Texas
APPLESEED

TEXAS AT THE CROSSROADS

Protecting Privacy and Civil Rights

April 2021

TABLE OF CONTENTS

Executive Summary

The absence of a robust, uniform approach to data privacy in the US is highlighted by news stories and first-hand accounts detailing the fallout of the collection, use, and sale of a wide range of personal data. The use of this personal data is always intrusive and often discriminatory, resulting in a host of inequities and abuses based on factors such as race, gender, sexual orientation, demographics and biometrics, political opinions, health status, geolocation, browsing habits, social networks, tagged photos, and a multitude of other indicia.

The situation in Texas mirrors that of the US as a whole.

Increasing access to and use of technology for communications and commerce is fueling debates as to a proper course of action: stem the tide or watch as the tsunami erodes the privacy and civil rights so fundamental to our democratic underpinning. While this struggle at the intersection of privacy and civil rights is not new, recent events have laid bare the egregious exploitation of personal data.

While the US has a smattering of lackluster and generally unenforced privacy statutes, some states, including Texas, are considering or taking steps to protect the personal information of their citizens. In the 2019 legislative session, the Texas Legislature established the Texas Privacy Protection Advisory Council to study data privacy laws in Texas, other states, and relevant foreign jurisdictions. The Council issued a report in September 2020, with general recommendations for future proposed privacy legislation. In the 2021 session, bills have been introduced to protect personal data held by public and private entities.

How does the lack of privacy protection impact Texans?

Data collected by companies is used to influence consumer behavior, control access to opportunities, and impose financial burdens on all of us – including those most vulnerable to this digital sleight of hand. Real-time bidding in advertising, predatory loan pricing, resume-sorting, and facial recognition are just some of the ways your data can be used against you.

What's wrong with existing laws? They are widely recognized as obsolete and seldom enforced.

How can Texas do its part to remedy the situation? We recommend a three-pronged approach: legislation, rulemaking, and enforcement. First, pass a state privacy bill that clearly defines rights for consumers as well as requirements for businesses, embedding civil rights protection directly into the bill. Second, bring citizens, companies, and the state to the table to develop effective regulations. Third, demand vigorous enforcement.

Texas can and should implement meaningful privacy protections.

SB 16 prohibits the disclosure of personal data by the state of Texas. HB 3741 gives Texas residents the right to know, access, and delete their personal information, as well as the right to correct inaccurate information. While each of these measures could be improved, the basic principles of ensuring data control and privacy for Texans are important.

HB 3741 is a step in the right direction, requiring companies to specify — before any information is gathered — what data is collected, how the data is processed, and who has access to the data. We do recommend three additions:

- Allow consumers to opt out of the sale of their data to third parties,
- Forbid companies from retaliatory measures when citizens exercise their privacy rights, and
- Include a strong statement that protected class variables not be used to discriminate against Texans.

As the Texas Privacy Protection Advisory Council declared last year, "Texans have the right to know how their personal information is being used and the Legislature should consider ways to strengthen that right." It is time for the legislature to prioritize privacy and civil rights.

Introduction

Aliyah and Amy were roommates in college. After graduation, they both moved to Dallas and started their careers. With work and their new lives, they drifted apart but kept up on Facebook. A few years later, both wanted to buy a home. Aliyah, who is Black, got together with Amy, who is white, for lunch to talk about their house hunting experiences. As they talked, Aliyah said all the online ads she sees are for homes in predominantly African American neighborhoods. Amy was surprised and said she sees online ads for a wide range of neighborhoods. They wondered why.

The reason is fairly simple. Facebook "collects millions of data points about its users, draws inferences about each user based on this data, and then charges advertisers for the ability to micro-target ads to users based on [Facebook's] inferences about them."[1] The Department of Housing and Urban Development brought a suit against Facebook for violating the Fair Housing Act, specifically for targeting users based on their personal characteristics, including race, religion, sex, familial status, national origin, or disability.

Two questions come to mind. How can Facebook gather such detailed personal data? Why is Facebook allowed to offer discriminatory advertising?

The intersection of privacy and civil rights

"Texas does not have a privacy law that applies to private companies and specifically addresses online privacy," according to Bart Huffman, University of Texas at Austin law professor.[2] And at the federal level, the US does not have a comprehensive privacy law that governs the collection, use, and sale of consumer information. Laws exist for specific sectors, such as financial and healthcare data, as well as protecting children online. But Daniel Solove and Paul Schwartz, law professors at George Washington University Law School and University of California, Berkeley, respectively, describe US privacy statutes as a "fragmented, inconsistent patchwork of laws."[3]

Beyond privacy concerns, your own personal data might be used against you, as the Facebook discrimination lawsuit shows. Agencies protecting privacy rarely consider protecting civil rights. Agencies protecting civil rights rarely consider protecting privacy. Consumer privacy advocates recommend directly connecting privacy protection with civil rights protection.[4]

> ***At its core, privacy is "controlling how personal information is used and ensuring that this information is not used against the interests of individuals.[4]***
>
> Cameron F. Kerry, Distinguished Visiting Fellow - Governance Studies, Center for Technology Innovation, Brookings

Some states, including Texas, have started to show an interest in protecting the personal information of its citizens. In the 2019 session, the state legislature set up the Texas Privacy Protection Advisory Council to study data privacy laws in Texas, other states, and relevant foreign jurisdictions. The Council issued a report in September 2020, with general recommendations for future proposed privacy legislation.[5] In the 2021 session, bills have been introduced to protect personal data held by public and private entities; these will be discussed later.

California was the first state to enact a comprehensive data privacy law, the California Consumer Privacy Act (CCPA), in 2018,[6] with further changes in 2020.[7] These reforms address two key principles regarding data privacy: the "right to know" and the "right to say no." That is, consumers should know what personal data companies collect and should be able to say no to the sale of their data.

[1] HUD Charges Facebook With Housing Discrimination Over Company's Targeted Advertising Practices, from the U.S. Department of Housing and Urban Development (HUD) March 28, 2019 press release.
[2] Texas - Data Protection Overview. Huffman, Bart et. al. (Reed Smith LLP UK), published by OneTrust DataGuidance (June 2020).
[3] ALI Data Privacy: Overview and Black Letter Text (January 24, 2020). UCLA Law Review, Vol. 68, 2020, available at: https://ssrn.com/abstract=3457563 or http://dx.doi.org/10.2139/ssrn.3457563.
[4] Bridging the Gaps: A path forward to federal privacy legislation. Kerry, Cameron et. al., published by the Brookings Institution (June 2020).
[5] Texas Privacy Protection Advisory Council Issues Interim Report. Stauss, David, published by Husch Blackwell LLP (September 13, 2020).
[6] "California's Privacy Law Goes Into Effect Today. Now What?" Edelman, Gilad, published in WIRED (January 1, 2020).
[7] The California Privacy Rights Act of 2020, provisions in an HTML form by the International Association of Privacy Professionals (IAPP).

How does the lack of privacy protection impact Texans?

Companies use all the data they collect to influence behavior, encouraging people to buy something or do something. Although legal, this activity can violate a fundamental human right: privacy.[8] Currently, Texans have minimal control over what data is collected about them online or how that data is used. Moreover, such uses of personal data can be discriminatory,[9] resulting in loss of job opportunities based on gender, higher insurance rates based on sexual orientation or gender identity, or higher loan rates based on certain residential zip codes.

During COVID, far fewer than 10% of Americans downloaded a contact tracing app. The University of Michigan found that, "*concern about privacy is one of the things that's suppressing adoption.*"

Christian Sandvig, Dir., Center for Ethics, Society, and Computing
Time, November 10, 2020

Many online business decisions — who sees a particular job posting, who receives a better insurance rate, or who is offered a higher-cost loan — are made by algorithms. Think of algorithms as a recipe; a set of rules to be followed to solve a problem. While algorithms may sound objective, they can be biased. In its 2016 report on Big Data, the Federal Trade Commission (FTC) suggested that unchecked data processing and algorithmic decision making can amplify discrimination based on protected characteristics such as race, gender, and sexual orientation.[10] Not much has changed since that report.

Below are few examples of how civil rights might be violated because of weak privacy regulations.

Real Time Bidding in Advertising Can Push Some Towards Inferior or Over-Priced Products

Type "car parts" into Google. Several of the first few search results will be ads, delivered based on algorithmic decisions. The algorithm decides, based on each person's digital dossier — demographic and biometric information, including age, gender, race, location, and more — if a person fits the desired target audience at a reasonable cost to an advertiser. Then, the system presents a targeted ad. Advertisers call this "real time bidding." In Europe, which has stronger privacy laws than the US, Google has been fined for "illegally collecting and bartering in special category data" which can include a person's race, sexuality, health status or political opinions.[11] This same bidding process happens here, but it is currently legal in the US.

> ***Under data protection law [in Europe], using people's sensitive personal data to serve adverts requires their explicit consent, which is not happening right now.[11]***
>
> Simon McDougall, Ex. Dir., Tech. and Innov.,
> Information Commissioner's Office

Fintech Lending Utilizing Alternative Data May Lead to Racial Biases in Loan Pricing

Did a friend default on a loan? It might hurt your own chances of receiving a loan. Fintech lenders — financial technology firms offering loans online — have transformed financial services over the last ten years. They collect a wide variety of data on potential borrowers, including "alternative data" like social network connections, exchanged messages, tagged photos, browsing habits, searches, and geolocation data from mobile phones.[12] Then, algorithms use those factors to estimate creditworthiness.

> ***Machine learning algorithms that sift through vast amounts of data could unearth variables that predict the consumer's likelihood of default (or other relevant outcomes), but are also highly correlated with race, ethnicity, sex, or some other basis protected by law.***
>
> Consumer Financial Protection Bureau | "Alternative Data & Financial Access: The Good, the Bad, and the Ugly"

[8] "Privacy is a Human Right – It Can't Be Bought or Sold - Consumer Federation of America." Grant, Susan (CFA Director of Consumer Protection and Privacy), published by the Consumer Federation of America (CFA) (December 17, 2019).
[9] "COMPREHENSIVE FEDERAL PRIVACY LEGISLATION: Discriminatory Data Practices." Published by the Center for Democracy & Technology (January 30, 2019).
[10] "Big Data: A tool for inclusion or exclusion? Understanding the issues." Published by the Federal Trade Commission (January 2016).
[11] "Adtech industry operating illegally, rules UK regulator." Murgia, Madhumita, published by the Financial Times (June 20, 2019).
[12] "Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process." A notice published by the Federal Register (February 2, 2017).

On the one hand, considering alternative data may expand low-cost lending to borrowers with limited credit histories. On the other, lax standards for data collection and usage may enable predatory lending practices, leading to over-charging of desperate borrowers or borrowers residing in particular zip codes. These black box algorithms make it nearly impossible for individuals to control how personal data is used or to understand necessary steps to access credit at a lower cost. The algorithms also could conceal practices that have discriminatory effects.

> ***Critics of AI acknowledged it could be exceedingly difficult to sue an employer over automated hiring: Job candidates might never know it was being used.*** [13]
>
> Rachel Goodman, ACLU

Rejections by Algorithm Can Perpetuate Pre-existing Biases and Systemic Discrimination

Amazon receives hundreds of resumes every month from engineers, but only hires a few. How do they cull through these resumes efficiently to identify the best ones to hire? They hit upon the idea of using data from existing employees to "train" an artificial intelligence (AI) system.[13] Resumes contain information such as the university attended, major, grade point average, and social activities, such as clubs and sports. Employees also had performance ratings from the company on a scale of 1 to 5 indicating how successful they had been with Amazon. The new AI system identified resume characteristics related to employees who earned higher performance ratings. Resumes of new applicants were run through the system and assigned an estimated rating on a scale of 1 to 5. The system was appealing because it saved time for the human resources department and seemed, on its face, to be objective. But, Amazon noticed a problem. Since the pool of existing employees was predominantly male, the applicants receiving top ratings by the algorithm were men. The system rarely rated female applicants highly because they attended different schools and participated in different social activities compared to the stars in the original employee data set. Instead of creating an objective standard, the system perpetuated the lack of diversity among current employees by exhibiting bias against women. Amazon dropped the system, but nothing stops other companies from using similar algorithms.

Facial Recognition Software Can Be Spotty in Its Spotting

> ***It forces you to violate their privacy (by not asking for consent)… to build something that likely will function in ways you can't even predict. That's really the nature of where we're at.***
>
> Deborah Raji, MIT Technology Review
> This is how we lost control of our faces | MIT Technology Review

Joy walked up to the facial scanner at her new employer's entrance. She smiled and waited for the door to unlock once it recognized her, a young Black woman. But it didn't work. What happened? Facial analysis programs tend to be accurate, with less than a 1% error rate when scanning white males. But the error rate can exceed 34% for Black women.[14] Facial recognition software "learns" by looking for patterns in huge training sets, thousands of pictures of faces versus other objects. In the case of her company, the training and testing were flawed and biased due to a small number of female faces and a small number of faces from different racial and ethnic backgrounds.

One US software company has amassed a database of over three billion images, mainly scraped from the internet. Law enforcement agencies buy access to the system to identify suspects.[15] Accuracy and biases have not been tested by an objective third party and there are few guardrails to protect privacy and civil liberties around facial recognition. The expanded use of these systems, in particular by law enforcement, could lead to misidentifying people who are not white and male, potentially furthering discrimination and racial profiling.

[13] "Amazon scraps secret AI recruiting tool that showed bias against women." Dastin, Jeffrey, published in Reuters (October 10, 2018).
[14] "Study finds gender and skin-type bias in commercial artificial-intelligence systems." Published by Massachusetts Institute of Technology's MIT News (February 11, 2018).
[15] "The Secretive Company That Might End Privacy as We Know It." Hill, Kashmir, published in The New York Times (Jan. 18, 2020, and updated March 18, 2021).

Why don't existing laws protect privacy and stop online discrimination?

Over twenty years ago, the US enacted federal laws that protect privacy in specific sectors. But that was long before the internet of today. For example:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires written authorization before a health care provider, health care clearinghouse, or health plan can use an individual's health information for marketing purposes.[16]
- The Gramm-Leach-Bliley Act of 1999 (GLBA) applies to sharing and disclosure of nonpublic personal information by financial institutions and entities that receive such information from financial institutions.[17]

And the "granddaddy" of them all, the Federal Trade Commission Act, was enacted in 1914.[18] Much of our privacy regulation rests on Section 5 of that Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[19] However, the FTC traditionally has limited its privacy enforcement actions to an entity's violation of its own written privacy policy.[20]

In a 2020 survey, the Internet Association, a lobbying group representing Google, Amazon, and Facebook, among others, found that 85% of consumers say they should have more control over the personal info they share online.

Internet Association Survey On Data Privacy

In the last decade, the US Government Accountability Office (GAO) conducted several studies related to information resellers, financial technology, internet privacy, and consumer data protection. These studies included analyses of relevant laws, regulations, and enforcement actions, with input from federal agencies, trade associations, consumer groups, privacy groups, and resellers.

- A 2013 report detailed the lack of a comprehensive federal privacy law for governing the collection and sale of personal information among private-sector companies, and exposed gaps in the federal privacy framework.[21]
- A 2015 report found that the federal privacy framework had not kept pace with technology advances, such as tracking and facial recognition.[22]
- Follow-up reports in 2019 found that the ability of the FTC to police internet privacy by addressing unfair and deceptive trade practices was insufficient, due at least in part to the lack of authority to levy penalties for privacy and data security violations.[23,24]

These studies led to GAO recommendations for Congress to shore up the consumer privacy framework to keep pace with market developments and to implement broad internet privacy legislation.[25] To date, Congress has done neither.

In 2019, a majority of state attorneys general echoed these concerns, urging the FTC to renew its focus on consumer privacy and antitrust enforcement against tech platforms that collect and leverage consumer data.[26]

[16] HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996. The Office of Assistant Secretary for Planning and Evaluation. (August 21, 1996).
[17] GRAMM–LEACH–BLILEY ACT. Public Law 106–102, 106th Congress (November 12, 1999).
[18] 15 U.S.C. CHAPTER 2, SUBCHAPTER I: FEDERAL TRADE COMMISSION.
[19] "Section 5 of the FTC Act: principles of navigation." Ohlhausen, Maureen K., published by the Journal of Antitrust Enforcement, (2013), pp. 1–24, doi:10.1093/jaenfo/jnt013 (October 18, 2013).
[20] "Consumer Privacy: Changes to Legal Framework Needed to Address Gaps." GAO-19-621T. Statement of Alicia Puente Cackley, Director Financial Markets and Community Investment, published by the U.S. Government Accountability Office (June 11, 2019).
[21] "Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace." GAO-13-663. Published by the U.S. Government Accountability Office (September 2013)
[22] "Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law." GAO-15-621. Published by the U.S. Government Accountability Office (July 2015).
[23] "Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility." GAO-19-52. Published by the U.S. Government Accountability Office (January 2019).
[24] "Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer." GAO-19-196. Published by the U.S. Government Accountability Office (February 2019).
[25] Consumer Privacy GAO-19-621T
[26] "Majority of US states interested in probe of Google, other tech giants." Swift, Mike, published by MLex News Hub (September 3, 2019).

"Information about how everyday people spend their lives and their money has become extremely valuable, especially when aggregated into large sets and analyzed and packaged for targeted marketing," Texas Attorney General Ken Paxton said. "But technology platforms often lack the incentive to provide strong privacy protections for consumers."[27]

There are, of course, several laws that prohibit discrimination based on race and other personal characteristics, including the Civil Rights Act, Fair Housing Act, and Voting Rights Act. But existing laws do not address the intersection of privacy and civil rights. Earlier we saw that HUD charged Facebook for using race in selecting which ads to show customers. Consumer advocates caught this discriminatory targeting, not HUD or FTC. In fact, the FTC has never issued a complaint about algorithmic bias,[28] though incoming Chair Rebecca Slaughter has asked her staff to "actively investigate biased and discriminatory algorithms."[29]

How can Texas do its part to remedy the situation?

We have three recommendations to remedy the lack of a strong privacy law that protects civil rights:

- **Legislation** — Pass a state privacy bill that defines consumer rights and corporate responsibilities, while addressing the intersection of privacy and civil rights
- **Rulemaking** — Involve the public, companies, and the state government in writing regulations based on this new privacy legislation
- **Enforcement** — Provide rigorous enforcement of the new privacy law, including the power to stop illegal activities and impose substantial penalties

Each of these recommendations is described in more detail below.

Legislation

Pass a state privacy bill that clearly defines both rights for consumers and requirements for businesses. Other states have stepped up to introduce comprehensive privacy bills.[30] The International Association of Privacy Professionals identified three basic consumer rights included in most state measures:[31]

- Right of access — consumers can see exactly what personal data a company is collecting about them and what data it is sharing with other companies
- Right to deletion — consumers can request that their data to be deleted in a timely manner, sometimes referred to as the "right to be forgotten"
- Right to opt out — consumers can stop the sale or disclosure of their personal data to third parties

Plus, two business requirements:

- Requirement to provide notice and transparency — companies must obtain consumer consent to gather data and be clear about how they will use that data
- Requirement not to restrict or deny consumers — companies must still provide service to consumers who exercise their privacy rights

Without downplaying differences between states and the need for additional provisions, this list shows that there is broad agreement on a number of basic points. The CCPA in California, as well as the bills in a dozen more states, include all five of these.

Write civil rights protections directly into the privacy bill. We suggest including language that cements the connection between privacy and civil rights, stopping data driven discrimination, such as:

[27] "AG Paxton Urges FTC to Consider the Role of Consumer Privacy and Data in Antitrust Enforcement." Press release by the Texas Office of the Attorney General (June 11, 2019).
[28] "Addressing Challenges at the Intersection of Civil Rights and Technology." Moy, Laura and Rejous, Gabrielle, published by the Day One Project (An initiative of the Federation of American Scientists).
[29] "Protecting Consumer Privacy in a Time of Crisis: *Remarks of Acting Chairwoman Rebecca Kelly Slaughter*." Federal Trade Commission (February 10, 2021).
[30] "Complete Guide to Privacy Laws in the US." Green, Andy, published by Varonis (April 2, 2021).
[31] "US State Comprehensive Privacy Law Comparison." Rippy, Sarah, published by the IAPP (March 22, 2021).

- A company shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability, in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: housing; employment; credit; education; or the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.[32]

A new Texas privacy law should directly address this intersection of privacy and civil rights, ensuring that online data will not be used in discriminatory ways.

Reconcile federal and state privacy laws. Assuming that both Congress and Texas pass privacy bills in the near future, how do we reconcile any differences between them? Consistent federal standards across the country would benefit industries and individuals, as long as the standards are strong. Ideally a federal law will serve as a baseline for the collection, processing, sharing, and security of personal information. We recommend that existing state laws such as those related to consumer protection laws, prohibiting unfair and deceptive practices, protecting civil rights, among others, remain in place. We will be on the watch for weak federal laws that preempt stronger state laws.

Rulemaking

Bring citizens, companies, and the state to the table to develop effective regulations. After Texas passes a strong privacy bill, clear regulations must be written to operationalize the law. California allowed a year for the AG's office to write privacy regulations.[33] There are complex, technical points to work through, such as "algorithmic accountability" — how to hold companies responsible for the decisions made by their algorithms. Regulators need to be able to assess information about variables or proxy variables that are included in models, how the equations are constructed and tested, and how a company should explain its algorithms to customers.[34] Rulemaking will need input from the public, companies, and enforcement stakeholders. And it will be an on-going process to update rules as technology and markets evolve.

Enforcement

Finally, after passing a strong privacy law and writing effective rules, demand vigorous enforcement. Once a law is adopted and rules are promulgated, the next step is robust enforcement, including stopping illegal practices and imposing meaningful penalties. GAO studies found that, even when laws are in place, they are hard to enforce without the authority to levy penalties.[35] In Texas, enforcement of privacy and civil rights fall under the state Attorney General.[36] Some states plan to establish a new enforcement entity. California's Privacy Protection Agency, for instance, will have the power and jurisdiction to implement and enforce privacy laws.[37] Whether executed by the attorney general or a new agency, enforcement is a key component of an effective privacy law.

Texas Can and Should Pass Meaningful Privacy Protections

Texas has reached a crossroads. Texans know that we have little control over the collection, use, and sale of our personal data. Companies exploit weak laws and regulations, at times even using our own data against us. Partly because of these weaknesses, few lawsuits have been brought based on existing laws. Someday, a comprehensive federal privacy law will pass. Until then, privacy protections fall to the states, and, like most states, Texas has not yet met the challenge.

During the current legislative session, however, bills have been introduced to address privacy issues. SB 16 prohibits the disclosure of personal data by the state of Texas, saying:

- A state agency may not disseminate to any person any personal data of an individual without the individual's written consent.[38]

This bill would protect Texans from disclosures by state agencies. Although Texans are concerned about how the state uses our data, they are also concerned about how businesses use our data.

---

[32] SECOND SUBSTITUTE SENATE BILL 5062, State of Washington, 67th Legislature 2021 Regular Session (February 17, 2021).
[33] "CCPA Regulations." The Office of the Attorney General of the State of California (August 14, 2020).
[34] "Using Artificial Intelligence and Algorithms" Smith, Andrew, Director of the Federal Trade Commission, published by the FTC (April 8, 2020).
[35] "INTERNET PRIVACY AND DATA SECURITY: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility." GAO-19-427T. Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate, published by the U.S. Government Accountability Office (March 7, 2019).
[36] HB 4390 Texas Legislature - 86(R) for example.
[37] "What is the California Privacy Protection Agency?" Torre, Lydia and Brown, Glenn, published by the IAPP (November 23, 2020).
[38] SB 16 - Texas Legislature - 87(R)

Another bill,[39] HB 3741, directly addresses these concerns by increasing requirements on the private sector. The bill provides for several of the consumer rights and business duties we outlined earlier, such as:

- Giving Texas residents the right to know, right to access, right to deletion, right to correct inaccurate information, and right to data portability.
- A company must tell consumers what items of information are gathered, how it is processed, why it is being processed, and what other parties may receive their data, all before gathering data.

Although this bill is a step in the right direction, we recommend two additions: allow consumers the right to opt out of the sale of their data to third parties and require companies not to restrict or deny service to consumers who exercise their privacy rights.

In a unique turn, HB 3741 defines "categories" of personally identifiable information.

- Category one — "civic and business" information such as social security number, driver's license number, financial account number, and biometric information.
- Category two — personal information such as constitutionally protected class data including race, religion, age, impairments, plus geolocation and genetic information.

Companies may collect and process both types of data but may not sell or transfer category two data. The second category echoes our admonition to enshrine civil rights directly into the privacy bill. We recommend adding a strong statement that protected class variables not be used to discriminate against consumers.

As the Texas Privacy Protection Advisory Council recommended last year, "Texans have the right to know how their personal information is being used and the Legislature should consider ways to strengthen that right." It is time for the legislature to take a stand to protect our privacy rights and our civil rights. These two bills are good starting points.

[39] HB 3741 - Texas Legislature - 87(R)

Report Authors:

Steve Perkins is former Associate Dean of Graduate Programs in the School of Management at the University of Texas at Dallas and a Certified Information Privacy Professional.

Ann Baddour is the director of the Fair Financial Services Project at Texas Appleseed.

About Texas Appleseed

Texas Appleseed is a public interest justice center that works to change unjust laws and policies that prevent Texans from realizing their full potential. Our nonprofit conducts data-driven research that uncovers inequity in laws and policies and identifies solutions for lasting, concrete change. For more information, visit www.TexasAppleseed.org.