Texas Privacy Protection Advisory Council

Report

September 2020

The Honorable Greg Abbott
Governor of Texas

The Honorable Dan Patrick
Lieutenant Governor of Texas

The Honorable Dennis Bonnen
Speaker, Texas House of Representatives

Dear Governor Abbott, Lieutenant Governor Patrick, Speaker Bonnen, and members of the Legislature:

The Texas Privacy Protection Advisory Council submits this report in accordance with House Bill 4390, 86th Texas Legislature.

Respectfully submitted,

Senator Jane Nelson, Co-Chair

Representative Giovanni Capriglione, Co-Chair

Senator Carol Alvarado

Representative Rafael Anchia

Senator Kelly Hancock

Representative Matt Shaheen

Buffy Dyess

Dusty Hoffpauir

Bart Huffman

Justin Koplow

Audra Sawicki

Audra Sawicki

Joseph Schneider

Jeanette White

Lemuel Williams, Jr.

Michael Wyatt

I. Background

Americans are creating larger data footprints than ever before, and the way personal information is being collected, stored and disseminated is evolving rapidly. Some data is collected but never used. Other data is collected for marketing purposes or sold to third parties. In the wrong hands, personally identifiable information puts individuals at risk for identity theft, financial loss and even physical harm, yet many Americans feel powerless to control their own data. A recent Pew study found that over 80 percent of Americans believe they have little or no control over their personal information, while 70 percent said they feel their data is less secure today than it was five years ago. Only 4 to 6 percent said they actually understood how their data was being used.[1]

Current existing rights, precedents and laws that protect Texans' privacy from both government and private intrusion may be insufficient. A federal, nationwide proposal continues to elude Congress.[2] The Supreme Court has taken up cases over the past few decades dealing with wiretapping public pay phones and the use of thermal imaging technology, establishing that an individual's right to privacy exists even outside the scope of the physical home.[3]

The 86th Legislature approved House Bill 4390, which created the Texas Privacy Protection Advisory Council. The Council is composed of five members appointed by the Speaker of the House, three appointees being members of the House of Representatives and two being from the prescribed list of industries; five members appointed by the Lieutenant Governor, three appointees being members of the Texas Senate and two being from the prescribed list of industries; five members appointed by the Governor, three of whom being from the prescribed list of appointees, one representing a nonprofit organization that studies data privacy laws and one being a law school professor knowledgeable on the topic of data privacy. The Council is tasked with studying laws governing privacy and protection of information linked to a specific individual, technological device, or household and to make recommendations to the Legislature by September 1, 2020 concerning privacy and protection of Texans' information.[4]

II. Overview of Current Practices in Texas

The Texas Department of Information Resources (DIR) is Texas' lead agency for coordinating information resources, cybersecurity, and data storage across state government. DIR is also responsible for developing standards to protect the highly sensitive data maintained by state agencies.

Texas Government Code 2054 requires that agencies handling sensitive personal information, confidential information, or individually identifiable information submit a biennial data security plan. Those agencies must also conduct vulnerability and penetration tests of their websites. DIR is also required to adopt and post on its website a policy protecting the "personal information of members of the public who access information from or through a generally accessible internet site maintained by or for a state agency."[5] All of these requirements work to ensure that state agencies are aware and diligent when it comes to the personal information they handle.

Chief Data Officer

The Chief Data Officer position was codified in 2019 with the passage of Senate Bill 819.[6] The Chief Data Officer provides leadership and supports collaboration among state agencies and institutions of higher education.[7] The Chief Data Officer established the Statewide Data Management Program (SDMP). The program focuses on five key areas related to developing and sustaining agency data management.

1. Data Management Practices - Leveraging an industry best practice methodology, the SDMP provides a common framework of key principles such as Data Governance, Master Data Management and Data Quality to be used by agency data officers in establishing their individual data programs.
2. Data Sharing – To facilitate a consistent method of compliance with state and federal laws regarding data sharing and data security, the program established the Texas Statewide Data Sharing Exchange Compact (TSDEC). The TSDEC is a uniform data sharing and data security agreement for participating Texas state agencies and institutions of higher education. It contains the standard terms and conditions that any agency would require for data exchange. Once executed by all parties, it enables a more efficient and effective method of data sharing.
3. Data Analytics – Raw data alone is not meaningful. Unlocking the true value of data requires applying context and analytical practices. The program provides guidance into the various vendor-partner solutions to organize, categorize, analyze, and visualize raw data elements so that agency business decision makers can leverage data as a strategic asset to better serve their customers.
4. Open Data Portal/Closed Data Portal – The Open Data Portal (ODP) and Closed Data Portal (CDP) are described in detail below.
5. Data Literacy – An important component of any sustainable effort is education. The program has created and delivered various Data Management Practices and Open Data Portal classes and resource guides. These provide agency data leaders with knowledge to develop their individual programs and educate others within their organization on the key principles of data management and open data.

Texas Open Data Portal

DIR facilitates best practices in the areas of data governance, data sharing, data analytics, and government transparency through the Texas Open Data Portal. The Texas Open Data Portal (ODP) has existed since 2014, but in 2019 the 86th Texas Legislature passed Senate Bill 819, which designated the ODP as the official central repository of publicly accessible electronic data for the State.[8] As data published on the ODP is intended for public consumption, only publicly available data is accessible, which excludes personally identifiable information and other regulated data such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Criminal Justice Information Services data.[9] Ensuring that the proper security measures are put in place to protect private citizens' data is the responsibility of each publishing state agency, which follows its own internal data governance model to approve data for publishing on the ODP. As administrator of the ODP, DIR bears the responsibility of access control and setting user permissions. The ODP offers tremendous value

to state agencies as it provides a path for governmental entities to provide greater transparency. Redirecting constituents to the ODP is a great economic and performance benefit to governmental entities as it reduces the number of Public Information Requests. This saves governmental entities time and resources while still being open and transparent.

Texas Closed Data Portal

In addition to the Open Data Portal, agencies may also request their own instance of the Closed Data Portal. While the ODP is the official central repository for all publicly accessible open data sets, the CDP is a private data sharing environment intended to host private or sensitive data between state agencies.[10] The CDP is utilized for vertical data sharing, involvement between departments of the same agency, as well as horizontal data sharing, which is sharing between various agencies collaborating on a common project or topic. Unlike the ODP, the CDP is Federal Risk and Authorization Management Program, or FedRAMP Moderate authorized, which means that it meets federal requirements to protect the confidentiality, integrity, and availability of personally identifiable information. Access to data in the CDP is private and by invitation only. While DIR is the administrator of the ODP, the sponsoring agency administers access control and user permissions in its own CDP use, and likewise the agency follows its own data governance and workflow approval process before uploading data to the CDP. The value that the CDP offers participating agencies is not only that it is a free data sharing platform for the agency, but that by making data of mutual interest available, agencies reduce the duplicity of data collection efforts while increasing the efficiency and productivity of work performed on behalf of the citizens of Texas.

The Office of the Chief Data Officer (OCDO) established a collaborative set of teams that provide a forum for agency data leaders to share knowledge and experiences.[11] These are outlined in the table below.

Texas Enterprise Information Management (TEIM) group	• membership totaling between 35-50 members and representation of up to 30 different state agencies, higher education, and local governmental entities • facilitates sharing success stories, teachings, templates/tools, and other work products. • meets on a quarterly basis to discuss and learn from each other and the OCDO
Data Management Council (DMC)	• membership includes newly hired agency CDOs and Data Officers, • discusses more strategic elements of data management, leverage each other's experiences and that of the Chief Data Officer to further data programs.
Open Data Portal User Group (ODPUG)	• membership includes customers who use and publish on the ODP • similar to the TEIM and DMC, sharing collaboration team that focuses exclusively on the features and capabilities of the ODP • vendor that provides the infrastructure and ODP platform for the state joins meetings to provide updates on new product releases • share insights into how their agency leverages the ODP, how open data is governed and published, as well as other valuable tips and information.

Cybersecurity Prioritization

While determining what data is gathered and retained is important, an equally important piece of protecting sensitive data is cybersecurity. Cybersecurity is a critical function of state government. Since 2011 the Texas Legislature has made cybersecurity coordination and support a priority. In 2013 the Legislature entrusted state cybersecurity oversight with the Department of Information Resources (DIR), establishing the role of the State Cybersecurity Coordinator within DIR. Additionally in 2013 the Legislature directed each state agency to develop an information security plan to protect the agency's information. These bills established the current system of information security. DIR uses the system to provide guidance and direction to agencies, which in turn are responsible for their own cybersecurity.

Per its statutory requirement, DIR has promulgated Texas Administrative Code 202 (TAC 202) which sets a minimum baseline for cybersecurity standards for state agencies and institutions of higher education. First established in 2003, the code is continually reviewed and updated to keep pace with technology changes. Since its inception, it has been amended to address wireless technology, firewalls, encryption, and incident management. It outlines the responsibilities of agency heads, chief information security officers, and agency staff. However, each agency is required to develop, and periodically update, an information security plan for protecting the security of said agency's information. [12]

Similarly, cybersecurity continues to be a priority for private entities. Personal data is sometimes a key component in hack exploits, assisting in the targeting of victims. With phishing, extortion, data breaches, identity theft, romance fraud, and internet financial fraud on the rise, minimizing the collection of personally identifiable information and improving the security of the data becomes critically important. According to the Federal Bureau of Investigation's 2019 Internet Crime Report the state of Texas tied for the second highest number of internet crime victims in the U.S., with total losses to Texans estimated to be $221 million.[13] While federal and state laws do require cybersecurity and system protections for a variety of industry silos, most businesses have no requirements. A consumer entering their information online through a cellphone app or any other device has little knowledge of how or where that data ultimately resides.[14]

Aside from cybersecurity, privacy and data protection issues show up in other forms. Defamation and doxing are two methods frequently seen in online attempts to ruin a person's reputation. Defamation involves false statements while doxing is the publication of private information, such as an address or phone number. With the proliferation of the internet and a corresponding decrease in privacy, it has become much easier to employ these two damaging attacks.[15]

Privacy Laws

The Texas Legislature has taken several steps to protect the privacy of Texans' personal information, including:

- Student Data Privacy Act restricts the use of certain personally identifiable information, including personally identifiable information, by operators of a website, online service, online application, or mobile application;.[16]

- Texas Medical Records Privacy Act adds privacy protections for Texas patients that go above and beyond federal HIPAA requirements; and
- Texas Biometric Privacy Act limits a person from capturing, selling, or disclosing a person's biometric identifier – e.g. iris scan, fingerprint, or face geometry – without consent. The penalty for violation of the statute is a $25,000 civil penalty for each act.[17]

Further, the Business and Commerce Code contains several protections for personal data. The Identity Theft Enforcement and Protection Act states that a "person may not obtain, possess, transfer, or use personally identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name." The Act further requires a person who conducts business in the state and owns or licenses computerized data that includes sensitive personal information to disclose any discovered breach to individuals whose personal information was or is reasonably believed to have been affected. This disclosure must be made as quickly as possible. [18] House Bill 4390, which established the Texas Privacy Protection Advisory Council also requires Texas residents to be notified of a data security breach within 60 days of the determination that a breach has occurred. The bill also required that if a breach impacts more than 250 Texas residents, the business responsible for maintaining the information must provide notice of the incident to the Texas Attorney General within the same 60 day time period that governs notification of Texas residents.[19] Companies have a duty to protect sensitive personal information. The law requires businesses to implement and maintain reasonable procedures and take corrective action to protect sensitive personal information from unlawful use or disclosure.[20]

Texas has codified federal privacy protection laws, including the Federal Fair Credit Reporting Act, which protects credit related data and personal information, security alerts and security freezes to protect against ID theft.[21] Additionally Texas has codified the Federal Drivers Privacy Protection Act, which limits disclosure of personal information residing in motor vehicle records to entities that have a permissible purpose under the law.[22] Texas also has applicable laws related to accident reports and criminal records.[23]

Federal Laws

The private sector's use of data for commercial purposes is also subject to several federal laws that provide data privacy and safeguards. The Children's Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Video Privacy Protection Act and various other limitations on company practices with respect to the use and disclosure of information collected about individuals.[24]

Over the years many bills have been filed to holistically address data privacy from a national perspective, but none have become law. An omnibus federal privacy bill remains stalled in the United States Congress. In Congress, lawmakers have introduced data privacy laws to provide greater data security, transparency and regulatory oversight.[25]

III. Other States

As states across the country begin exploring ways to update their privacy laws, many are looking to the European Union. In January 2012, the EU approved General Data Protection Regulation (GDPR). The GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy. This new plan took effect in May 2018, essentially extending the EU's jurisdiction beyond those member countries. Any global business that sells to or has EU customers is subject to the GDPR, regardless of where that business is based. The GDPR sets forth rules about how companies treat the personal data of EU citizens, including those purchasing U.S. products or services or living in the U.S.[26] The GDPR has two components, individual/consumer rights, and business/corporate rules. Individuals have the right to:[27]

- information about the processing of their personal data;
- obtain access to the personal data held about themselves;
- ask for incorrect, inaccurate or incomplete personal data to be corrected;
- request that personal data be erased when it's no longer needed or if processing it is unlawful;
- object to the processing of their personal data for marketing purposes or on grounds relating to their particular situation;
- request the restriction of the processing of their personal data in specific cases;
- receive their personal data in a machine-readable format and send it to another controller ('data portability');
- request that decisions based on automated processing concerning themselves or significantly affecting you and based on their personal data are made by natural persons, not only by computers. They also have the right in this case to express their point of view and to contest the decision.

Along with the enactment of the GDPR in June 2018, the California Consumer Privacy Act of 2018 (CCPA) was enacted and then amended in September. The CCPA will become effective Jan. 1, 2020. CCPA is one of the most comprehensive, and most controversial, online privacy laws passed in the US., affecting companies across the country that do business with California residents. For California residents, it creates rights over their data. The most significant categories are "the right to know" and "the right to say no." Meaning users will be entitled to see what data companies have gathered about them, have that data deleted, and opt out of those companies selling it to third parties.[28]

Proposition 24, also referred to as the California Privacy Rights Act of 2020, if passed on the Election Day ballot, would leave California with the strictest data privacy laws in the United States.[29] This bill would establish the California Privacy Protection Agency and remove current allowances for companies to correct violations before punishment and fines (also known as the right to cure). The proposition would also give consumers certain rights, including the option to opt-out of the collection of sensitive data (such as certain specific geolocation, health, or

financial data), the ability to change inaccurate information, and add permission requirements from consumers under certain ages while tripling current applicable fines for violations regarding the sale and collection of children's personal information.[30]

In 2018, Vermont enacted a law requiring data brokers (businesses that collect and sell or license personal information to third parties) to disclose to individuals which data is being collected and to permit them to opt out of the collection.[31]

In 2018, the Ohio Legislature passed the Ohio Data Protection Act. This law created an affirmative defense to a tort action against a covered entity because of a data breach, if the entity is accused of failing to implement reasonable information security controls and the entity has a cybersecurity program that meets the act's requirements.[32] Proponents of the law noted that by creating a safe harbor, businesses would be incentivized to improve their cybersecurity systems and would minimize the collection of personal information in order to achieve this defense. Some opponents of the law suggested that the bar was set too high when it came to protecting consumer information.

In July 2020, the Florida Legislature passed a bill, prohibiting "issuers of life insurance, long-term care insurance, and disability income insurance from canceling, limiting, or denying coverage, and from setting different premium rates, based on personal genetic information."[33] Arguably, genetic information is the most fundamental and unique personally identifiable information and can be used to accurately (or falsely) discover previously unknown medical conditions for either the individual who consented to the test or even, at some point, individuals who did not consent to the test.

In March 2020, Washington passed a bill relating to the use of facial recognition services. The law increased regulation, oversight and accountability for the use of facial recognition software by state and local entities and did not incorporate the use of facial recognition technologies in the private sector.[34] Proponents of the legislation wanted the legislature involved in any design, procurement, or use of facial recognition technology, while many opponents wanted to ban its use entirely. The intent of the bill was to prevent discriminatory use and to acknowledge the high false positive/false negative rates. This was a contentious bill, passing the House 53-43 and later, partially vetoed by the Governor. [35]

Similar to Texas, other states have passed legislation establishing Councils or organizations to study data privacy laws and make recommendations. [36] Many other states have considered legislation representing a broad range of ideas related to personal data management. One of the most notable recent attempts was the Washington Privacy Act, which failed in conference committee. The act would have provided consumers, in part, the right to access, correct, and delete personal data, as well as the right to opt out of the collection and use of personal data for certain purposes.[37]

IV. Recent Legislative Actions (Texas)

As discussed previously, Texas has prioritized the protection of citizen's data through robust cybersecurity policies. The Legislature has made significant changes to current law and practices

concerning data privacy, cybersecurity, and information technology. Major legislation passed in the 86th Regular Legislative Session is summarized below:

- House Bill 1, the budget, included $1.8 billion in all funds for cybersecurity, legacy modernization (replacement of obsolete or inefficient hardware or software), and other information technology projects: enhancements, process improvements, procurement of new systems and other IT infrastructure upgrades.
- Senate Bill 819 improves the effectiveness of statewide information technology by establishing a statewide Chief Data Officer at DIR and agency-level data management officers; authorizing DIR to establish a Digital Transformation guide to assist agencies with digital initiatives and digitization efforts; and, requiring state agencies to consider developing new software applications as "cloud native".
- Senate Bill 64 bolsters cybersecurity in Texas by commissioning a study to incentivize cybersecurity higher education degree programs; bringing additional state agencies under DIR oversight; analyzing cybersecurity incidents across agencies for DIR review; improving electrical grid integrity by formalizing cybersecurity monitoring at the Public Utility Commission; and encouraging Information Security Officer services for small agencies and local governments.
- Senate Bill 820 assists school districts with cybersecurity by requiring superintendents to designate a cybersecurity coordinator and requires coordinators to report to the state any attack or incident once discovered, and to notify parents if student data is impacted.
- Senate Bill 936 develops a framework for collaboration between the Public Utility Commission, electric utilities, and ERCOT to secure critical electric infrastructure from cyber threats.
- House Bill 1421 requires the Secretary of State to adopt rules defining best practices to reduce the risks related to electronic election data and systems and requires counties to notify the Secretary of State when data breaches occur.
- House Bill 2984 updates the State Board of Education (SBOE) technology curriculum to included coding, computer programming, computational thinking, and cybersecurity for students in kindergarten through 8th grade. This ensures the curriculum is relevant to student education and aligned with current job market demands. Also the bill established a computer science strategic advisory committee to develop and provide recommendations for increasing computer science instruction and participation in public schools.
- House Bill 3834 requires DIR and the Cybersecurity Coordinator to certify training programs. State and local government employees and state contractors are required to complete a certified program.
- House Bill 4390 creates the Texas Privacy Protection Advisory Council and strengthens current data breach notification laws.

V. Private Sector

As mentioned previously, the rate of data collected, shared, sold, transferred, and lost across the globe continues to overtake laws that would protect individuals from negative consequences. Outlined below are several common issues of the larger topic.

Privacy Notices

Even with current state and federal legislation, Americans are still faced with many challenges related to the collection and use of their personal information. As previously stated, consumers usually have little to no knowledge of the extent to which their personal information is used even with safeguards that exist, such as privacy notices.[38]

Privacy notices, which are often treated by courts and regulators as enforceable promises made by a company to consumers, vary in form and length but should provide consumers with easy-to-follow guidelines about how their data is stored, used, and accessed. Comprehensive privacy notices generally include the types of personal data collected both actively and passively, how the information is used, how to access or correct personal information, and so on.[39] Most of these frameworks are very long and are written in complicated legalese, with the only actual choice consumers are given is to accept. Essentially consumers are left with a choice to accept all the conditions or they cannot access the webpage or services.[40]

Consumer Consent Practices

Organizations, aligning with either company privacy notices or regulations, face challenges in managing user preferences in regard to data collection. The two most common types of consent are opt-in and opt-out.[41] With opt-in consent, a company may not use or collect one's personal information without giving specific permission to do so. With opt-out, a company must allow a mechanism by which an individual can prevent their personal information from being sold or shared.[42] While this method is the preferred solution by regulators and industries, many consumers have expressed frustrations at the difficulty in attempting to even find the privacy opt-out options. Some private companies are not honoring the opt-out preferences of customers. While a "do not track" system would have allowed users to globally set their opt-in/opt-out preferences on internet connected devices, this method never caught on for a variety of reasons.[43]

Finally, there are situations where there is no actual choice for consent. This is expected in a myriad of situations where there is no reasonable expectation for the consumer to sign an opt-in or opt-out, and instead there is implicit consent for the organization to share personal information.[44] An example of such a situation would be the sharing of personal information by an online seller with the shipping and processing agents necessary to complete an online transaction.[45]

Complicating the issue further, once a user has been given notice and the consent exists, the right to view and correct that information is not always available. For example, any individual can request a free copy of their own credit report, review the information for inaccuracies, and submit corrections to those agencies.[46] Consumers might not be aware of the inaccurate information being collected and if they do know, review and correction of that information is often unavailable. This could lead to allowing false or misleading data to be propagated about an individual.

Data Collection & Data Brokers

Industries argue that constant data collection has many life-enriching benefits for consumers, such as an individually tailored buying experience for each consumer. Digital advertisers also argue that the current climate of collection and advertising creates an environment where

providers of all sizes and age can compete against the most dominant, established players.[47] Yet, it seems current protections do not fully safeguard the collection or use of sensitive personal information. For example, Google and YouTube recently agreed to pay a $170 million civil penalty to the Federal Trade Commission and New York to settle allegations that its video sharing service illegally collected personal information from children without their parents' consent.[48] Bad actors often deceptively collect consumer information for a described purpose while also using that information for a variety of reasons that were not conveyed to users. For instance, in August 2020, a popular fertility app used by more than half a million Android and Apple consumers, including many Texans, was accused of selling personal information without consumer permission to third party advertisers in China.[49] Facebook recently settled a suit involving the use of Facebook's facial-recognition technology without user consent. The Ninth Circuit Court of Appeals found that the use of this technology without consent "invades an individual's private affairs and concrete interests," and is an actual injury.[50]

Companies and organizations collect a variety of information, sometimes in real time, with consumers often unaware of the extent of data collection. Taken together much of this data can be used to build psychographic and behavioral models of each consumer using a person's lifestyle and beliefs, along with their purchases and real-life interactions. This can be used to either make predictions about their future actions or guide those actions. Some examples of data collection points include:

- Smart watches: precise GPS location, rate of travel, brain activity, body temperature, age, weight, gender, blood/oxygen levels, sleep patterns, etc.[51]
- Automobiles: onboard cameras, eyelid movements, driving techniques, number of children and passengers in vehicle, etc.[52]
- Cell Phone: precise location, facial recognition, contacts and proximity to friends, relatives and other individuals, microphone recordings, fingerprint, etc.[53]
- Apps: access to texts, friends, contacts, photos, phone logs, credit card information, account balance, dating and other social behavior, etc. Many reports note that some of these apps routinely violate the privacy of children.[54]
- Web browsing: purchases, videos watched, medical searches, travel information including length of time away from home, religious affiliation, sexual orientation, etc.[55]

Much of the information collected and stored on consumers is done by data brokers. The Federal Trade Commission (FTC) has characterized the information broker, or data broker, industry as the collection of consumer data from multiple sources, typically without the user's consent or knowledge. The FTC identified the three broad services typically offered by data brokers as marketing, risk mitigation, and location of individuals.[56] As noted previously, the Vermont data broker law requires data brokers to improve their security standards as well as to be registered with the state.[57]

Other Issues for Consideration

As is evident by the significant number of complaints, lawsuits and privacy bills being generated across the country, privacy issues are becoming increasingly important to the public.[58] A multitude of policy issues are raised on every side of the debate. Additional topics to evaluate going forward include:

- The regulatory and compliance costs of CCPA and GDPR which may have created uneven benefits and restrictions to certain consumers and businesses. Many companies in Texas are already complying with both laws and any Texas law should seek to compliment and not conflict with existing federal laws and frameworks.[59]
- The Fourth Amendment protections.
- The duties and responsibilities of application resellers in governing privacy policies of third-party vendors.
- The impact of COVID-19.[60]

VI. Request For Information

Due to the ongoing global pandemic and concerns regarding the spread of COVID-19 the Council was unable to meet in person. In an effort to provide maximum input from citizens, consumer right organizations, and industry stakeholders, the Council provided an online survey. The survey focused on three areas, private data, public data, and device/household privacy. The Council received over thirty responses that detailed competing ideas and concerns. The primary concern from many industry stakeholders was the concern over a patchwork of state laws. As most companies operate in many different states having consistent and similar laws is helpful and cost effective. Many respondents suggested waiting on a nationwide law from Congress to address concerns. Despite the potential for conflicting laws and standards, the protection of Texas' citizens and their data is the primary focus. Texas has always been a leader, and the Council's work will help shape the national conversation. Many responses highlighted the need for several factors to be considered in adopting an effective privacy framework, those are: control, transparency, consent, parity, uniformity, and security.

Another issue that was raised by numerous respondents was the impact of CCPA and GDPR. Many companies in Texas are already complying with both laws and any Texas law should seek to compliment and not conflict with existing laws and frameworks. Several responses highlighted the study by Berkeley Economic Advising & Research which has estimated the CCPA has cost California businesses $55 billion to comply.[61]

VII. Recommendations

a. Process for ensuring that all state agencies are adhering to privacy standards, and policies are continually updated to reflect new technologies, business practices, and risks.
b. Proposals should consider a new and appropriate balance between additional consumer privacy protections and data security within a fair regulatory/compliance privacy framework.
c. Proposals should consider the impact to highly regulated data, like health information or banking data, and how those proposals compliment applicable federal law.

d. Legislation should be written broadly enough to allow the adoption of new technology and business standards.
e. Proposals should consider existing laws in Texas and other states in order to not conflict.
f. Texans have the right to know how their personal information is being used and the Legislature should consider ways to strengthen that right.

---

[1] Brooke Auxier et al., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION PEW RESEARCH CENTER: INTERNET, SCIENCE & TECH (2020), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[2] *See* Alexandra S. Levine, WHERE FEDERAL PRIVACY BILL STALLS, COVID PRIVACY BILL TAKES SHAPE POLITICO (2020), https://www.politico.com/newsletters/morning-tech/2020/05/01/where-federal-privacy-bill-stalls-covid-privacy-bill-takes-shape-787279.
[3] *See* Katz v. United States, 389 U.S. 347, 348 (1967) (establishing Fourth Amendments extends to oral communication without actual physical trespass under property law); Kyllo v. United States, 533 U.S. 27, 29 (2001).
[4] H.B. 4390, Leg., 86th Reg. Sess. (Tex. 2019).
[5] TEX. GOV'T CODE § 2054.
[6] TEX. GOV'T CODE § 2054.0286.
[7] *Id*.
[8] S.B. 819, Leg., 86th Reg. Sess. (Tex. 2019).
[9] *See* TEX. GOV'T CODE § 2054.070.
[10] *See* Presentation from Department of Information Resources, Closed Data Portal (available upon request).
[11] *See* S.B. 819, Leg., 86th Reg. Sess. (Tex. 2019).
[12] TEX. GOV'T CODE § 2054.133.
[13] INTERNET CRIME COMPLAINT CENTER, 2019 INTERNET CRIME REPORT, https://pdf.ic3.gov/2019_IC3Report.pdf.
[14] Auxier, *supra* note 1.
[15] Ashu M. G. Solo, COMBATING ONLINE DEFAMATION AND DOXING IN THE UNITED STATES RESEARCHGATE (2019), https://www.researchgate.net/publication/334604707_Combating_Online_Defamation_and_Doxing_in_the_United_States.
[16] TEX. EDUC. CODE § 32.
[17] TEX. BUS. & COM. CODE § 503.
[18] TEX. BUS. & COM. CODE § 521.001.
[19] H.B. 4390, Leg., 86th Reg. Sess. (Tex. 2019).
[20] TEX. BUS. & COM. CODE § 72.004; TEX. BUS. & COM. CODE § 521.052.
[21] TEX. BUS. & COM. CODE § 503.
[22] TEX. TRANSP. CODE § 521; TEX. TRANSP. CODE § 730; TEX. GOV'T CODE § 411.
[23] TEX. TRANSP. CODE § 521; TEX. TRANSP. CODE § 550; TEX. GOV'T CODE § 411.
[24] *See* CONGRESSIONAL RESEARCH SERVICE ET AL., (2019), https://fas.org/sgp/crs/misc/R45631.pdf.
[25] Levine, *supra* note 2.
[26] Pam Greenberg, 2019 CONSUMER DATA PRIVACY LEGISLATION (2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx (last visited Aug 20, 2020).
[27] *See* What are my rights?, EUROPEAN COMMISSION - EUROPEAN COMMISSION (2019), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en (last visited Sep 1, 2020).
[28] Greenberg, *supra* note 21.

[29] Stacey Gray, Pollyanna Sanderson & Katelyn Ringrose, *Comparison of the proposed 2020 Washington Privacy Act (SSB-6281) to: GDPR, CCPA, California Ballot Initiative, and the 2019 WA Proposal*, FUTURE OF PRIVACY FORUM, 2020, at 1–8.
[30] Qualified Statewide Ballot Measures, QUALIFIED STATEWIDE BALLOT MEASURES | CALIFORNIA SECRETARY OF STATE, https://www.sos.ca.gov/elections/ballot-measures/qualified-ballot-measures/ (last visited Sep 1, 2020).
[31] Greenberg, *supra* note 21.
[32] *See* OHIO'S DATA PROTECTION ACT (2019), https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2019-ohio-lawyer/ohios-data-protection-act/.
[33] Invest in Biomedical Research, 2019 LEGISLATIVE PRIORITIES, https://www.bioflorida.com/page/2020LegislativePriorities.
[34] *See* Monica Nickelsburg, WASHINGTON STATE PASSES LANDMARK FACIAL RECOGNITION BILL, REINING IN GOVERNMENT USE OF AI GEEKWIRE (2020), https://www.geekwire.com/2020/washington-state-passes-landmark-facial-recognition-bill-reining-government-use-ai/.
[35] Letter from Jay Inslee, Governor, Washington, to Senate of the State of Washington (March 31, 2020) https://crmpublicwebservice.des.wa.gov/bats/attachment/vetomessage/559a6f89-9b73-ea11-8168-005056ba278b (explaining the partial veto was for budget reasons).
[36] Greenberg, *supra* note 21.
[37] S.B. 6281, State of Washington, 66th Legislature (2020). http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/6281-S.pdf?q=20200830101129
[38] Auxier, *supra* note 1.
[39] PETER P. SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 107-112 (2nd ed. 2018).
[40] https://fpf.org/2019/09/13/10-reasons-why-the-gdpr-is-the-opposite-of-a-notice-and-consent-type-of-law/
[41] Swire, *supra* note 35, at 78-79.
[42] *Id.*
[43] Swire, *supra* note 35, at 117.
[44] Swire, *supra* note 35, at 79.
[45] *Id.*
[46] *See* Disputing Errors on Credit Reports, CONSUMER INFORMATION (2018), https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports.
[47] Letter from American Association of Advertising Agencies (4A's), the American Advertising Federation (AAF), the Association of National Advertisers (ANA), the Interactive Advertising Bureau (IAB), the Network Advertising Initiative (NAI), and the Digital Advertising Alliance (DAA), to Texas Privacy Protection Advisory Council, http://networkadvertising.org/sites/default/files/final_response_to_texas_privacy_council_survey_8.21.2020.pdf.
[48] *See* Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, FEDERAL TRADE COMMISSION (2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.
[49] Tonya Riley, A POPULAR FERTILITY APP SHARED DATA WITHOUT USER CONSENT, RESEARCHERS SAY, THE WASHINGTON POST (2020), https://www.washingtonpost.com/technology/2020/08/20/popular-fertility-app-shared-data-without-user-consent-researchers-say/.
[50] Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).
[51] *See* Francisco De Arriba-Pérez, Manuel Caeiro-Rodríguez & Juan Santos-Gago, *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios*, 16 SENSORS 1538 (2016), https://www.researchgate.net/publication/308887529_Collection_and_Processing_of_Data_from_Wrist_Wearable_Devices_in_Heterogeneous_and_Multiple-User_Scenarios.
[52] *See* Jeff Plungis, WHO OWNS THE DATA YOUR CAR COLLECTS? CONSUMER REPORTS (2018), https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/.
[53] *See* Louise Matsakis, THE WIRED GUIDE TO YOUR PERSONAL DATA (AND WHO IS USING IT) WIRED (2019), https://www.wired.com/story/wired-guide-personal-data-collection/.
[54] *Id.*
[55] *Id.*
[56] *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N, (2014).https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[57] https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%2520Act%2520Summary.pdf
[58] Auxier, *supra* note 1.

[59] *See* ECONOMIC IMPACT STATEMENT, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std399.pdf.
[60] Lisa Weintraub Schifferle , COPPA GUIDANCE FOR ED TECH COMPANIES AND SCHOOLS DURING THE CORONAVIRUS FEDERAL TRADE COMMISSION (2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus.
[61] Lauren Feiner, CALIFORNIA'S NEW PRIVACY LAW COULD COST COMPANIES A TOTAL OF $55 BILLION TO GET IN COMPLIANCE CNBC (2019), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.