Texas' Digital Bill of Rights

September 2022

The Issue

Over the last decade, data collection, sale, and distribution practices have become more commonplace, lucrative, and precise. User information is increasingly commodified with little to no user consent, control, or privacy. Despite the purported benefits, more than 80% of the public nationwide says that the risks of data collection practices outweigh the benefits.

According to the Texas Privacy Protection Advisory Council, there are several problems:

- 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;
- 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.

The council's findings stem from the current data collection and sale model and a lack of data privacy protections for Texans. Currently, many companies receive user data either by users inputting data directly—such as their birthday, location, likes and dislikes—and by employing cookies to track users while they are browsing other websites. And even those who choose to deactivate their Facebook account, for example, are still tracked by the company. Some of this data is used to provide tailored services, but many additional applications exist.

Another application is the data brokerage model. Data brokers collect personal information, bundle it together, and sell to third-party buyers. They cunningly employ data scrubbing tactics to scour through personal information users provide while using services like social media, search engines, news sites, apps, and more, and work with major companies to buy user data. By tracking users online and offline, these data brokers assemble incredibly thorough data profiles on individuals, whereupon users are sorted into neatly organized categories that are packaged and sold to third parties. This data has been sold to governments, nefarious actors/criminals, and predatory advertisers, among others—any interested buyer is eligible. The amount of information data brokers have access to is stunning, and Texans have virtually no way of knowing what personal data is being collected, who has access to it, and no say in whether a business can sell their data.

Data has also been used for purely criminal purposes—hacking, cyber extortion, identity theft, and other means of illegally obtaining or using personal information. As data breaches have become more prominent—4,000 data breaches exposed more than 22 billion records in 2021 alone—users sense the risk and want more control over what data is held by companies and for companies to take cyber hygiene more seriously.

continued

The Facts

- Some examples of the types 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 in 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 temperature.
- According to a poll conducted by WPA intelligence on August 1, 2022, 90% of likely voters in Texas agree that users should have to grant permission for businesses to be able to collect data or share data with third parties.
- The data brokerage industry rakes in more than $200 billion in revenue annually and continues to grow.
- Five states (California, Virginia, Colorado, Connecticut, and Utah) have passed a digital bill of rights to give users more agency, control, and transparency over their private data.

Policy Recommendation

- Pass the nation's most comprehensive digital bill of rights that affords Texans:
  - The right to know what data is being collected.
  - The right to have inaccurate information corrected.
  - The right to delete any personal information.
  - The right to data portability.
- Also worth exploring is the right to not be discriminated against for exercising these rights.
- A Texas digital bill of rights should address data security concerns as well. This bill could allow for enforcement by the attorney general or a private right of action that allows individual plaintiffs or a class to seek statutory damages in instances where security breaches impact sensitive categories of personal information, which are caused by the failure of a business to incorporate appropriate security measures.

Resources

Dunmoyer, D., & Whiting, Z. (2022). *Why Texas needs a digital bill of rights.* Texas Public Policy Foundation. https://www.texaspolicy.com/why-texas-needs-a-digital-bill-of-rights/

Security Made Simple. (2022, February 1). *What does a data broker do?* https://www.securitymadesimple.org/cybersecurity-blog/what-does-a-data-broker-do

Texas Privacy Protection Advisory Council. (2020, September). *Report*. https://www.house.texas.gov/_media/pdf/committees/Texas-Privacy-Protection-Advisory-Council-Report.pdf