Texas
APPLESEED

House Committee on Business & Industry

September 15, 2022

Interim Charge 6

Evaluate the overall state of data privacy and online consumer protections in Texas and study the related laws and legislative efforts of other states. Make recommendations to ensure consumer data protections and online privacy.

Introduction

Chair Turner, Vice Chair Hefner, and committee members - thank you for this opportunity to offer written testimony to the House Business & Industry Committee regarding the overall state of data privacy and online consumer protections in Texas.

My name is Briana Gordley, and I am a policy analyst with the Fair Financial Services Project at Texas Appleseed, a nonprofit that works to change unjust laws and policies that prevent Texans from realizing their full potential. Our Fair Financial Services Project advocates for fair market practices for Texas consumers and works to address predatory payday and auto title lending, unjust debt collection practice, and financial abuse and coerced debt. Texas Appleseed is also a member of the Texas Coalition on Coerced Debt,[1] a coalition of attorneys, policymakers, financial professionals, and diverse advocates interested in promoting identity theft protections for survivors of family violence. My testimony addresses the intersection of data privacy and consumer protection where vulnerable groups, particularly survivors of domestic violence, are exposed to greater risks of financial harm and safety concerns.

Human Impacts of Scattered Data Privacy Protections

Advances in digital technologies have allowed consumer behavior to be incessantly monitored. Every day, mass amounts of data are collected from us using a range of methods, including online cookies, registered loyalty cards, public social media platforms, device or browser identifiers, and more.[2] Data brokers are major players in collecting and selling our personal data

[1] Texas Coalition on Coerced Debt and Texas Appleseed, "About Texas Appleseed and the Texas Coalition on Coerced Debt." (2022).
[2] Lois Beckett, "Everything We Know About What Data Brokers Know About You." ProPublica, (June 13, 2014).

to any party willing to pay. They collect data by purchasing it from other parties we do business with and through internet searches. With that data, they often place us into "audience segments," adding categories their algorithms define to data profiles on individual consumers. They then sell our data to interested parties, such as companies looking to advertise their products and businesses to better understand consumer trends, as well as to any person who may be looking for information about us and willing to pay.

Data brokers collect expansive lists of data about individuals.[3] Data collected often include full names, home addresses (both current and previous), telephone numbers, email addresses, age, gender, social security number, marital status, income, education history, and household income. They add a vast trove of digital information to that data, including web browser identification, web history, profile data, location information from mobile apps, and purchase history. Little to no accountability exists regarding what can be collected, who has access to the data, or how it is protected.

Consumers are becoming increasingly aware of the harmful ways that data is used, such as through targeted advertisements that can manipulate consumer decision-making or exploit vulnerable circumstances.[4] As our data gets passed around among countless third parties with whom we have no direct relationship, a vast array of companies profit from our data and create more possibilities for our data to be leaked or breached in a way that causes real harm.[5] A 2019 Pew Research Center study found that 81% of respondents expressed feeling that they have very little to no control over their data being collected from companies, and 79% expressed concern about how companies are using their data.[6] A lack of data privacy protections gives broad access to all of our vulnerabilities. Texas has the ability to protect individual privacy by enacting consumer data privacy laws and protections that give Texans the right to control their own data.

Federal and state data privacy laws

Currently, the United States does not have a singular data privacy law. There are a variety of data privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA),[7] Family Educational Rights and Privacy Act,[8] and the Fair Credit Reporting Act,[9] that are designed to address only specific types of data, such as medical, education, and credit records.[10] The lack of a comprehensive data privacy law leaves Texans vulnerable. In July of this year, the U.S. House

---

[3] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability." (May 2014).
[4] Jeannie Paterson, Shanton Chang, Marc Cheong, Chris Culane, Suelette Dreyfus, and Dana McKay, "The Hidden Harms of Advertising by Algorithm and Interventions from the Consumer Protection Toolkit." International Journal on Consumer Law and Practice, Volume 9, pp. 1-24, (September, 2021).
[5] In recent years, we have seen major data breaches from T-Mobile, Equifax, Robinhood, Edfinancial, which put millions of consumer's personal, private financial data at risk, and have brought about growing data privacy concerns from consumers.
[6] Brook Auxier, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, " Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center, (November 15, 2019).
[7] 42 U.S.C. § 1320d–2.
[8] 20 U.S.C. § 1232g; 34 CFR Part 99.
[9] 15 U.S.C. § 1681.
[10] Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." New York Times: Wirecutter, (September 6, 2021).

Energy and Commerce Committee passed out of committee the American Data Privacy and Protection Act (H.R. 8152), which is the first bipartisan compromise on a federal data privacy bill.[11] Though this bill is an important step forward, it is far from becoming law, and Texans need robust data privacy protections now.

State data privacy laws in Texas have similar shortcomings to those currently in place at the federal level. Texas has several statutes that provide some degree of accountability for data collection and use, but there is no comprehensive law that protects the right to privacy. Some of these scattered statutes include the Medical Records Privacy Act (comparable to HIPAA),[12] Texas Cybersecurity Act,[13] Student Privacy Act,[14] and amendments to Texas law governing data breaches,[15] which, respectively, protects and maintains confidentiality of medical records, enhances the state's cybersecurity programs, prohibits the sale of student education data, and expands on data breach notification laws. The amendments to laws governing data breaches, which passed in June of 2019, also created the Privacy Protection Advisory Council with the goal of advising the state legislature on current privacy laws. In the Council's report in 2020, one of the Council's recommendations to the state legislature was for policymakers to consider ways to strengthen Texans' "right to know how their personal information is being used."[16] To date, that recommendation has yet to be fulfilled. The Council's recommendation was a step forward in considering consumer-facing privacy issues but also left clear gaps in providing a full assessment of key consumer-facing privacy issues that need to be addressed.

Data privacy impacts for survivors of domestic violence

When thinking about survivors of domestic violence, data privacy is not the first thing that comes to mind for most people. However, advocates in this work understand how rapidly growing technology brings benefits and risks to the well-being and security of survivors. The way data today is used and abused has significant ramifications for individual safety and protection. Privacy is crucial for a survivor's safety. Privacy concerns for a survivor's safety and self-sufficiency can cause:

- Fear of asking for help or seeking non-shelter domestic violence services
- Fear of entering a protective space or shelter due to a lack of trust in confidential information procedures
- Homelessness to "stay off the technological radar"
- A refusal to get any type of state/government identification

Technology is a dominant force in society today. Under the current scattered approach to data privacy protection, and with expansive data collection and sharing, survivors are finding it

---

[11] House Committee on Energy & Commerce, "Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act." July 20, 2022 press release.
[12] Tex. Health & Safety Code § 181
[13] Texas Cybersecurity Act of May 30, 2017, 85th Leg., R.S., H.B 8, available at: https://capitol.texas.gov/tlodocs/85R/billtext/html/HB00008F.htm.
[14] Tex. Education Code § 32, Subchapter D
[15] Act of May 27, 2019, 86th Leg., R.S., H.B. 4390, available at: https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04390F.htm.
[16] The State of Texas, "Texas Privacy Protection Advisory Council." (September 2020) at 12.

increasingly difficult to maintain any form of privacy. With this new digital age of innovative technology comes ingenious ways for abusers to gain access to their victim's personal identifying information and have an even more significant impact on their victims' financial stability and physical safety.

Economic exploitation

Economic exploitation is one way that abusers can use the vast collection of data available to continue to harass and harm victims both when they are in an abusive relationship and long after they have left the relationship. Data show that economic exploitation is prevalent in abusive relationships.

In a 2021 nationwide study by the Center for Survivor Agency and Justice (CSAJ) on domestic violence and economic well-being, participants were asked about the abuse perpetrated in the intimate relationship for which they were currently seeking help.[17] Notably, survivors were asked about their experiences with economic restriction (e.g., the abuser kept the survivor from going to work) and exploitation (e.g., the abuser took out a credit card in the survivor's name) perpetrated by their abuser. Among the survivors surveyed, 97% were subjected to economic abuse. A 2019 report by the National Domestic Violence Hotline found that nearly one in three Texans who called the hotline disclosed experiencing economic/financial abuse, and 19% disclosed experiencing digital abuse, which was defined as abuse through "the use of technologies such as texting and social networking to bully, harass, stalk, or intimidate a partner."[18]

A specific form of abuse called *coerced debt* can burden the survivor with bad credit caused by the abuser. Coerced debt, defined as non-consensual, credit-related transactions occurring in an abusive intimate relationship, is a form of identity theft where an abuser obtains credit using the survivor's identifying information through threats, fraud, and/or coercion.[19] Although coerced debt is often associated with domestic violence, it is also found in cases of elder financial abuse, financial abuse of a person with disabilities, or child abuse/exploitation of youth. After a survivor has left their abuser, the abuser can continue to perpetrate acts of violence by financially exploiting their victim by taking out coerced debts – even if they no longer have physical access to their victim's important information – by purchasing their data through data brokers. Referencing the 2021 CSAJ study, over one-third of survivors reported an abuser taking out a loan or buying something on credit in the survivor's name without permission. This type of abuse is enabled by the ease of accessing and using another person's data.

Safety concerns

In addition to economic abuse and exploitation, abusers can use access to online data as a way to continue abuse and intimidation of a survivor, such as through doxxing. Doxxing –when

---

[17] Adrienne Adams and Sara Wee, "Domestic Violence and Economic Well-being Study." Center for Survivor Agency and Justice, (April 2021).
[18] National Domestic Violence Hotline, "Texas State Report." (2019).
[19] Angela K. Witten, "Coerced Debt: The Role of Consumer Credit in Domestic Violence." *California Law Review*, Volume 100, pp. 1-74, (June 1, 2012).

sensitive, personally-identifying information is purposefully released on someone –is an abusive practice that perpetrators of violence utilize to publicly shame, harass, and stalk their victim.[20] In addition, the sale of location information is a physical safety issue for survivors of domestic violence.[21] Before coming into my current role at Texas Appleseed, I worked as a domestic violence victim advocate at SAFE Alliance, the local domestic violence program servicing Travis County. I saw first-hand how determined abusers were to track down their victims, including by harassing friends and family members, incessantly calling shelters, and even going to the police to file a missing person's report to determine their victim's whereabouts. We cannot underestimate an abuser's tenacity and creativity in locating their victim to further exert power and control over them because it almost always has devastating consequences.

One of the most infamous examples of this is Amy Boyer and her stalker, Liam Youens.[22] Youens was obsessed with Amy since the two attended high school together and had subsequently started stalking her every movement. In 1999, abuser Youens contacted Docusearch, an internet-based investigation and information service, and requested personal information on Amy. Piece by piece, Docusearch located the information Youens requested – Amy's birthdate, social security number, home address, and workplace address – and sold him that information, no questions asked. Youens then used this information to locate Amy's workplace, where he fatally shot her before shooting and killing himself.

Amy's tragic death is not a one-off occurrence of the lengths that abusers will go to locate and further perpetrate abuse against their victims. More than twenty years later, Texans still face similar threats from abusers, as it has become cheaper and easier to access personal information in a legal environment with no data control or protections. The Safety Net Project, which focuses on how technology impacts domestic violence to address the safety and privacy of survivors, found in a 2014 survey that 97 % of domestic violence programs reported that the survivors in their programs experienced harassment, monitoring, and threats by their abusers through technology.[23] Survivors should have the undeniable right to control their own information and live free of harassment and abuse, and Texas Appleseed supports steps to increase privacy and control of personal data for Texans.

Texans Need Strong Data Privacy Protections

Texas Appleseed urges you to consider the profound implications that a lack of data privacy protections can have on Texans, especially the most vulnerable groups. There are several ways that Texas can better protect consumer data:

---

[20] Reports Committee for Freedom of the Press, "The dangers of doxxing." (May 19, 2015).
[21] Earlier this year, Texas Attorney General Ken Paxton sued Google for violating Texas' Deceptive Trade Practices Act – which protects Texas individuals and companies from commercial scams – for tracking consumers' location after users believed they had disabled Google's ability to do so and failing to disclose to consumers the other ways in which the company is able to track user location.
[22] EPIC, "The Amy Boyer Case." (June 15, 2006).
[23] Kaofeng Lee, "A Glimpse From the Field: How Abusers are Misusing Technology." Safety Net, (February 17, 2015).

- Allow Texans to see what data companies have collected and to request to have their data deleted,
- Require companies to ask consumers' permission to "opt-in" (instead of opting out) to sharing and/or selling data to third parties,
- Prohibit companies from collecting unnecessary data outside of the service they are providing, and
- Prohibit targeting of advertisements that has the effect of exploiting a vulnerability or discriminating against consumers with certain characteristics (e.g., lending discrimination based on race data collected).[24]

A 2021 Texas Appleseed report on data privacy and civil rights looks at how consumers have their civil liberties violated due to nonexistent and weak data privacy regulations. Demographic and location data collected can have crucial financial impacts on the type and cost of financial products offered to consumers, which can become discriminatory when race and location biases are factored into the cost of essential products, such as car insurance, forcing vulnerable groups to pay more than their counterparts for a product. Similarly, determining loan pricing for consumers in need of financial assistance becomes a data privacy issue when the use of alternative data – which may be incorrect – is factored into pricing.[25] Taking into account the inability of Texans to determine what personal data has been collected, shared, and sold, there is currently no way for consumers to address these issues that result from a lack of data privacy protections.

Texans should be able to freely and safely participate in this increasingly expanding digital society without fear that their personal data will be abused. It is crucial for companies to be held accountable for invasive and unnecessary data collection and sharing practices that lead to detrimental safety and financial outcomes for consumers. Data privacy is an issue that affects us all. Texas has the ability to prioritize data privacy protections and put control back in the hands of survivors, vulnerable groups, and all Texas consumers.

[24] CBS News, "Justice Department to Investigate "digital redlining" in lending." (October 22, 2021).
[25] Ann Baddour and Steve Perkins, "Texas at the Crossroads: Protecting Privacy and Civil Rights." (April 2021).