# WHY TEXAS NEEDS A DIGITAL BILL OF RIGHTS

by David Dunmoyer and the Honorable Zach Whiting

September 2022

Texas Public Policy Foundation

## September 2022

By David Dunmoyer and the Honorable Zach Whiting
Texas Public Policy Foundation

## Table of Contents

# Why Texas Needs a Digital Bill of Rights

David Dunmoyer and the Honorable Zach Whiting

### Key Points

- Data collection practices have become more rampant, sophisticated, and granular, leaving many users unaware of their data and privacy rights.
- Users have very little control over how their data is being used, and data application practices can have concerning consequences.
- Other states have passed data privacy laws to tackle this issue, and the EU adopted the GDPR to secure data privacy and protection.
- The Texas Legislature has addressed some data rights issues in previous sessions; however, more is needed to adequately address data privacy rights.
- With a digital bill of rights, Texans can have improved privacy online, knowledge on how their data is being used, and data collection controls.

## Introduction

In 2006, British mathematician Clive Humby mused that "data is the new oil." At the time, few could have imagined the extent to which the data commoditization would occur. By the early 2010s, many Americans became familiar with the story of retailers deploying data collection and customer tracking tactics to a new degree of efficiency. By monitoring shopping trends, Target's statistical software determined that a high school female from Minneapolis was pregnant, and they proceeded to send coupons for diapers and baby formula to her father's home. While these coupons initially seemed inappropriate to the father, he would later learn that they were being sent because Target knew before he did that his daughter was pregnant (Lubin, 2012).

Today, this story is relatively benign compared to contemporary data collection practices—the orders of magnitude in which data volume has increased in the last decade alone are staggering. For example, in 2012, the volume of data created, captured, copied, and consumed worldwide was 6.5 zettabytes (one zettabyte is equivalent to about 1 billion terabytes). That number has risen exponentially year over year, to 79 zettabytes worldwide in 2021 (Statista Research Department, 2022). This meteoric rise is fueled by a mutually reinforcing feedback loop, whereupon data collection practices become more sophisticated while consumers spend more time online and create more data inputs.

While social media companies and other businesses that stand to profit off data collection argue that it increases accuracy for targeted advertisements and tailored content, more than 80% of the public say that the risks of data collection practices outweigh the benefits (Auxier et al., 2019). These risks include confusion over data privacy, concern over how the data is shared, security breaches exposing personal data, and, ultimately, lack of control over the data individuals create and personal information they share. And with each new app, device, and data harvesting practice introduced, the public becomes less clear on what data is being collected, and generally more concerned with the perceived invasiveness.

As public awareness surrounding the activities of data brokers, data harvesters, and other entities collecting and using data enters the public's consciousness, states and other nations have taken action to safeguard the privacy of individuals' data. Specifically, the European Union enacted a sweeping data privacy and security law in 2018, and, as of this writing, five states have passed a Digital Bill of Rights to put users in greater control of their data and improve data security standards. The push for state-based solutions to data privacy accelerated in the late 2010s, and more than 20 states have introduced bills to codify data privacy protections for consumers.

Texas has taken steps in the right direction, attempting to enact legislation that would provide basic rights and protections for Texans while online. But thus far, efforts have fallen short. The best way for the Texas Legislature to effectuate data privacy, control, and security is to pass a comprehensive digital bill of rights. Doing so would place needed checks on actors who collect, process, and sell user data, while empowering Texans with transparency, control, and recourse for a commodity that should be recognized as personal private property.[1] Given the handful of states that have signed a digital bill of rights into law—as well as the European Union model—Texas can augment and modify existing models to create the greatest protections in the nation for its residents.

## Modern Data Collection Practices

Personal data is any form of information tied to one specific individual. Generally, a compendium of information is assembled on individuals, creating a robust "data profile" based on geographic, demographic, psychographic,[2] behavioral, and other information (European Commission, n.d.). Take Facebook, for example. When an account is created, basic information like age, location, relationship status, employment, etc., provide initial data inputs. From here, everything from uploaded photos to location-tracking to likes and comments on posts provides a perpetually refining data profile from which Facebook—under the existing terms and conditions—can scrape insights. Over time, how long you spend reading certain posts and which posts you elect to comment on will allow Facebook to better understand your political proclivity, mood, granular interests, purchasing patterns, and even whether you are happy in your current job. This Facebook example explains two common ways businesses collect data: directly asking customers and indirectly tracking customers. Facebook gets data by directly asking its users their age, location, and other information when they sign up; they indirectly track users by monitoring their habits and extrapolating behavioral data. One additional collection tactic, which has drawn increasing scrutiny, is the use of cookies by companies to track users while they are not on their site (Fowler, 2021).

According to Facebook's data policy, cookies are used to "provide, protect and improve the Meta Products, such as by personalizing content, tailoring and measuring ads, and providing a safer experience" (Facebook, 2022a, "Why do we use cookies" section). Another section titled "Third-party websites and apps" discloses that "business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook account or are logged in." Many social media users have a cursory understanding of this, having been served ads on social media sites stemming from outside web searches on Google and other businesses' websites.

For Facebook, this process generally works as follows. Facebook will give tracking software to their business partners so that it can be embedded in their app, website, and other digital touch points. Businesses that stand to benefit from digital advertising are quick to adopt this, making this a mutually beneficial partnership. Then Facebook will link the data created on third-party sites to an individual Facebook account, allowing Facebook to further fine-tune the way it tailors content and modifies the user's feed. According to 2020 data, Facebook's tracking software is on 23% of websites in the U.S., surpassed by Amazon at 29.4% and Google at 79.5% (Ghostery, 2020).

While it is true that consumers acquiesce to their data being harvested by companies when they create an account and sometimes blindly accept the terms of service, the terms and conditions are often crafted in an opaque

[1] Discussions of property ownership and rights date to biblical times. America's Founders were influenced by Enlightenment-era philosophy and jurisprudence, particularly the writings of John Locke. The Founders recognized that private property is the foundation of freedom. Property rights allow people to acquire, use, and dispose of property freely, and the limited role of the state is to provide for procedural safeguards of those rights from private actors as well as government (see, U.S. Constitution, Fifth Amendment).

Historically, data has been treated as intangible property. Texas law defines intangible property as "[a] claim, interest (other than an interest in tangible property), right, or other thing that has value but cannot be seen, felt, weighed, measured or otherwise perceived by the senses, although its existence may be evidenced by a document" (Texas Tax Code, Sec. 1.04(6)). Texas law defines tangible property as "personal property that can be seen, weighed, measured, felt, or otherwise perceived by the senses, but does not include a document or other perceptible object that constitutes evidence of a valuable interest, claim, or right and has negligible or no intrinsic value" (Sec. 1.04(5)). Data should thus be recognized as tangible property, which can be measured and perceived, at the very least. Regardless of its classification as intangible or tangible, the key is that it ***is*** property—defined under Texas law as "any matter or thing capable of private ownership" (Sec. 1.04(1)).

The authors of this paper philosophically hold that data is property and ought to be considered the property of the user generating this data. For example, a painter owns their painting—not the canvas manufacturer or art supply store. Data should be treated like the painting. The Legislature should codify data as property of the user to acquire, use, and dispose freely of this digital property.

[2] Psychographics is the study of consumers based on their activities, interests, and opinions.

manner that nudges consumers toward selecting options that extract and track the largest amount of data (Kerry & Chin, 2020). Notably, 91% of U.S. consumers do not read the terms of service before consenting, with an even higher rate of 97% for users ages 18–34 (Guynn, 2020). A series of privacy complaints filed by consumer rights groups against Google in June 2022 allege that the company deceptively designed the account creation process to steer users toward agreeing to invasive data processing. The group found that it takes a total of 10 clicks and a proficient ability to navigate "unclear, incomplete, and misleading" information to set up a more privacy-friendly option (Lomas, 2022, para. 5). Alternatively, the standard option takes just one click. But as is the case with other "privacy-friendly options" when creating accounts online, the terms are still not crafted in a manner that sees personal information and data as the property of the user. And even those who choose to deactivate their Facebook account, for example, are still tracked by the company (Ng, 2019). In summary, large social networking platforms design their services—and the terms and conditions therein—very carefully to acquire the largest volume of user data possible, while granting users little or no control or authority over the data they generate.

The above illustrations are but a few examples of a long line of data collectors and data collection methods. It is well established that data harvesting is pervasive for all the larger household name companies like Facebook, Google, and Amazon, but data collection is being used by businesses of all sizes—approximately 80% of businesses collect personal data from users in the United States (Statista, 2022). The precipitous rise in data collection has rendered it a practice that no longer provides a strong comparative advantage but rather allows businesses to simply remain competitive in their targeted ads, marketing, and other customer acquisition practices. Furthermore, the amount of data collected continues to grow due to declining costs of storing data, the increase in the number of digital devices in each household, new vectors to increase the volume of data generation, and improved data processing algorithms (Dhawan & Zanini, 2014).

## Big Data

This phenomenon has given rise to the term "big data." Big data is defined as "large, diverse sets of information that grow at ever-increasing rates" (Segal, 2022, para. 1). Big data is discussed in terms of the three V's—the volume of information, the velocity at which it is collected, and the variety of data in consideration. Volume refers to the complexity of the data sets in play, rather than just their size. Velocity is the speed at which data can be made available for analysis and insight development. And finally, variety indicates the diverse forms of structured and unstructured data in existence, like text, numeric, video, audio, and log files (Dhawan & Zanini, 2014). These three features make it different than traditional data sets in that they require complex processing that conventional data processing software cannot handle. In fact, the field of statistics itself has had to adapt given this transition from inert data sets to dynamic data that is being produced every second (Macnish & Galliott, 2020). This technological shift has happened dramatically, due to both the profitability associated with big data and the need for unfettered implementation to realize the purported benefits of big data. Because of the push to obtain more user data, individual privacy has been deemed of secondary importance in the push for service personalization and "data-driven solutions." According to philosopher and computer scientist Kieron O'Hara, "In order to be helpful to an individual, a system based on big data must be one of total surveillance" (O'Hara, 2020, p. 23).

In 2022, big data is enmeshed in practically every facet of life—from shopping, traveling, and banking, to interacting with state and local government and public utility providers, to sports, entertainment, and health. To understand the variety aspect of big data for digital consumers, some examples of the types of data collected include sent and received emails; social media posts, comments, and engagement; time spent viewing content; purchasing habits; search history; personal appearance; voice; facial movements; photos stored in your phone; physical location; personally identifiable information (or PII) such as driver's license numbers, social security numbers, phone numbers, and your address, and even more granular data like heart rate, gait, breathing patterns, and temperature (Cooper, 2022; Slynchuk, 2021; Vigderman & Turner, 2022). This list is certainly not exhaustive but illustrates the axiom that most things we do online can be monetized.

This, of course, is merely the current state of data collection practices. Assuming even a modest rate of progression in the development of new technologies—such as Apple's suite of augmented reality offerings on the horizon or newer vehicles that are collecting huge swaths of data on drivers and other vehicles on the road—the amount of harvestable consumer data is going to exponentially increase not only in size but also in precision (Apple, n.d.; Keegan & Ng, 2022). When thinking about new or improving technologies—from autonomous vehicles to the Internet of Things to smart home devices—new avenues are constantly emerging for companies to collect more information on users. And for companies that want to create the most personalized experience with their technology, they will be relying on increasingly granular data to do so.

## How the Data Is Then Used

Once major companies collect enough data on users, this information is used for diverse purposes. The first and most broadly advertised reason is to personalize ads and improve a business's products and services. For example, Google's Privacy & Terms reads:

> *We collect information to provide better services to all our users—from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls. … We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.* (Google, 2022)

While Google declares, "We never sell your personal information to anyone," this clever wordsmithing belies reality (Google, n.d., "Ads that respect your privacy" section). Large companies like Google monetize user information by (1) building individual profiles based on their data and then letting advertisers target people based on their data and (2) by sharing data with advertisers directly and then opening it up for bids on ads (Cyphers, 2020). Because Google "anonymizes" user information, they can technically make the above declaration, even if the data is rich enough to determine who the user is without the inclusion of a name or other more obvious personal identifiers.[3]

As another example, Facebook's privacy policy states:

> *We use the information we have to deliver our Products, including to personalize features and content (including your ads, Facebook News Feed, Instagram Feed, and Instagram Stories) and make suggestions for you (such as groups or events you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products.* (Facebook, 2022b, "How do we use this information?" section)

Other data applications directly help businesses improve efficiency, service delivery, and, potentially, profit margins. For example, IBM's Deep Thunder weather analytics package is a big data effort undertaken to provide targeted forecasting in a manner much more granular and specific than traditional meteorology. This project is used for agricultural efficiency, such as helping farmers know precisely when to irrigate crops. Another example is Royal Dutch Shell, which has developed a "data-driven oilfield" to bring down the cost of drilling for oil. Specifically, they have compiled big data across sites to determine the presence of hydrocarbon resources at a site as a means of increasing drilling efficiency (Dhawan & Zanini, 2014).

### Data Brokers

The next major application of user data lies within the data brokerage model. Data brokers exist to collect personal information, bundle this information together, and sell to third-party buyers. They cunningly employ data scrubbing tactics to scour through personal information users provide while using services like social media, search engines, news sites, apps, and more, and work with major companies to buy user data. By tracking users online and offline, these data brokers assemble incredibly thorough data profiles on individuals, whereupon users are sorted into neatly organized categories to be sold to third parties (Latto, 2020). This industry, which generates more than $200 billion annually, is highly lucrative given the number of interested buyers and the potency of this data (Brathwaite, 2022). Below are just a few examples of ways data brokers use and sell the information they collect:

- Data brokers have found rewarding clients in political campaigns. Most notably, the Cambridge Analytica campaign that targeted "persuadables" using personality and psychographic data received information through third-party data brokers (Pegoraro, 2020). After buying user data from brokers, the campaign was

[3] This same model of data sharing is employed by many major companies that collect rich user data. However, the massive amounts of information generated on social media platforms make them a very attractive target for organizations looking to collect information.

able to pinpoint swing voters in precincts that were not a stronghold for either political party and served them tailored content to nudge them toward a political candidate.

- Data brokers have also found government clients willing to buy their information. For example, in 2020, a data broker shared billions of "highly sensitive" phone location records with the District of Columbia. This data was scraped and then given to the government to track how people maneuvered through the city amidst the COVID-19 pandemic (Harwell, 2021).

- Data brokers will generally sell the data they have obtained to any interested buyers, with little oversight to whom they may sell personal information. In one harrowing case, a disgruntled lawyer obtained the address and personal information of a United States district court judge through a data broker. Upset with the judge over the pace she set for a lawsuit filed in her court, he used this information provided by data brokers to exact revenge by killing the judge's son and critically wounding her husband (Salas, 2020). This underscores a broader point in the need for data privacy: Data brokers exist to obtain user data to turn a profit, with no oversight over whether this information is sold to a local business or a foreign actor.

- During a 2013 congressional hearing, Executive Director of the World Privacy Forum Pam Dixon divulged sensitive lists that data brokers were selling. These lists included personal information on victims of rape, individuals with alcoholism, and AIDS/HIV sufferers (Hill, 2013). These lists were assembled with the intent to sell 1,000 names for $79 to any interested advertisers or other buyers.

- Other data brokers deal in risk mitigation. By compiling data on an individual's history or propensity of risk—such as the frequency of check-ins at one's gym and other indicators of an active lifestyle—life insurance premium costs might change based on risk for health issues.

- Some data brokers deal in fraud detection. Before issuing loans, some banks will turn to data brokers to ascertain whether an individual looking to take out a loan is providing accurate information or whether they are fraudulently seeking a loan.

The above examples capture the major categories of data brokers, highlighting the truly consequential power they have in their industry. Election nudging, predatory advertising, physical monitoring, risk profiling, and more raise genuine concerns over presumed privacy and the commoditization of personal information. The Government Accountability Office (GAO) stated that:

> *While current laws protect privacy interests in specific sectors and for specific uses, consumers have little control over how their information is collected, used, and shared with third parties for marketing purposes. … Thus, the current privacy framework warrants reconsideration in relation to a number of issues, including consumers' ability to access, correct, and control their personal information used for marketing; the types of personal information collected and the sources and methods for collecting it; and privacy controls related to relatively new technologies.* (GAO, 2013, p. 46).

Later in this paper, we will discuss how this has changed in some states. However, in Texas, this reality is still largely the same.

## Criminal Data Application

Big data has also been used for nefarious purposes—hacking, cyber extortion, and other means of illegally obtaining or using personal information. Data breaches are becoming increasingly more prominent and lucrative. In 2021 alone, more than 4,000 data breaches exposed more than 22 billion records (Risk Based Security, 2022). One of the more well-known breaches was Equifax in 2017. More than 145 million Equifax customers had their data stolen—names, Social Security numbers, dates of birth, credit card numbers, and driver's license numbers. It would later be revealed that this breach was part of a series of attacks from China to target American officials (FBI, 2020). An even larger data breach happened in 2013, when three billion Yahoo! users' data was hacked, including personal information like names, email addresses, telephone numbers, and dates of birth. Later, it was discovered that these hackers were able to obtain passwords too, as they attempted to sell more than 200 million Yahoo! accounts on the dark web (Cox, 2016). For all data breaches, the overwhelming majority—some 90%—are motivated by the lucrative nature of the crime. Most frequently, attackers will use stolen data to commit additional crimes, such as breaking into user accounts, committing fraud, transferring funds, etc. Moreover, it is common for attackers to use breached information from one account to target accounts on different platforms (LMG Security, 2022). Finally, inadequate security on the part of businesses and employee negligence is a significant contributor to data breaches. According to Verizon's Data Breach Investigations Report (2022), the human element drove 82% of breaches in the past year. This includes everything from inadequate IT training for employees to poor password security and cybersecurity hygiene.

### Growing Consumer Concern

Alongside the growth of consumer awareness is an increasing desire for policies that secure data privacy. According to recent survey data from KPMG, 86% of the U.S. general population believes that data privacy is a growing concern. Specifically, 68% of the population is concerned about the level of data being collected by businesses, with 40% distrusting companies to use their data ethically (KPMG, 2021). Moreover, an overwhelming majority of Americans feel like they have very little control over the data that companies and the government collect about them—81% for data collected by companies and 84% for the government (Auxier et al., 2019). Those who express increasing concern over data collection practices broadly agree on the solution, too. Approximately 75% of Americans want the federal government to enshrine national data privacy standards, expressing a broad desire for a digital bill of rights (AP NORC, 2021). While poll-tested support for this policy solution exists at the federal level, the federal government has not made significant progress on a digital bill of rights or broader data privacy protections for Americans. As of this writing, federal data privacy legislation has come to the fore in both chambers with the American Data Privacy and Protection Act. As it is being actively considered, the bill is receiving pushback from California representatives who note that the federal legislation has a preemption clause that would effectively supplant stronger data privacy protections that have been enacted in states like California (Lima, 2022).

## State-Based Solutions to Data Privacy

At the time of this publication, five states have enacted data privacy in the form of a digital bill of rights. Below is a breakdown of each law, including how each addresses many of the core privacy concerns identified in the previous section.

### California

In 2020, California enacted the California Consumer Privacy Protection Act (CPPA), making it the first U.S. state to codify a digital bill of rights. At a high level, this act provides Californians with the right to know what personal data is being collected about them; the right to know whether their personal data is sold or shared and to whom; the right to say no to the sale of personal data (the right to opt out); the right to access personal data; the right to request a business to delete any personal information about a consumer collected from the consumer; and the right for consumers to not be discriminated or retaliated against because they exercised any privacy rights. In addition, new limits were placed on the sale, sharing, and use of personal information and sensitive personal information (California Consumer Privacy Act, 2018). The CPPA applies to for-profit entities doing business in California that meet any of the following criteria: gross annual revenues in excess of $25 million; entities that annually buy, receive, sell, or share personal information of 50,000 or more California consumers, households, or devices; or businesses that bring in at least half of their annual revenues from selling California consumers' personal information (BakerHostetler, 2019).

The body responsible for enforcing the CCPA is the Office of the Attorney General (OAG). In its role as enforcer, the OAG sends notices of noncompliance to companies allegedly violating consumer rights outlined in the CCPA. Once a company is made aware of potential noncompliance, it has 30 days to cure the issue. Failure to do so results in civil penalties of $2,500 for each violation or $7,500 for each intentional violation after notice and the 30-day window (State of California Department of Justice, n.d.). In addition to the OAG's enforcement, private plaintiffs can bring civil actions against businesses if a data security breach causes unauthorized access and exfiltration, theft, or disclosure of an individual's personal information. This statute allows for "recovery of up to $750 per consumer, per incident, or actual damages, whichever is greater" (BakerHostetler, 2019, p. 6).[4]

Because California has the longest standing digital bill of rights, it is the one model that has produced some preliminary outcomes worth noting. When it comes to Californians exercising their right to opt out of the sale of personal information, consumers have struggled to locate

[4] In November 2020, California voters passed California Proposition 24, modifying the CCPA with the newly passed Consumer Personal Information Law and Agency Initiative. This expanded California's consumer data privacy laws by providing consumers the ability to direct businesses not to share their personal information, while removing the period businesses had under CCPA to cure violations (before being subject to a penalty) and creating the Privacy Protection Agency to enforce data privacy laws (Legislative Analyst Office, n.d.).

the website features to exercise this right. Specifically, for 42.5% of websites that were tested by Consumer Reports' Digital Lab, one in three users could not find the opt out link (Mahoney, 2021). This has exposed some flaws in the opt-out model adopted by California, suggesting newly drafted digital bills of rights should contain more specifics requiring greater visibility and accessibility for opt-out links on business websites. Moreover, as an option to make exercising privacy preferences easier, Texas should require the ability to opt out of all data sales in one step, rather than what can be an onerous, multi-step process for users looking to exercise their digital rights. An additional problem is the hamstringing of attorney general enforcement due to the 30-day cure period. The same Consumer Report study encourages tightening the cure period as a means of incentivizing timely compliance.[5] Finally, there is evidence to suggest that California's law would have been more successful if privacy had been protected by default, rather than placing the burden on users to exercise their rights, which can be burdensome and complex.

However, there have also been notable successes from the law. In July 2021, California Attorney General Rob Bonta reported that after businesses received notices of noncompliance, 75% of businesses corrected the issue within the allotted 30-day window. And for the remaining businesses, they were either within the 30-day cure period or were under active investigation by the attorney general's office (California Office of the Attorney General, 2021). Moreover, more than a quarter of the companies that received noncompliance notices received them for not having "do not sell my personal information" links on the website, suggesting enforcement is beginning to tackle some of the concerns outlined in the above paragraph. California has also found success in improving the transparency of companies' data collection practices, as well as the ease of understanding how their digital rights apply. In one example, a business received a notice of noncompliance for a privacy policy that the OAG found difficult to read and replete with legal jargon (Raether et al., 2021). In terms of the private right of action, it took time for users to understand how to exercise this enforcement power, but class action filings have steadily risen since the CCPA went into effect. For example, in 2021, 281 federal court cases were filed related to the law (which excludes cases brought by individuals outside of class action mechanism), marking a 44.10% increase in litigation filings relative to 2020 (Valdetero & Zetoony, 2022).

Ultimately, with how transformative a policy this is and with the time it has taken for businesses to adjust to this new privacy for users, there has not been enough time for a comprehensive analysis of its outcomes. However, as we suggest later in this paper, we can learn from some of the shortcomings of the CCPA to ensure the Texas model is as robust and sound as possible.

### Virginia

Virginia was the second state to enact a broad data privacy law, with Governor Ralph Northam signing the Virginia Consumer Data Protection Act (VCDPA) into law on March 2, 2021. The law will go into effect on January 1, 2023. The Virginia law was influenced heavily by both the CCPA and the European Union's General Data Protection Regulation (GDPR), yet it remains unique in a few respects (Hart & Zick, 2021). The VCDPA enumerates the following rights for consumers: the right to confirm whether or not a controller is processing a consumer's personal data; the right to access personal data; the right to correct inaccurate personal data; the right to delete personal data; the right to obtain a portable and transmittable copy of the consumer's personal data; the right to opt out of the processing of personal data for purposes of targeted advertising, selling personal data, or profiling; and the right to appeal if a business fails to respond to a consumer request within the defined 45-day window (SB 1392, 2021, pp. 3–4). The scope of data protections is comparable to that of California and Colorado, with the VCDPA applying to businesses that control or process the personal data of 100,000 or more consumers per year. However, for businesses that receive 50% or more of gross revenue from selling personal data, the threshold is reduced to 25,000 consumers (Hart & Zick, 2021).

As is the case with Colorado, the VCDPA made it explicit that there is no private right of action for any data privacy violations. This leaves enforcement of the law solely up to the attorney general's office. The attorney general is given the authority to take individual businesses to court and hold them liable to secure civil penalties of up to $7,500 per data violation. The act requires that the attorney general give the business a written notice 30 days before any action is brought to court, and businesses are given the ability to

[5] Of note, in the section titled "Texas' Digital Bill of Rights," the authors outline a plan to sunset this cure period as a means of improving lackluster noncompliance enforcement.

avoid legal trouble by correcting any violations. Ultimately, enforcement only occurs when a business fails to comply; if a business offers a written statement notifying the attorney general's office that all violations have been addressed, they are effectively exonerated (Moomaw, 2021). Finally, this act created the Consumer Privacy Fund on the books of the state comptroller. All funds collected from civil penalties, expenses, and attorney fees are allocated to the fund and used to support the Office of the Attorney General's enforcement of the VCDPA (SB 1392, 2021, p. 8).

### Colorado

In July 2021, Governor Jared Polis signed the Colorado Privacy Act into law, which will go into effect on July 1, 2023. Similar to the CCPA, Colorado's data privacy legislation will afford consumers the following rights: the right to opt out of data processing for targeted advertising, sale, or profiling using their personal data; the right to access data that a company has collected about them; the right to have any data corrected that is either incorrect or outdated; the right to have any data collected deleted; and the right to data portability (transferability of data to another entity; SB 21-190, 2021, pp. 18–20). In addition, consumers may submit requests to opt out of their PII from being processed for targeted advertising, to know and gain access to their PII if a controller is processing it, to correct inaccurate items in their PII, and to elect to delete PII (Usercentrics, 2021). These protections apply to Colorado businesses that either control or process the personal data of at least 100,000 consumers per year or control or process personal data for 25,000 or more consumers and derive any revenue or receive a discount on the price of goods or services from the sale of personal data (Koley Jessen, 2021).

Unlike the CCPA, the Colorado Privacy Act does not afford consumers a private right of action against businesses. Moreover, the "cure period" is twice the length of California's, with businesses allotted 60 days to rectify violations of alleged noncompliance. Enforcement is left exclusively up to the attorney general and district attorneys. Furthermore, under this law, a violation is deemed a deceptive trade practice, with penalties as high as $20,000 per violation. And while California's law provides special protections for personal information deemed "sensitive"—such as personal information detailing race, religion, social security numbers, a consumer's precise geolocation—Colorado's act requires covered entities to receive consumer consent before processing all sensitive personal information (Koley Jessen, 2021).[6]

### Other States

Utah and Connecticut recently enacted comprehensive data privacy legislation, in March and May 2022, respectively. In the Utah Consumer Privacy Act, consumers are given the right to access, deletion, and portability, and the ability to opt out of targeted advertising and the sale of personal data. This act is very similar to that of Virginia and Colorado, as the attorney general is granted exclusive authority to enforce provisions—with no private right of action—when it goes into effect on December 31, 2023 (Holland, 2022). The Connecticut Data Privacy Act (CTDPA) also has few significant departures from its predecessor laws in Virginia and Colorado. When this law goes into effect on July 1, 2023, Connecticut residents will have the right to access, portability, knowledge of whether data is being processed, data correction, and deletion, with the same enforcement mechanism provided in Utah, Colorado, and Virginia (SB 6, 2022, pp. 9–10).

### International: The General Data Protection Regulation (GDPR)

The GDPR, put into effect by the European Union on May 25, 2018, is considered the "toughest privacy and security law in the world" (Wolford, n.d., para. 1). This provided a legal framework for the collection and use of personal information for citizens of the member states of the EU—even if the business in question is headquartered outside the EU—while giving citizens much more control over their personal data. Under this structure, a number of rules are enforced, such as notifying website visitors what data would be collected and asking for their consent to collect it; timely notification if any personal data collected by a website is breached; mandatory assessments for website data security; and many more data privacy principles that require organizations to, "by design and default," consider data protection (GDPR, 2016, chap. IV, § 1, art. 25). This last piece is particularly important, as the EU has proclaimed that the GDPR is "large, far-reaching, and fairly light on specifics" (Wolford, n.d., para. 2). Failure to comply with the GDPR results in harsh fines, with penalties climbing as high as €20 million or a penalty of 4% of a company's worldwide annual revenue, whichever is higher.

[6] Pursuant to the codified version of the Colorado Privacy Act, sensitive data is defined as "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status (SB 21-190, 2021, p.8)).

**Table 1**

*Comparing State and International Data Privacy Standards*

| Consumer Rights Include: | California CCPA | Virginia VCDPA | Colorado CPA | Utah UCPA | Connecticut CTDPA | European Union GDPR |
|---|---|---|---|---|---|---|
| **Effective Date** | 1/1/2020 | 1/1/2023 | 7/1/2023 | 12/31/2023 | 7/1/2023 | 5/25/2018 |
| **Data Access Rights** | X | X | X | X | X | X |
| **Data Correction Rights** |  | X | X |  | X | X |
| **Data Deletion Rights** | X | X | X | X | X | X |
| **Data Portability Rights** | X | X | X | X | X | X |
| **Right to Opt Out of Sale** | X | X | X | X | X |  |
| **Private Right of Action** | X |  |  |  |  |  |
| **Potential Cost of Single Violation** | $2,500 | $7,500 | $20,000 | $7,500 | $5,000 | €20 million |

*Note*. Information taken from relevant state law and the GDPR.

## Texas

Currently, Texas does not have a comprehensive law on consumer data privacy and protection. However, the Texas Legislature has considered this issue in previous sessions and established the Texas Privacy Protection Advisory Council in the 86th Legislature to study data privacy laws in Texas, other states, and relevant foreign jurisdictions (HB 4390, 2019).[7] In September 2020, the council published its first report, leading with a recognition that "current existing rights, precedents and laws that protect Texans' privacy from both government and private intrusion may be insufficient" (Texas Privacy Protection Advisory Council, 2020, p. 1). They note that Texas passed major legislation in the 86th legislative session concerning cybersecurity and information technology project modernization (HB 1), bolstering education to include more technology-oriented studies (HB 2984), and other important legislative progress. However, the group cited the following shortcomings with data privacy protections:

- Texans generally have little knowledge of how their personal information is used, even with current safeguards such as privacy notices;
- Texans are rarely given the choice to consent to data collection. Rarely are consumers afforded accessible means of opting out of data collection, and there are many situations where the consent is implicit for organizations to share personal information;
- Texans rarely have the ability to view personal information collected about them. In the instances where this personal information can be viewed, it is rare that consumers are able to review and correct (potentially erroneous) information;
- Existing protections do not go far enough to safeguard sensitive personal information collection practices; and
- Bad actors continue to use deceptive means of collecting personal information, and then may use information for reasons that have not been conveyed to users (Texas Privacy Protection Advisory Council, 2020).

In this same report, the advisory council provided the following recommendations to the Texas Legislature:

- *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.*
- *Proposals should consider a new and appropriate balance between additional consumer privacy protections and data security within a fair regulatory/compliance privacy framework.*
- *Proposals should consider the impact to highly regulated data, like health information or banking data, and how those proposals compliment [sic] applicable federal law.*

[7] In 2019, lawmakers introduced HB 4518 (the Texas Consumer Privacy Act) in an attempt to pass comprehensive consumer data privacy protections. This bill ultimately did not advance as it remained pending in committee.

- *Legislation should be written broadly enough to allow the adoption of new technology and business standards.*
- *Proposals should consider existing laws in Texas and other states in order to not conflict.*
- *Texans have the right to know how their personal information is being used and the Legislature should consider ways to strengthen that right.* (Texas Privacy Protection Advisory Council, 2020, pp. 11–12)

Notably, this report was published prior to the 87th Legislature, in which several data privacy bills were introduced. Initially, a few bills were signed into law concerning state and local government technology and cybersecurity, consumer privacy for state agencies, and other security and technological advancements for public entities (Vaughn & Paylor, 2021). This includes HB 3746 (2021)—which requires the attorney general's data breach portal to be public and show information concerning victims—and SB 15 (2021)—which stipulates that the state of Texas may not sell individuals' motor vehicle records. While SB 15 and HB 3746 were enacted into law, HB 3741 (2021) never received a committee hearing in the House. HB 3741 would have provided Texans with a robust standard of data privacy protections. In short, this would have afforded Texans a digital bill of rights:

- The right to know: Disclosure and use of collected personal information;
- The right to have inaccurate information corrected;
- The right to access and obtain information; and
- The right to delete sensitive personal information (HB 3741, 2021, pp. 8–9).

While HB 3741 has similarities to the CCPA, some important modifications were made. First, the bill separated data into three distinct categories:

- category one information, which means "personal identifying information that an individual may use in a personal, civic, or business setting,"[8]
- category two information, which means "personal identifying information that may present a privacy risk to an individual, including members of a constitutionally protected class,"[9] and
- category three information, which means "specific facets of personal identifying information"[10] (HB 3741, 2021, pp. 1–2).

The bill also precluded businesses from collecting and selling certain data and required "express written consent" for the sale and collection of geolocation data. Finally, the Texas Attorney General's office would have enforced the law, with the ability to seek "a civil penalty in an amount of not more than $10,000 for each violation, not to exceed a total of $1 million" (p.15). While this bill did not advance, it provides a roadmap for how Texas can provide its residents with robust data privacy standards that safeguard against nefarious actors, invasive data collection, and violations of civil liberties.

## Texas' Digital Bill of Rights

As a matter of privacy, security, property rights, user empowerment, and, ultimately, civil liberty, Texans should have more robust data privacy protections in the form of a digital bill of rights. Given that five states (and the European Union) have codified comprehensive data privacy protections, Texas has the opportunity to build off existing models and incorporate the strongest user privacy protections in the nation. The need for such legislation has been addressed above. Moreover, as federal legislation continues to stall and data collection practices only increase in scope, the time for Texas to act is now. Below are the recommendations for a Texas digital bill of rights.

### Rights

Initially, the following rights ought to be included.

First, individuals should have the right to know, specifically by requiring data controllers to inform users on what data is being collected, the source of the information, the purpose for collection, and the third parties that have been

[8] Includes a social security number, a driver's license number, financial account number, unique biometric information, physical or mental health information, and the private communications of an individual.

[9] Includes racial or ethnic origin information, religious affiliation or practice information, age, and precise geolocation tracking data.

[10] Includes time of birth and political party or association.

given access to one's information. This right will provide the animating principle of transparency that is key to Texans' understanding of how the data collection processes affect them and will shine a light on the black box that is the final location of their data.

Second, the right to have inaccurate information corrected. That is, if a consumer notes that personal information collected by a business is inaccurate, businesses are required to rectify the issue after notice from an individual. It is important for both consumers and businesses to have correct information, because inadequate or false user information might result in unreliably tailored services and potentially harmful consequences if, for example, an individual's criminal record was submitted to a business incorrectly.

Third, Texans should have the right to delete any personal information. But unlike other state models of comprehensive data privacy protection, deletion rights should be reserved for any user data, or personally identifiable information, not just the sensitive class. Consumers should have the right to know what data is being collected and, therefore, could determine what personal information is being stored to then have it deleted if they so choose.

Fourth, Texans should have the right to obtain and reuse their personal data for their own purposes across different services—also known as the right to data portability. This would allow users to access personal data such as browsing history, location data, raw data processed by smart devices, and data on social networking sites, for example. They would then be able to use it for personal use, storing, or transmission to another data controller. This right would provide a step in the right direction toward a model of data ownership, as consumers could choose to use their data for purposes that they see fit (such as sharing contact information, posts, photos, videos, etc. across various social networking platforms).

Fifth, Texans should have the right to opt out of the sale or dissemination of their personal information. Specifically, consumers should be able to direct a business that collects, sells, or shares personal data to not sell, share, or use this information for targeted ads. Of course, this right strikes at the core of consumer control over their data, as well as ownership in the sense that businesses will have to defer to individual users rather than engage unfettered with few consequences.

A bonus consideration is the right not to be discriminated against for exercising any of the aforementioned rights. For example, if a user decides to opt out from the sale of their data by a business, the business may not discriminate in any form—including, but not limited to, denying goods or services to the consumer, charging different rates for goods or services, etc. Embedded within is a right to post-facto opt out of personal data collection. Personal data ownership should stay with the individual and be conceived as being "on loan" to the third party which can be recalled at any time.[11]

Mechanically, these rights would work as follows. Businesses would need to provide two methods for users to submit requests for the rights enumerated above. This could include an email address, hard copy form, landing page, toll-free phone number, etc. Using any of these methods, a user could request the deletion of personal information, for example, and the business would be required to respond to the request within 45 calendar days. The only right that varies mechanically is the right to opt out of the sale or sharing of personal information. The Texas digital bill of rights would require that businesses provide a clear and easily accessible link for users to submit an opt-out request. If a business meets the threshold for application of the law, not complying with a conspicuous link would be considered a violation.

## Application

Carefully crafting the scope and application of the Texas digital bill of rights is key to both protecting the private property of Texans, while ensuring undue harm does not impact small businesses. This legislation would apply to for-profit businesses that conduct business in Texas, have more than 50 employees, and collect personal identifying information of more than 5,000 individuals, households, or devices. In addition, businesses satisfying one of the following thresholds fall under the purview of the act: a business with annual gross revenue exceeding $25 million or that

[11] The effect of a digital bill of rights is a recognition of data as an individual private property right, with a prescribed set of protections for this right. A non-discrimination clause is an important safeguard for consumers because the enumerated protections could effectively be neutralized.

However, this suggestion is a bonus consideration because it presents constitutional questions that need further exploration. The state has a legitimate interest in protecting consumers from unfair, deceptive, and discriminatory business practices. For example, the California Consumer Privacy Act's non-discrimination provision is still enforced in California. How such a provision in a Texas digital bill of rights squares with state, federal, and case law is something that could be considered by the courts if the law is challenged.

derives 50% or more of its revenues by processing personal identifying information.

## Enforcement

There are two primary methods of creating a sound enforcement mechanism. The first is to grant the attorney general broad enforcement powers to bring an enforcement action against entities that violate the act. Civil penalties occur if a business violates any of the individual rights or data practices required in such legislation and fails to rectify the issue within an allotted 30-day "cure period." As in other states, the attorney general would send notices of noncompliance to businesses allegedly in violation of the law, and the business would receive 30 days to cure the issue lest they face penalties. Failure to cure in a timely fashion would result in steep penalties per violation. This applies to violations of any component of the act.[12] Fines received by the state will go into the General Fund. Additionally, once businesses in Texas have a strong understanding of their obligation under a digital bill of rights, the goal would be to sunset the "cure period" provision after five years of the law being active. This provides businesses a reasonable window to operationally comply with the act.

The second mode of enforcement is a private right of action. This mechanism is crucial to reflect the reality that data privacy is a matter of property rights, affording users a way to redress grievances directly and seek remedy for harm. In instances where security breaches impact certain sensitive categories of personal information—which are caused by the failure of a business to incorporate appropriate security measures—a private right of action would allow individual plaintiffs (or a class) to seek statutory damages. Ultimately, this would provide an additional accountability mechanism for businesses to take seriously the sensitivity and privacy of user data. Further, this would put Texans in the driver's seat when it comes to safeguarding their property rights. The damages awarded would be calculated based on actual or statutory damages—whichever is larger. Actual damages should be defined as direct losses incurred from a business's failure to adequately secure user data.

## Conclusion

Data collection has become an increasingly lucrative venture that continually increases in scope as Texans spend more time online and companies become more proficient in refining data harvesting practices. With this coveted commodity, numerous threats have emerged that put Texans in harm's way—often unwittingly. Whether it is data brokers selling personal information for concerning purposes, data breaches that compromise sensitive user information, or invasive surveillance that violates autonomy, there is a real need to enhance the privacy and security of Texans' data.

Passing a digital bill of rights in Texas' 88th Legislature would be a step in the right direction of affording Texans data privacy while protecting an asset that is *their* property. Ultimately, the plan outlined herein takes into account components of other states' bills of rights and the GDPR, incorporating the elements that strengthen these rights for Texans, while omitting those that diminish the potency of such a legislative solution.

Of note, Virginia's digital bill of rights has been criticized for being diluted by special interest groups. It is understandable that companies that derive significant revenue from the status quo model will have concerns with giving control and autonomy to the users. Ultimately, lawmakers should consider all sides of the argument on this issue, as this engenders good public policy. However, the real concerns about privacy raised in this paper are of paramount importance and ought to trump any pecuniary interests.

Finally, in understanding the current strengths, opportunities, weaknesses, and threats associated with big data and how user data is used, it is important to recognize that methods are sure to become more sophisticated. Therefore, the Texas Legislature ought to enact a digital bill of rights while recognizing the need to continuously revisit this issue to find ways to stave off evolving threats to data privacy. ✯

[12] For enforcement of this legislative solution to be successful, financial penalties must be strong enough to incent businesses to adhere to data privacy standards rather than incur the financial penalties and have the fines offset by revenues from violative data collection and sale practices.

## References

Apple. (n.d.). *Augmented reality.* Retrieved June 9, 2022, from https://www.apple.com/augmented-reality/

Associated Press-NORC Center for Public Affairs Research. (2021). *Trust in government is low, but Americans are united around investments in technology.* https://apnorc.org/wp-content/uploads/2021/09/MeriTalk-Omnibus-2021_Report-Formatted_v7.pdf

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

BakerHostetler. (2019). *The California Consumer Privacy Act: Frequently asked questions.* https://www.bakerlaw.com/webfiles/Privacy/2019/Briefs/California-Consumer-Privacy-Act-FAQs.pdf

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

California Office of the Attorney General. (2021, July 19). *Attorney General Bonta announces first-year enforcement update on the California Consumer Privacy Act, launches new online tool for consumers to notify businesses of potential violations.* State of California Department of Justice. https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-first-year-enforcement-update-california

California Consumer Privacy Act. (2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cooper, L. (2022, January 12). How health and fitness trackers are about to get a lot more granular. *The Wall Street Journal.* https://www.wsj.com/articles/how-health-and-fitness-trackers-are-about-to-get-a-lot-more-granular-11641999617

Cox, J. (2016, August 1). *Yahoo 'aware' hacker is advertising 200 million supposed accounts on dark web.* Vice. https://www.vice.com/en/article/aeknw5/yahoo-supposed-data-breach-200-million-credentials-dark-web

Cyphers, B. (2020, March 19). *Google says it doesn't 'sell' your data. Here's how the company shares, monetizes, and exploits it.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

Dhawan, V., & Zanini, N. (2014). Big data and social media analytics. *Research Matters, Issue 18.* https://www.cambridgeassessment.org.uk/Images/465808-big-data-and-social-media-analytics.pdf

European Commission. (n.d.). *What is personal data?* Retrieved June 10, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Facebook. (2022a, January 4). *Cookies & other storage technologies.* https://www.facebook.com/policy/cookies/

Facebook. (2022b, January 4). *Data policy.* https://www.facebook.com/privacy/policy/version/20220104/

FBI. (2020, February 10). *Chinese military hackers charged in Equifax breach.* https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

Fowler, G. (2021, August 29). There's no escape from Facebook, even if you don't use it. *The Washington Post.* https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

Ghostery. (2020). *Tracking the trackers 2020: Web tracking's opaque business model of selling users.* https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users

General Data Protection Regulation, chap. IV, §1, art. 25. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

Google. (n.d.). *Ads and data.* Retrieved June 10, 2022, from https://safety.google/privacy/ads-and-data/#:~:text=Your%20personal%20information%20is%20not,your%20personal%20information%20to%20anyone

Google. (2022, February 10). *Privacy policy.* https://policies.google.com/privacy?hl=en-US

Government Accountability Office. (2013, September). *Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate.* https://www.gao.gov/assets/gao-13-663.pdf

Guynn, J. (2020, January 28). What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy. *USA Today*. https://www.usatoday.com/story/tech/2020/01/28/not- reading-the-small-print-is-privacy-policy-fail/4565274002/

Harwell, D. (2021, November 10). Data broker shared billions of location records with District during pandemic. *The Washington Post*. https://www.washingtonpost.com/technology/2021/11/10/data-broker-shared-billions-phone-location-records-with-dc-government-part-covid-tracking-effort/

Hart, C. & Zick, C. (2021, July 7). *Virginia's new data privacy law: An uncertain next step for state data protection.* JD Supra. https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/#

HB 3741. Introduced. 87th Texas Legislature. Regular. (2021). https://capitol.texas.gov/tlodocs/87R/billtext/pdf/HB03741I.pdf#navpanes=0

HB 3746. Enrolled. 87th Texas Legislature. Regular. (2021). https://capitol.texas.gov/tlodocs/87R/billtext/pdf/HB03746F.pdf#navpanes=0

HB 4390. Enrolled. 86th Texas Legislature. Regular. (2019). https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04390F.htm

Hill, K. (2013, December 19). *Data broker was selling lists of rape victims, alcoholics, and 'erectile dysfunction sufferers'.* Forbes. https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/

Holland, J. (2022, March 24). *Utah privacy bill signed, marking fourth state with such a law.* Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/utah-privacy-bill-signed-marking-fourth-state-with-such-a-law

Keegan, J., & Ng, A. (2022, July 27). *Who is collecting data from your car?* The Markup. https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car?

Kerry, C. & Chin, C. (2020, January 6). *Hitting refresh on privacy policies: Recommendations for notice and transparency.* Brookings. https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/

Koley Jessen. (2021, July 8). *Colorado enacts privacy act, becoming third state with comprehensive privacy law.* https://www.koleyjessen.com/newsroom-publications-colorado-enacts-privacy-act

KPMG. (2021, August). *Corporate data responsibility: Bridging the consumer trust gap.* https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html

Latto, N. (2020, October 29). *Data brokers: Everything you need to know.* Avast. https://www.avast.com/c-data-brokers

Legislative Analyst's Office. (n.d.). *Proposition 24.* Retrieved June 10, 2022, from https://lao.ca.gov/BallotAnalysis/Proposition?number=24&year=2020#main-content

Lima, C. (2022, July 26). Pelosi in a bind as California leaders object to federal privacy bill. *The Washington Post*. https://www.washingtonpost.com/politics/2022/07/26/pelosi-bind-california-leaders-object-federal-privacy-bill/

LMG Security. (2022, January 4). *What hackers do with stolen data & how to reduce your risk after data is taken.* *https://www.lmgsecurity.com/what-hackers-do-with-stolen-data-how-to-reduce-risk-after-data-is-taken/*

Lomas, N. (2022, June 29). *Google's 'deceptive' account sign-up process targeted with GDPR complaints.* TechCrunch. https://techcrunch.com/2022/06/29/google-account-gdpr-complaint/

Lubin, G. (2012, February 16). *The incredible story of how Target exposed a teen girl's pregnancy.* Business Insider. https://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2

Macnish, K. & Galliott, J. (2020). *Big Data and democracy.* Edinburgh University Press.

Mahoney, M. (2020, October 1). *California Consumer Privacy Act: Are consumers' digital rights protected?* Consumer Reports. https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

Moomaw, G. (2021, March 30). *Virginia's new big tech-backed data privacy law is the nation's second. Critics say it doesn't go far enough.* Virginia Mercury. https://www.virginiamercury.com/2021/03/30/virginias-new-big-tech-backed-data-privacy-law-is-the-nations-second-critics-say-it-doesnt-go-far-enough/

Ng, A. (2019, April 9). *Facebook still tracks you after you deactivate your account.* CNET. https://www.cnet.com/news/privacy/facebook-is-still-tracking-you-after-you-deactivate-your-account/

O'Hara, K. (2020). *Big Data and Democracy: Big Data, Consequentialism, and Democracy.* Edinburgh University Press.

Pegoraro, R. (2020, October 8). *The real problem wasn't Cambridge Analytica, but the data brokers that outlived it.* Forbes. https://www.forbes.com/sites/robpegoraro/2020/10/08/the-real-problem-wasnt-cambridge-analytica-but-the-data-brokers-that-outlived-it/

Raether, R., Taylor, A. & Mirza, S. (2021, August 6). *Top takeaways from a year of CCPA enforcement.* Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/top-takeaways-from-a-year-of-ccpa-enforcement

Risk Based Security. (2022, February 4). *Data breach report: 2021 year end.* https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/

Salas, E. (2020, December 8). My son was killed because I'm a federal judge. *The New York Times*. https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html

SB 6. Enrolled. Connecticut General Assembly. (2022) https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

SB 15. Enrolled. 87th Texas Legislature. Regular. (2021) https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SB00015F.pdf#navpanes=0

SB 21-190. Enrolled. 72nd Colorado General Assembly. Regular. (2021) https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

SB 1392. Enrolled. 161st Virginia General Assembly. Special Legislative Session I. (2021) https://lis.virginia.gov/cgi-_bin/legp604.exe?212+ful+CHAP0036+pdf

Segal, T. (2022, March 28). *Big data.* Investopedia. https://www.investopedia.com/terms/b/big-data.asp

State of California Department of Justice. (n.d.). *CCPA enforcement case examples.* Retrieved June 22, 2022, from https://oag.ca.gov/privacy/ccpa/enforcement

Slynchuk, A. (2021, July 22). *Big brother brands report: which companies might access our personal data the most?* Clario. https://clario.co/blog/which-company-uses-most-data/

Statista Research Department (2022, May 23). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025*. Statista. https://www.statista.com/statistics/871513/worldwide-data-created/

Statista Research Department. (2022, July 7). *Do you collect personal data from data subjects in any of the following regions and countries?* Statista. https://www.statista.com/statistics/1172965/firms-collecting-personal-data/

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

U.S. Const. amend. V.

Usercentrics. (2021, October 19). *Colorado Privacy Act – an overview*. https://usercentrics.com/knowledge-hub/colorado-privacy-act/

Vaughn, B. & Paylor, B. (2021, September 15). *2022-2023 state budget*. Texas Department of Information Resources. https://dir.texas.gov/sites/default/files/2021-09/87th%20Legislative%20Session%20Wrap%20up%20FINAL.pdf

Verizon. (2022). *Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Valdetero, J. & Zetoony, D. (2022, March 7). *CCPA ligation up 44.1%*. National Law Review. https://www.natlawreview.com/article/ccpa-litigation-441#:

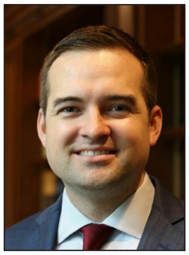
Vigderman, A., & Turner, G. (2022, March 23). *The data big tech companies have on you*. Security.org. https://www.security.org/resources/data-tech-companies-have/

Wolford, B. (n.d.). *What is GDPR, the EU's new data protection law?* GDPR.EU. Retrieved June 15, 2022, from https://gdpr.eu/what-is-gdpr/

## ABOUT THE AUTHORS

**David Dunmoyer** is the campaign director for Better Tech for Tomorrow and serves as the chief of staff for the Foundation's executive team. He has been with TPPF since 2020, and applied his two years of experience working in public affairs in Sacramento, California, where he worked issues ranging from transportation to technology. He is currently pursuing his Master of Public Affairs from the University of Texas at Austin's LBJ School of Public Affairs with an emphasis in technology policy and public finance.

David has a BA in strategic communication from Texas Christian University and despite his current ties to UT, considers himself a Horned Frog first. When he's not working to bring sound technology policy to the Lone Star State or studying for his classes you can find him playing guitar, reading, or exercising.



**The Honorable Zach Whiting** is senior fellow of technology policy and policy director for Better Tech for Tomorrow at the Texas Public Policy Foundation.

Prior to joining the Foundation, he served as a state senator in his native state of Iowa. In the senate, Zach championed conservative values, protected personal liberties, and worked to reduce the size and scope of government. He served as assistant majority leader, chair of the Labor and Business Relations Committee, and vice chair of the Administrative Rules Review Committee.

Prior to the senate, Zach worked as a legislative assistant and policy advisor to a member of Congress. He graduated summa cum laude with a B.A. in political science from Stetson University and earned a J.D. from the Regent University School of Law.

## About Texas Public Policy Foundation

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

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

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

Texas Public Policy Foundation

901 Congress Avenue | Austin, Texas 78701 | 512.472.2700 | www.TexasPolicy.com