate](#), gait, breathing patterns, and body temperature. This is not an exhaustive list, but it illustrates that most things we do online can be monetized.

New means of user data extraction have also meant new, lucrative opportunities to use that personal information. We are now in the era of “big data,” which is [defined as](#) “large, diverse sets of information that grow at ever-increasing rates.” Because of the push to obtain more user data for service personalization and “data-driven solutions,” individual privacy has been deemed of secondary importance. According to philosopher and computer scientist Kieron O'Hara, “In order to be helpful to an individual, a system based on big data must be one of total surveillance” (O'Hara, 2020, p. 23). Consequently, data privacy has taken a backseat as new, increasingly invasive and accurate means of dissecting our minds and lives have rolled out.

Finally, there is the reality of how that data is used. While many companies rightly suggest that personal information is used to better tailor services to individual users, this is only one of many uses. Initially, large companies [monetize user information by](#) (1) building individual profiles based on their data and then letting advertisers target people based on their data and (2) sharing data with advertisers directly and then opening it up for bids on ads.

Then there are data brokers, the third-party companies that exist to collect personal information, bundle it together, and sell it to third-party buyers. They obtain tremendous amounts of user data that then allows users to be sorted into neatly organized categories—ranging from innocuous categories like fans of baseball to harrowing lists such as victims of rape—to then sell to the highest bidding third party. Lastly, much of this data remains in storage that can prove a severe security risk for consumers. [In 2021 alone](#), more than 4,000 data breaches exposed more than 22 billion records. And much of this could have been prevented through improved security safeguards, as [82% of data breaches](#) in 2021 were attributed to human error.

As noted by the [Texas Privacy Protection Advisory Council](#)—a group assembled following the passage of HB 4390 in the 86th Legislature to study data privacy laws in Texas and around the world—the status quo in Texas is insufficient:

- Texans generally have little knowledge of how their personal information is used, even with current safeguards such as privacy notices;
- Texans are rarely given the choice to consent to data collection. Rarely are consumers afforded accessible means of opting out of data collection, and there are many situations where the consent is implicit for organizations to share personal information;
- Texans rarely have the ability to view personal information collected about them. In the instances where this personal information can be viewed, it is rare that consumers are able to review and correct (potentially erroneous) information;
- Existing protections do not go far enough to safeguard sensitive personal information collection practices; and
- Bad actors continue to use deceptive means of collecting personal information, and then may use information for reasons that have not been conveyed to users.

House Bill 4

House Bill 4 introduces comprehensive data privacy and security reforms that would benefit all Texans by addressing the core problems outlined above. Broadly, House Bill 4 would empower Texans to have more control over their data while enhancing safeguards to sensitive personal information. The bill would accomplish this in several ways.

First, when it comes to data privacy legislation, it is of particular importance that the definitions included in the bill are strong, clear, and broad enough to capture the universe of digital activity and data. The definitions included in this bill do just that, ensuring that HB 4 is not at odds with existing federal law that preempts state authority; defining key terms such as “personal data” and “sale of personal data” in a way that provides strong protections for consumers without being unnecessarily onerous on industry; and including key definitional terms to capture new and emerging methods of data collection.

Second, the bill includes strong “digital rights” for Texans to exercise, empowering them to have ownership and control of their data. House Bill 4 affords Texans the following rights:

- The right to know what information is being collected;
- The right to correct inaccurate information;

- The right to delete certain personal data;
- The right to access and obtain an accessible copy of personal data;
- The right to opt out of the processing of personal data used for targeted advertising, the sale of personal data, or profiling; and
- The right to not be discriminated against for exercising one's digital rights.

Texans would be empowered to exercise these rights at any time by submitting a request directly to the controller. Further, for the processing of data belonging to a child, the child's parent or legal guardian is entitled to exercise these rights on the child's behalf. This would put Texans back in control of their personal information.

Third, House Bill 4 takes the important step of cutting back on excessive and unnecessary data collection. By limiting the amount of data that companies can collect on users to what is necessary, the bill immediately enhances consumer privacy even before they exercise their digital rights, and it reduces cybersecurity risks.

Fourth, House Bill 4 creates a framework for better cybersecurity hygiene of personal information. Specifically, this bill addresses concerns raised earlier by requiring data controllers to implement physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

Finally, House Bill 4 provides for strong and clear enforcement through the Office of the Attorney General. It lays out duties for data controllers, the process for complying with consumer requests, a consumer complaint process, investigative authority, a notice and cure period, and a potential civil penalty of up to \$7,500 per violation. Together, this will encourage compliance by data controllers and participation by Texas consumers.

Again, we are grateful for your consideration of House Bill 4 today. The Foundation strongly supports House Bill 4, as it protects the digital and physical safety of Texans, while affording Texans the civil liberty of online privacy. While technology moves faster than policy, this bill would establish strong and much-needed guardrails so industry and consumers alike understand the rules and rights they are entitled to.

Sincerely,

David Dunmoyer, Campaign Director
ddunmoyer@texaspolicy.com

The Honorable Zach Whiting, Policy Director and Senior Fellow
zwhiting@texaspolicy.com

About Texas Public Policy Foundation

The Texas Public Policy Foundation is a 501(c)3 non-profit, non-partisan research institute. The Foundation promotes and defends liberty, personal responsibility, and free enterprise in Texas and the nation by educating and affecting policymakers and the Texas public policy debate with academically sound research and outreach.

Funded by thousands of individuals, foundations, and corporations, the Foundation does not accept government funds or contributions to influence the outcomes of its research.

The public is demanding a different direction for their government, and the Texas Public Policy Foundation is providing the ideas that enable policymakers to chart that new course.

