Florida TaxWatch

Who Knows What?

An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida

October 2021

106 North Bronough Street, Tallahassee, FL 32301 floridataxwatch.org o: 850.222.5052 f: 850.222.7476

Senator George S. LeMieux
Chairman of the Board of Trustees

Dominic M. Calabro
President & Chief Executive Officer

Dear Fellow Taxpayer,

From smartphones to laptops, fitness trackers to smart thermostats, the world has become more data-oriented and connected than ever before. Due to the rise in innovative technologies, data privacy has become a focal point for legislation around the U.S. and abroad. These laws seek to provide consumers with certain rights regarding their personal information while also requiring businesses to take certain steps to protect privacy related to collecting, processing, sharing, or selling consumer data.

During the 2020-2021 Florida legislative session, Florida TaxWatch released a research brief that analyzed the potential cost of enacting certain consumer data privacy protections in Florida. While not a critique of privacy provisions themselves, the report estimated that compliance costs for the bills as initially introduced would surmount $36.5 billion in initial costs and between $301 million and $9.7 billion in ongoing costs over the next ten years. The estimates were preliminary findings that sought to raise attention about the potential economic impacts and unintended consequences of data privacy. Notably, the brief found compliance would have a disproportionate impact on small and medium-sized businesses.

Thanks in part to Florida TaxWatch's participation last year, the consumer data privacy legislation witnessed several changes to the bill language that effectively raised thresholds and lowered the burden on small to medium-sized businesses. By the end of legislative session, TaxWatch helped to ensure taxpayers were not unduly harmed.

Florida TaxWatch undertakes this updated, independent assessment to better understand the economic impacts that consumer data privacy legislation would have in Florida. The report details the individual cost components that would comprise compliance activities. Building upon the previous research brief, this report calculates the potential economic cost of litigation that a private right of action would produce. The recommendations contained at the end of the report provide policymakers with some key considerations to minimize adverse outcomes while attaining the core goal of data privacy.

Florida TaxWatch is pleased to present this report and its findings and looks forward to working with policymakers, industry leaders, and stakeholders during the present legislative session and beyond.

Sincerely,

Dominic M. Calabro

Dominic M. Calabro
President & Chief Executive Officer

Contents

Executive Summary

Drawn from everyday consumer interactions, digital information has become a pervasive part of the modern economy. Underpinning this explosion of digital data is the availability of personal information—traditionally understood to cover categories of information such as names, addresses, passwords, social security numbers, credit cards, and more. Due to new technologies, personal information has become decidedly broader and more complicated to define, encompassing new areas such as engagement and attitudinal data that provide insights on customer behavior.

Addressing the perceived need for consumer data privacy, governments across the world have begun extensively legislating on the safe handling and protection of personal information. At the center of most of this legislation is the principle that consumers should be afforded certain rights regarding how their personal data is used, such as the ability to know, correct, delete, or opt-out of the sale of personal information. Given differing interpretations of what exactly constitutes "personal information," however, consumer data privacy legislation has produced numerous technical complexities and direct costs for covered businesses.

The Florida Legislature has endeavored to pass substantive consumer data privacy legislation. Although more detailed than presently described, the efforts would grant consumers certain rights, require a covered business to follow certain obligations regarding the use of personal data, and provide for an enforcement mechanism. Based on specified threshold requirements, only certain businesses would be required to comply, but failure to do so would conceivably lead to some statutory remedy or potential civil litigation. Compliance would require some companies to hire additional staff, build out IT infrastructure, improve security safeguards, and more.

Florida TaxWatch analyzed the potential costs of compliance and litigation that would result from a consumer data privacy law in Florida and estimated the following based on various assumptions:

- The direct cost of initial compliance is estimated to be between $6.2 billion and $21.0 billion for the state of Florida;
- The direct cost of ongoing compliance is estimated to be between $4.6 billion and $12.7 billion annually for the state of Florida; and
- If included, a private right of action provision is estimated to produce more than 80 class-action lawsuits initially and exceed $4.2 billion in litigation costs. This amount would be expected to grow over time due to more compliance difficulties, enforcement actions, and number of cases.

There are also several non-quantifiable considerations and secondary effects that are worth noting. Even if small to mid-sized businesses are not primarily covered under a consumer data privacy law, they may still feel compelled to adopt data privacy measures to remain competitive, despite many having fewer resources than larger firms. This outcome would create an unintended competitive advantage for larger businesses and create a market expectation for many smaller businesses. Additionally, inferences and probabilistic identifiers—potential categories in consumer data privacy legislation—create practical difficulties for companies to comply and therefore raise the potential cost of litigation.

To minimize the economic costs of consumer data privacy legislation while achieving the goal of strengthening privacy protections, passing a comprehensive federal consumer data privacy law would be the ideal course of action. Such a federal law would supplant a patchwork of state laws and standardize consumer rights, business obligations, and enforcement mechanisms across all fifty states. In the absence of a federal framework, however, legislative measures such as omitting a private right of action or delaying an implementation date to 2024 or beyond would be preferable options to reduce potential compliance and litigation costs.

Introduction

Data-driven products and services have become ubiquitous in the 21st century, marked by steady advancements in information technologies over the past two decades. Harnessing the power of big data, digital innovation has spurred connectivity and productivity for many portions of the economy, transforming how businesses and consumers go about their daily routines. Even as the technical capabilities to collect, store, and process large quantities of information expand, these new technologies provoke considerations about privacy and protection for many consumers.

Despite the pervasiveness of data-directed technologies, many individuals have voiced their concerns over privacy in recent years. According to the Pew Research Center, some 81 percent of U.S. adults feel they had very little control over the data that companies collect about them and 79 percent indicate they are concerned about how their data are used.[1] Around seven in ten adults report feeling worried that their personal information is less secure than in previous years; however, very few admit fully paying attention to privacy policies and terms of service.[2] Although overall sentiment tends to evidence concern, consumers express greater trust in the healthcare and financial services industries to protect their data and privacy.[3] Consumers express greater trust in industries that have an extensive history with federal regulations overseeing the handling of personal information.

In response to the perceived need for consumer data privacy, governments around the world have increasingly begun passing comprehensive data privacy legislation. The European Union passed the General Data Protection Regulation ("GDPR") in 2016 to regulate how businesses handled personal information. Following its passage, the GDPR became a basic framework for similar consumer data privacy legislation in other countries, including Brazil, Japan, South Korea, Argentina, and Chile.[4] Notably absent, the U.S. has not passed federal legislation regulating consumer data privacy in the same form as other countries, leaving the onus to individual states to pass laws regulating personal information use.

Enacted in 2018, the California Consumer Privacy Act ("CCPA") became the first consumer data privacy legislation to pass in the U.S. The seminal law provided a framework for citizens to exercise certain rights over their data, such as the ability to know, delete, and opt-out of the sale of personal information. Furthermore, the CCPA applied to businesses meeting certain threshold requirements and prescribed a private right of action relating to data breaches. A few years later, in 2021, Virginia passed the Virginia Consumer Data Protection Act ("VCDPA"), borrowing various provisions from the GDPR and CCPA. Finally, in the middle of 2021, Colorado joined California and Virginia as the third U.S. state to pass comprehensive data privacy legislation, enacting the Colorado Privacy Act ("CPA").

During the 2020-2021 Florida legislative session, lawmakers introduced legislation—House Bill (HB) 969 and Senate Bill (SB) 1734—that would have instituted consumer data privacy. Similar to other states, the bills stipulated certain rights for consumers, including the right to access personal information collected, the right to delete or correct personal information, and the right to opt-out of the sale or sharing of personal information.[5] Additionally, the bills would have required companies to publish privacy policies on their respective websites. Beyond what other states had previously done, however, Florida's two bills contained additional provisions that would have required businesses to address inferences drawn from consumers and probabilistic identifiers. Companies meeting certain thresholds would fall under the privacy law and would need to comply.[6] The Senate and House bills ultimately diverged in the enforcement mechanism, with the House version prescribing a private right of action for consumers if companies did not address consumer requests relating to deleting, correcting, selling, or

1 Pew Research Center, "Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information," Nov. 15, 2019.

2 Ibid.

3 McKinsey & Company, "The consumer-data opportunity and the privacy imperative," Apr. 27, 2020.

4 European Data Protection Supervisor, "The History of the General Data Protection Regulation," Accessed Aug. 27, 2021.

5 Florida House of Representatives, Staff Analysis for CS/CS/CS/HB 969, Released: Apr. 16, 2021.

6 Ibid.

sharing.[7] By the end of the legislative session, the bills did not pass but raised substantive questions about the respective costs for compliance and potential litigation if consumer data privacy were to pass in Florida.[8]

Florida TaxWatch undertakes this independent assessment to estimate the potential compliance and litigation costs of implementing consumer data privacy legislation in Florida. The analysis begins with a brief comparative analysis to highlight existing consumer data privacy laws in Europe and other U.S. states, drawing attention to key differences and some implementation experiences. Finally, the report provides future recommendations to both achieve the intended goals of consumer data privacy and minimize the potential unintended consequences and costs.

Consumer Data in the 21st Century

From gauging consumer satisfaction to conducting predictive analytics, companies have captured, stored, and analyzed consumer data for various reasons. The information is often used to better understand daily operations, make informed business decisions, or share materials with an outside party. Regardless of the intended use, there has been a proliferation of quantitative and qualitative consumer data in tandem with newer smartphone, computer, and other digital technologies.

Broadly speaking, the types of consumer data that businesses often use are:[9]

- Personal Data: Personally identifiable information, such as names, Social Security numbers, driver's licenses, email addresses, passwords, and non-personally identifiable information, including web browser cookies, device identifiers (IDs), and Internet Protocol (IP) addresses;
- Engagement Data: How consumers interact with a business's website, mobile apps, messages, social media, emails, paid ads, and more;
- Behavioral Data: Transactional details, including past purchases, interactions, and qualitative data (e.g., mouse movement information); and
- Attitudinal Data: Consumer satisfaction, product reviews, product desirability, and more.

Public policies regarding consumer data often fall under two categories: security and privacy. Even though the terms are interconnected and often used interchangeably, data privacy deals more with how companies collect, use, and share personally identifiable information. Data security contends with how companies protect personal information from unauthorized access or use, including the necessary safeguards to prevent large-scale breaches.[10] Although federal and state governments have previously passed legislation addressing data security, often targeted toward certain industries (e.g., healthcare, financial, education), states have only recently begun legislating consumer data privacy extensively.[11]

Consumer Data Privacy Laws in Europe and Other U.S. States

General Data Protection Regulation (GDPR)

In 2016, the European Union (EU) passed a broad consumer data privacy law outlining consumer rights regarding their personal information. Becoming effective in 2018, the GDPR unified the regulatory approach across EU member nations and has since served as the basis for similar legislation in other countries.[12] Personal data are at the core of the EU's GDPR, which broadly include any piece of information that relates to an identifiable person.

7 Klein, Moynihan, Turco, "Florida Privacy Law Runs Out of Time," May 4, 2021.

8 Florida TaxWatch, "Florida Proposed Privacy Protection Act," Mar. 29, 2021.

9 Business News Daily, "How Businesses Are Collecting Data (And What They're Doing With It)," Jun. 17, 2020. Referenced in Florida House of Representatives, Staff Analysis for CS/CS/CS/HB 969, Released: Apr. 16, 2021.

10 Varonis, "Data Privacy Guide: Definitions, Explanations, and Legislations," Sept. 28, 2020. Referenced in Florida Senate, Staff Analysis for CS/CS/SB 1734, Released Apr. 7, 2021.

11 Congressional Research Service, "Data Protection Law: An Overview," Mar. 25, 2019.

12 GDPR.EU, "What is GDPR, the EU's new data protection law?" Accessed on Sept. 1, 2021.

Examples include a person's name, location, or online usernames; even less apparent identifiers, such as IP addresses and cookie identifiers, fall under the GDPR's definition of personal data.[13]

The GDPR applies to any company or entity that processes personal data as part of its activities, even if the company or entity is located outside the EU but services EU citizens. Unlike subsequent data laws, the EU's GDPR does not have specific threshold requirements for companies to meet to fall under the law's provisions. The far-encompassing nature makes the GDPR applicable to many large, medium, and small-sized businesses across the EU and elsewhere.[14] The GDPR distinguishes between "controllers" and "processors" of personal data—controllers exercise control over the means and purposes of processing personal data, whereas a processor works on behalf of a relevant controller.[15]

Businesses that fall under the GDPR must ask consumers for explicit permission before collecting or processing personal data. The language must be clear and not hidden within dense legalese or terms of condition.[16] At the consumer's request, companies must confirm whether personal data are being processed, where it is being processed, and for what purpose. Companies must provide the consumer with a free electronic copy of the personal data being processed upon request. Under the GDPR, covered companies must also erase any personal data when asked to do so by the specific consumer. After that request, companies must cease any further processing or dissemination of the data.[17] Companies that fail to comply with the EU's GDPR are fined in proportion to their annual revenue, and data subjects have the right to seek compensation from such organizations for material damages.[18]

Since its implementation, the GDPR has led to several unintended consequences and costs. Given the law's wide application, regardless of company revenue or size, the law has produced high compliance costs across the economy. Medium-sized businesses spent close to $3 million in 2017-2018 to come into compliance, and regulatory costs reached $16 million for an average U.S. Fortune 500 company.[19] The law has disproportionately affected many small businesses, forcing many companies out of the EU market.[20] According to one study, the GDPR has had a chilling effect on investment, reducing weekly venture deals by 17.6 percent and negatively impacting new startup companies.[21] Failure to comply has also produced substantial fines for many companies across the EU. From May 2018 to January 2020, GDPR fines totaled $139 million; however, in just one year, total GDPR fines reached $332 million by January 2021.[22]

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

California became the first state in the U.S. to pass comprehensive data privacy legislation similar in form to the EU's GDPR. In 2018, California passed the CCPA to give consumers more control over their personal information. The CCPA defines personal information as any "information that identifies, relates to, or could reasonably be linked with, a particular consumer or household."[23] Based on the law, personal information can include a person's name, social security number, email, past purchases, internet browsing history, biometrics, geolocation, and even inferences from other personal information that can create a profile about preferences or characteristics.[24]

13 Wired, "What is the GDPR? The summary guide to GDPR compliance in the UK," Mar. 25, 2020. Referenced in Florida House of Representatives, Staff Analysis for CS/CS/CS/HB 969, Released: Apr. 16, 2021.

14 European Commission, "Who does the data protection law apply to?" Accessed Sept. 1, 2021.

15 Ibid.

16 U.K. Information Commissioner's Office, Guide to General Data Protection Regulation: Consent, Accessed Sept. 1, 2021.

17 TechRepublic, "GDPR: A Cheat Sheet," May 23, 2019. Referenced in Florida Senate, Staff Analysis for CS/CS/SB 1734, Released Apr. 7, 2021.

18 GDPR.EU, "What are the GDPR fines?" Accessed on Sept. 1, 2021.

19 George Washington University, "Unintended Consequences of GDPR: A Two-Year Lookback" Sept. 2, 2020.

20 Ibid.

21 National Bureau of EcoBlonomic Research (NBER), "The Short-Run Effects of GDPR on Technology Venture Investment," Nov. 2018.

22 DLA Piper, DLA Piper GDPR Fines and Data Breach Survey: January 2021, Accessed Sept. 1, 2021.

23 State of California Department of Justice, "California Consumer Privacy Act (CCPA)," Accessed Sept. 1, 2021.

24 Ibid.

According to the California Department of Justice, the CCPA provided California consumers with the following rights:[25]

- The right to know about the personal information a business collects, specifically about the consumer, and how it is used and shared;
- The right to delete personal information collected from them;
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

Unlike the GDPR, the CCPA only applies to for-profit businesses meeting certain thresholds. The CCPA applies to businesses meeting one or more of the following: (1) has a gross annual revenue of over $25 million; (2) buys, sells, or shares the personal information of 50,000 or more California residents, households, or devices; or (3) derives 50 percent or more of their annual revenue from selling California residents' personal information. Enforcing the law, California's Attorney General can fine non-compliant companies. Further, consumers may bring a private right of action against businesses when nonencrypted or nonredacted personal information is stolen in a data breach incident.[26]

The CPRA passed in 2020 as a statewide proposition, set to amend portions of the previously passed CCPA that went into effect on January 1, 2020. The CPRA established a dedicated office to handle concerns with the CCPA and provide consumers with new rights to prevent businesses from sharing information, correct inaccurate information, and limit the use of sensitive personal information. The CPRA also doubled the CCPA's threshold from 50,000 to 100,000 households to reduce the potential applicability to small and mid-sized businesses.[27]

Comparative to experiences after the GDPR's implementation, the passage of the CCPA resulted in compliance costs for many businesses in California. According to an economic impact assessment, California's privacy law was estimated to cost $55 billion in initial compliance costs.[28] The report also found that total costs from ongoing compliance could cost between $467 million and more than $16 billion over the next decade, with small firms facing a disproportionate share of compliance costs given fewer legal and technical resources.[29] The differential experiences between large and small firms is worsened by the fact many large companies have previous experience coming into compliance with the EU's GDPR, giving them a head start on the compliance front. Since the CPRA will not go into effect until January 1, 2023, it remains to be seen how the CPRA's modifications will affect future compliance costs.

Already being witnessed to some extent, extensive use of the CCPA's private right of action is a costly outcome of the law's implementation. Under the CCPA, individual consumers can seek damages between $100 and $750 per consumer per incident in instances when personal information is subject to a data breach. Between January 2020 and July 2021, there have been 141 class-action cases filed under the CCPA's private right of action provision.[30] Although the CCPA (and CPRA) only allow a private right of action under data breach incidents, this has not stopped consumers from filing claims under alleged violations of the law's other provisions dealing with knowing, deleting, or correcting personal information.

Virginia Consumer Data Protection Act (VCDPA)

Signed into law on March 2, 2021, Virginia's VCDPA became the nation's second comprehensive data privacy legislation following California. According to the VCDPA, personal data (instead of the term "personal information" used in the CCPA) refers to "any information that is linked or reasonably linkable to an identified or identifiable natural person."[31] The term does not apply to de-identified

25 State of California Department of Justice, "California Consumer Privacy Act (CCPA)," Accessed Sept. 1, 2021.

26 Ibid.

27 Bloomberg Law, "CCPA vs CPRA: What's the Difference?" July 13, 2021.

28 Berkeley Economic Advising and Research, LLC (Prepared for State of California Department of Justice), Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, Aug. 2019.

29 Ibid.

30 Perkins Coie, CCPA Litigation Tracker, Accessed Sept. 1, 2021.

31 Gibson Dunn, "Virginia Passes Comprehensive Privacy Law," Mar. 8, 2021.

data,[32] publicly available data, or pseudonymous data.[33] Set to come into effect on January 1, 2023, the VCDPA shares many of the same provisions found in the CCPA, especially as it relates to prescribed consumer rights.

The VCDPA provides individuals with the following consumer rights:[34]

- The right to access whether a controller is processing personal data about the consumer;
- The right to correct any inaccuracies in the consumer's personal data;
- The right to delete any personal data concerning the consumer;
- The right to opt-out of the processing of personal data for targeted advertising, sale, or profiling;
- The right to data portability to obtain a copy of the consumer's personal data in a portable, readily usable format; and
- The right to appeal a controller's refusal to take action on a request.

Similar to the CCPA, the VCDPA has several threshold requirements for businesses to fall under the law's provisions. Unlike the CCPA, however, the VCDPA does not have a revenue threshold, making the law less expansive in scope. The VCDPA applies to entities that conduct business in Virginia, produce products or services targeted toward residents, and control or process personal data of at least (1) 100,000 consumers during the calendar year or (2) 25,000 consumers and derive 50 percent of gross revenue from the sale.[35] The VCDPA is also slightly more limited in scope because it does not apply to particular entities.

Specifically, financial service companies that comply with the Gramm-Leach-Bliley Act ("GLBA"), healthcare companies that comply with the Health Insurance Portability and Accountability Act ("HIPAA"), nonprofits, and institutions of higher education are explicitly exempt from the law.[36]

Several other key differences exist between the VCDPA and the CCPA (as amended by the CPRA). Unlike the CCPA, which applies to employee data, the VCDPA specifically excludes individuals who are acting in an employment context, such as job applicants and current employees. The VCDPA also addresses "sensitive data"[37] and prohibits businesses from collecting sensitive data without prior consumer consent. Originally, the CCPA did not maintain a separate category for sensitive data; however, the CPRA rectified the issue by defining a separate category for "sensitive personal information."[38] Quite significant, the VCDPA does not have a private right of action if the law is violated—a substantive difference from the CCPA. Exclusive enforcement belongs to Virginia's attorney general, who can initiate certain penalties for companies after a statutory cure period.[39]

Overall, the VCDPA is less prescriptive than its predecessors and has been able to benefit from past experiences with other consumer data privacy legislation. Unlike in Europe and California, Virginia's data law received support from various industry groups for its less onerous compliance requirements. Additionally, the VCDPA's effective date on January 1, 2023, provides businesses with more time to come into compliance and avoid potential violations. Coupled with the benefit of advance preparation, the lack of a private right of action is another factor that has further yielded broad business and bipartisan support.[40]

32 "De-identified" means information that cannot be reasonably used to infer information about or otherwise be linked to a particular consumer or a device that belongs to the consumer.

33 "Pseudonymous data" is a GDPR borrowed term that refers to personal data that cannot be attributed to an individual without the use of additional information.

34 JDSupra, "Virginia is for lovers (of privacy) – The Consumer Data Protection Act passes into law," Mar. 5, 2021.

35 Virginia Legislative Information System, SB 1392: Consumer Data Protection Act Bill Text, Accessed Sept. 1, 2021.

36 Ibid.

37 "Sensitive data" is a category of personal data that includes: racial or ethnic origin, religious beliefs, mental or physical health diagnoses, sexual orientation, citizenship or immigration status, genetic or biometric data, personal data collected from a child, and precise geolocation data.

38 Cleary Gottlieb Steen & Hamilton LLP, "The 'New' Dominion of Privacy Law: Virginia Becomes Second State to Pass Comprehensive Consumer Data Privacy Act," Apr. 14, 2021.

39 Harvard Journal of Law & Technology, "Virginia's New Consumer Data Protection Act: Will Others Follow?" Mar. 16, 2021.

40 JDSupra, "Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection," July 7, 2021.

Colorado Privacy Act (CPA)

With the passage of the CPA, Colorado became the third state in the nation to enact some comprehensive data privacy law on July 7, 2021.[41] Comparable to the California and Virginia iterations, the CPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual," excluding de-identified or publicly available information.[42] The CPA also carves out a separate definition for sensitive data. In an effort to ensure companies have adequate time to comply, the CPA will go into effect on July 1, 2023.[43]

Under the CPA, consumers are afforded the following rights, which are very similar to laws in other states:[44]

- The right to access whether a controller is processing personal data about the consumer;
- The right to correct any inaccuracies in the consumer's personal data;
- The right to delete any personal data concerning the consumer;
- The right to opt-out of the processing of personal data for targeted advertising, sale, or profiling;
- The right to data portability to obtain a copy of the consumer's personal data in a portable, readily usable format; and
- The right to appeal a controller's refusal to take action on a request.

Reflective of established thresholds in other states, the Colorado consumer data privacy law only applies to entities that conduct business in Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more Colorado residents in a year, or (2) derives revenue from the sale of personal data and processes or controls the personal data of 25,000 or more consumers.[45]

The CPA's scope is slightly larger than the VCDPA given the application to businesses that may derive less than 50 percent of revenue from selling personal data and smaller than the CCPA's scope due to the absence of any standalone gross revenue requirement.[46]

The CPA also establishes several categories of exemptions that can be broken down into entity-level and data-level exemptions. In Colorado, higher education institutions and financial entities regulated by the GLBA are exempt; however, unlike in Virginia, health entities under HIPAA regulations are not exempt.[47] Dealing with enforcement, the CPA allows the state attorney general along with district attorneys to enforce the consumer data privacy law. This departs from the VCDPA in that the law allows district attorneys to participate. There is no private right of action provision under the CPA.[48]

To compare the four consumer data privacy laws discussed in this section, Table 1 on the next page provides a brief overview of the main similarities and differences between the four laws. Although the technical details in each law may vary in detail, language, and scope, each law provides certain consumer rights regarding their personal information, duties for controllers and processors to follow, and some enforcement mechanism. The private right of action and the amount of time to come into compliance have an important bearing on potential compliance and litigation costs for companies, as will be described in greater detail later. As such, it is important to note that only the EU's GDPR and California's CCPA (CPRA) allow a private right of action.

Other State Efforts

As of late September 2021, only three states in the U.S. have enacted a comprehensive consumer data privacy law: California, Virginia, and Colorado. Despite the seemingly small footprint, state-level momentum for consumer data privacy bills is at an all-time high, according to the International Association of Privacy Professionals (IAPP).[49] Based on the state privacy tracker, in 2021, twenty-one states have at least considered some form of

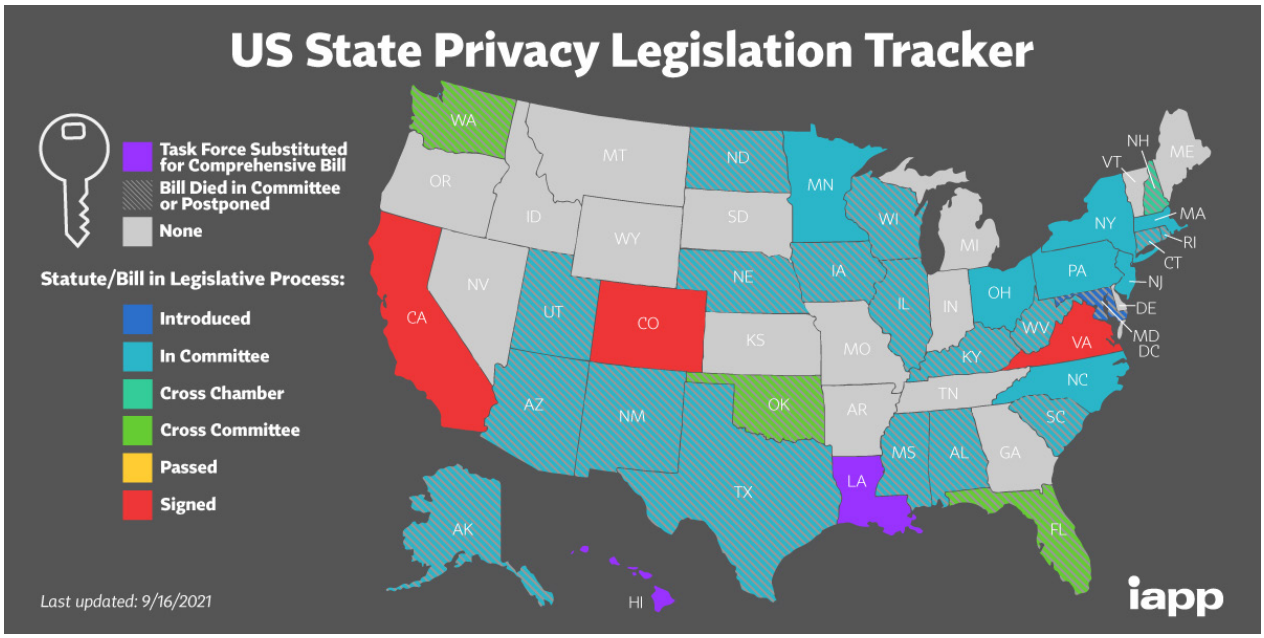
41 Colorado General Assembly, "SB 21-190: Protect Personal Data Privacy Bill Text," Accessed Sept. 1, 2021.
42 Ibid.
43 Ibid.
44 International Association of Privacy Professionals (IAPP), "Colorado Privacy Act Becomes Law," July 8, 2021.
45 Akin Gump, "Colorado Privacy Act: What Businesses Need to Know," July 26, 2021.
46 International Association of Privacy Professionals (IAPP), "Colorado Privacy Act Becomes Law," July 8, 2021.
47 Ibid.
48 Colorado General Assembly, "SB 21-190: Protect Personal Data Privacy Bill Text," Accessed Sept. 1, 2021.
49 International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker, Accessed Sept. 1, 2021.

Table 1. Comparison of Consumer Data Privacy Laws in EU and the U.S.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA
Right to opt-out of sale	✗	✓	✓	✓
Opt-in/opt-out for sensitive information	Opt-in	Opt-out	Opt-in	Opt-in
Violation cure period	✗	✓	✓	✓
Right to appeal denials of requests	✗	✗	✓	✓
Express obligations regarding de-identified data	✗	✗	✓	✓
Requirement to perform data protection impact assessment	✓	✓	✓	✓
Private right of action	✓	✓	✗	✗
Governmental enforcement entities	Data Protection Authorities (DPAs)	CPPA, Attorney General	Attorney General	Attorney General, District Attorneys
Penalties	Up to €10 million (€20 million), or 2% (4%) of worldwide annual revenue from the preceding financial year, whichever is higher in the case of less severe (more serious) violations.	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors	Up to $7,500 per violation	Up to $20,000 per violation
Operative date	May 25, 2018	January 1, 2023	January 1, 2023	July 1, 2023

Source: Florida House of Representatives Staff Analysis for HB 969 (2021). Table modified and updated by JDSupra and Florida TaxWatch.

Fig. 1. US State Privacy Legislation Tracker



Source: International Association of Privacy Professionals (IAPP)

consumer data privacy, with active bills still in Massachusetts, New York, North Carolina, Ohio, and Pennsylvania (See Figure 1).[50] Over the past year, there have also been various failed attempts to pass data legislation. Without a clear federal framework in place, it can be reasonably expected that more states will consider, and eventually come to pass, substantive consumer data privacy legislation across the U.S.[51] If each state continues to pass their own unique form of consumer data privacy, many businesses will have a challenging time complying with a patchwork of state laws, magnifying compliance and enforcement costs in the end.

Florida's Proposed Data Privacy Legislation

During the 2020-2021 legislative session, Florida entered the consumer data privacy landscape by introducing and considering privacy legislation specific to the Sunshine State. Similar in priority to other state consumer data privacy laws, the two Florida bills—SB 1796 and HB 969—aimed to provide consumers with certain rights over their personal information. The right to access, correct, delete, and opt-out of the sale of personal information were all commonalities between the two bills.

Additionally, compliance obligations for covered businesses included certain responsibilities, such as maintaining an online privacy policy, providing notice before the point of collection, implementing

50 International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker, Accessed Sept. 1, 2021.

51 Ibid.

Table 2. Comparison of Florida Senate and House Consumer Data Privacy Bills (By End of 2020-2021 Legislative Session)

	Florida House of Representatives (HB 969)	Florida Senate (SB 1734)
Consumer Rights	• Right to Know/Access • Right to Correct • Right to Delete • Right to Opt-Out • Right to Data Portability • Right to Non-Discrimination	• Right to Know/Access • Right to Correct • Right to Delete • Right to Opt-Out
Thresholds for Businesses to be Covered by Law	Satisfies two of the following: • Has annual global revenues in excess of $50 million • Annually buys, sells, or shares, personal information of over 50,000 consumers, households, or devices for targeted advertising • Derives 50% or more of global annual revenue from selling or sharing consumer information	Satisfies one of the following: • During a calendar year, controls the processing of the personal information of 100,000 or more consumers who are not covered by an exception. • Controls or processes the personal information of at least 25,000 consumers who are covered by an exception and derives over 50% or more of global annual revenues from selling personal information about consumers.
Compliance Obligations	• Online privacy policy • Notice at collection • Implement reasonable security measures • Respond to, and verify, requests (within 45 days) • Written contracts with service providers/processors • Opt-out links on website • Special protections for minors' data • Educate and train staff	• Online privacy policy • Notice at collection • Implement reasonable security measures • Respond to, and verify, requests (within 30 days) • Written contracts with service providers/processors • Opt-out links on website • Special protections for minors' data • Educate and train staff • Sensitive data
Enforcement	Attorney General Private Right of Action	Attorney General
Operative Date	July 1, 2022	July 1, 2023

Source: Florida TaxWatch; Information from HB 969 and SB 1734 Bill Texts[1]

1 To provide the comparative analysis for the House and Senate data privacy bills, Florida TaxWatch referenced the latest bill languages provided by the respective chambers. It should be noted that for the Florida Senate, TaxWatch used the language found in the strike-all amendment on April 28, 2021 that was subsequently sent back in messages to the House before the end of session.

security measures, and responding to verifiable consumer requests to change personal information. After receiving verifiable requests from consumers exercising their rights, covered businesses would have to respond to the request in a timely manner. Exemptions also tended to overlap between the two bills with both providing express exemption to employment data, personal health information regulated under HIPAA, and personal financial information under the GLBA.[52]

Despite some overlapping elements, the two bills diverged significantly by the end of the legislative session with regards to the business thresholds and enforcement mechanisms. For the Senate, the threshold for businesses to be covered excluded any annual revenue condition, which the House version included for businesses making more than $50 million in gross annual revenue. Most noticeably, the two bills differed in enforcement with the House opting to maintain a private right of action that was based on, but more expansive than, California's CCPA and CPRA's private right of action. In contrast, the Senate bill only allowed the Florida Attorney General to enforce the law's provisions.[53] A more detailed breakdown of key similarities and differences can be found below in Table 2.

Florida's proposed consumer data privacy underwent several changes in content and scope throughout the course of the 2020-2021 legislative session. Despite the various modifications, questions persist about the potential outcomes of implementing comprehensive data privacy in the state of Florida. To what extent consumers derive a benefit from such law, or businesses incur a litigation or compliance cost, depends on a variety of complex factors.

Given that the perceived need for consumer data privacy persists, and news reports indicate that it remains a priority for legislative leaders, Florida TaxWatch undertakes this report to present an updated analysis of consumer data privacy's economic impact in Florida. This analysis begins where legislative action ended last session and takes into account legislative attempts to raise thresholds, effectively reducing the number of small and mid-sized businesses affected. Building upon the previous research brief, this analysis estimates the potential litigation cost stemming from any private right of action. The report serves as a starting point for future conversations on consumer data privacy, and Florida TaxWatch looks forward to evaluating any bills as they are presented and amended.

Estimated Cost of Compliance in Florida

As observed in parts of the U.S. and the EU., consumer data privacy regulations often produce costs for businesses to come into compliance with the law. The same year the GDPR came into effect, a 2018 Ernst & Young and IAPP report found that companies spent an average of $1.3 million per year on compliance costs, including the cost to adapt products, services, IT infrastructure, and hire additional staff.[54] Although there is a dearth of data points for U.S.-based consumer data privacy laws, California's 2019 regulatory impact assessment for the CCPA is the closest source for compliance estimates. For companies coming into compliance with the CCPA, initial aggregate cost estimates averaged $55 billion and ongoing annual costs ranged between $466.9 million and $16.5 billion.[55]

During the 2020-2021 Florida legislative session, Florida TaxWatch released a similar research brief that estimated the potential cost of compliance for passing consumer data privacy legislation in Florida.[56] Based on the bills as initially introduced and incorporating methodology employed in the CCPA assessment, TaxWatch estimated the initial cost of compliance to be around $36.5 billion for Florida businesses. The brief also found that the cost of ongoing compliance over the next decade would range between $301 million and $9.7 billion due to ongoing staffing, training, and IT infrastructure costs. The threshold requirements had a significant bearing on the cost estimates,

52 Florida Senate, CS/CS/SB 1734: Consumer Data Privacy Bill Text, Last Action: Apr. 28, 2021. Florida House of Representatives, CS/CS/CS/HB 969: Consumer Data Privacy Bill Text, Last Action: Apr. 30, 2021. Accessed Sept. 1, 2021.

53 Ibid.

54 International Association of Privacy Professionals (IAPP) and Ernst & Young (EY), IAPP-EY Annual Governance Report 2018, May 25, 2018.

55 Berkeley Economic Advising and Research, LLC (Prepared for State of California Department of Justice), Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, Aug. 2019.

56 Florida TaxWatch, Florida's Proposed Privacy Protection Act, Mar. 2021.

suggesting any respective changes to the legislative framework would alter eventual costs.

To provide an updated analysis with newer compliance cost estimates, this report will consider specific cost components that contribute to a covered firm's overall compliance cost. Factors such as new staffing needs, training requirements, IT infrastructure, response to consumer requests, and data security measures will be incorporated into the following analysis with more specificity than before. Additionally, the updated analysis will incorporate current firm data to yield a more accurate estimate of how many Florida businesses would likely fall under a consumer data privacy law. While the exact compliance cost may vary between firm, industry, and region, it can be reasonably assumed that any such Florida consumer data privacy law would be associated with compliance costs for covered businesses.

Staffing and Training Needs

In response to any new consumer data privacy law, the need for additional staff is one of the clearest and most direct outcomes. The GDPR, for example, required companies to designate data privacy officers (DPOs) to oversee and coordinate compliance activities, leading to a boon in DPO hiring across Europe. In the future, the demand for data privacy professionals will steadily grow as more U.S. states and countries around the world begin to pass substantive data laws.[57] These privacy professionals will increasingly be called upon to oversee compliance activities for companies.

As a lower-bound estimate, this analysis assumes the passage of a Florida consumer data privacy law would lead to companies hiring one data privacy officer (DPO or related title[58]) to oversee a company's data compliance activities. As an upper-bound estimate, the analysis assumes larger companies would warrant the need for a DPO and two additional database administrators to handle the daily operations of managing extensive data warehouses. Similar assumptions are found in a technical report by the Information Technology & Innovation Foundation, which estimated the potential compliance cost for a U.S. federal consumer data privacy law.[59] In another report studying CCPA and GDPR impacts, 90 percent of surveyed organizations hired at least three additional data privacy professionals in response to privacy regulations.[60] These assumptions do not preclude the possibility of a company hiring or needing more (or fewer) privacy professionals, and these internal hires are assumed to be comparable in price to external data consultants.[61]

To quantify the potential employer cost for compensation, the analysis incorporates compensation data from the Bureau of Labor Statistics (BLS). Based on 2020 BLS data, annual salaries would average $107,680 for a DPO and around $98,860 for a database administrator.[62] Accounting for the potential benefits that typically accompany employment (e.g., health insurance, vacation time, retirement), the analysis adds 28 percent on top of the base salaries. This particular rate comes from the BLS average benefit rate for the U.S. south region in 2021.[63] Between salaries and benefits, the total employer cost for compensation is estimated to be between $137,830 and $390,912 due to consumer data privacy.[64]

Moreover, each new hire will need to devote time and training to understand the regulations and learn internal systems. To calculate the cost of training and preparation, this analysis assumes that all employees (the DPO and two database administrators) will each require a minimum of 20

57 International Association of Privacy Professionals (IAPP), "Expect the privacy job market to stay strong, even after the pandemic subsides," Mar. 5, 2021.

58 Titles vary for senior-level officials who oversee a company's data efforts. Comparable job titles include Chief Information Officer, Chief Technology Officer, Chief Privacy Officer, Data Protection Officer, and more. For this report, the title "Data Privacy Officer (DPO)" will be used.

59 Information Technology & Innovation Foundation, The Costs of an Unnecessarily Stringent Federal Data Privacy Law, Aug. 5, 2019.

60 DataGrail, The Age of Privacy: The Cost of Continuous Compliance, Feb. 2020.

61 Due to the wide variability in a company's decision whether to hire external contractors or develop in-house solutions, TaxWatch assumes the costs are roughly comparable for the purposes of this analysis. It should be noted, however, that a firm's size and amount of in-house engineering resources already available will be important factors in the eventual outcome.

62 Bureau of Labor Statistics (BLS), Occupational Outlook Handbook, Accessed Sept. 2, 2021. Note: For the Data Privacy Officer (DPO) salary, the analysis uses the 2020 median pay for a "Top Executive" since the term includes chief executives at companies.

63 Bureau of Labor Statistics (BLS), "Employer Costs for Employee Compensation for the Regions – March 2021," June 17, 2021.

64 To calculate the lower-bound estimate, the base salary for the DPO ($107.680) is increased by 28%: Lower-Bound = 1.28 * $107,680 = $137,830. For the upper-bound estimate, added to the lower-bound estimate are the two base salaries for the database administrators raised by 28%. Upper-Bound = (2 * 1.28 * $98,860) = $253,081.6 + $137,830 = $390,912.

hours for annual training and preparation.[65] The cost to the company is the opportunity cost of the employee's time.[66] Revisiting the base annual salaries mentioned above and finding the hourly wage equivalent, the training cost to the company is expected to be between $1,035 and $2,936 on top of the salary and benefits range above.[67]

For staffing and training requirements, the compliance cost for a single business is estimated to be between $138,865 and $393,848 annually due to a consumer data privacy law.

It should be mentioned, these calculations are the direct costs of employment due to consumer data privacy and do not include additional indirect costs that a company may end up paying for, such as overhead, general and administrative expenses, audits, rent, and utilities. Given these added costs, the range above is a conservative estimate for the staffing and training a company may need for consumer data privacy compliance.

IT Infrastructure and System Processes

In addition to expected hiring needs, companies will need to develop IT infrastructure and build out system processes at the onset to comply with consumer data privacy regulations. Companies will have to ensure IT infrastructure can adequately respond to consumer requests by identifying relevant personal information elements and executing the proper action (e.g. deleting or correcting information) expediently. Companies may also need to conduct data inventories to better understand existing data, identify gaps, and mitigate potential risks across different databases. After changes are made, companies will need to ensure the various servers are properly communicating with each other and that proper data management techniques are maintained for data quality. Together, these actions further affect a company's overall compliance cost.

To ensure companies can properly track, access, correct, or delete personal information, some companies will only need to hire a few specialized data engineers (or consultants) to develop new, or update existing, IT infrastructure. For some larger businesses, there may be an even larger capital investment in specialized technologies to build out data inventory capabilities and secure the integrity of millions of data elements. For this analysis, TaxWatch proxies the lower-bound cost to develop technological systems by incorporating the median annual salary for a data engineer in the U.S. Under this assumption, the economic value of developing sufficient technological infrastructure is intrinsically related to the amount of time an engineer (or outside consulting company) spends working. For the upper-bound estimate, the analysis references a report by the Ponemon Institute, which examined the average cost of specialized IT investments for large organizations in response to GDPR.[68]

Based on the BLS occupational wage data, in 2020, the median annual salary for a data engineer was $126,830.[69] As a lower-bound estimate, the analysis assumes companies require the time and resources of two data engineers to build adequate infrastructure, totaling $253,660. For the upper-bound estimate, companies are projected to spend around $1.3 million in capital investment for larger compliance-related technologies and systems.[70] In reality, costs may significantly differ between companies depending on the extent of in-house engineering capabilities, the use of legacy data systems, and the availability of commercial solutions. For the present analysis, however, the aforementioned costs provide an approximate range for IT infrastructure costs that a company incurs primarily at the onset of compliance.

For IT infrastructure and data inventory assessments, the compliance cost for a single business is estimated to be between $253,660 and $1,300,000 due to a consumer data privacy law.

65 This training time is a conservative lower bound estimate as some companies may devote more or less time to training/preparation. According to a research report by DataGrail that studied trends after the GDPR and CCPA, the amount of time staff spent preparing for compliance ranged from 1 day to more than 30 days. The lowest category was between 1-5 days, which is roughly reflected by the 20 hour amount used above. See DataGrail, The Age of Privacy: The Cost of Continuous Compliance, Released Feb. 2020.

66 In this context, opportunity cost refers to the foregone revenue that could have been earned if employees were working instead of training.

67 To calculate the lower-bound estimate of training, assume an annual salary of $107,680 for the DPO ($51.77/hour) and multiply by 20 hours of training. Lower-Bound = $51.77 * 20 = $1,035. For the upper-bound estimate, on top of the $1,035, add in the total cost of training for the two database administrators. Assuming an annual salary of $98,860 ($47.53/hour) and multiplying by 40 (20 hours each), the result is Upper-Bound = ($47.53 * 40) + ($1,035) = $2,936.

68 Ponemon Institute, The True Cost of Compliance with Data Protection Regulations, Dec. 2017.

69 Bureau of Labor Statistics (BLS), Occupational Outlook Handbook, Accessed Sept. 2, 2021. Note: For the Data Engineer salary, the analysis uses the 2020 median pay for a "Computer and Information Research Scientist."

70 See the compliance cost for specialized technologies in the Ponemon institute report, The True Cost of Compliance with Data Protection Regulations, Dec. 2017.

Responding to Consumer Requests

Once adequate IT infrastructure and processes are in place, companies incur a compliance cost when responding to consumer requests. Consumers, for example, may submit a verifiable request to delete any personal information that a business has collected about them. Afterward, a company would authenticate the request and then process it through the system to delete any relevant personal information. The entire process from start to finish can be seen as a processing cost for companies. Depending on the size and complexity of a consumer's request, the processing cost may either be expensive or inexpensive to execute. Over time, automating processes or employing artificial intelligence (AI) can potentially lower processing costs, but these would also represent technology costs to implement.

To estimate the number of consumer requests a Florida company may receive in a given year, the report references trends observed in California after the CCPA went into effect in January 2020. Analyzing privacy data, one report found that following CCPA implementation, companies processed between 100 and 190 requests per million consumer records in a year.[71] Throughout 2020, do not sell (DNS) requests were the most common type of data subject request at 46 percent, followed by deletion requests which comprised 31 percent of total requests.[72] As a benchmark, this report assumes that Florida companies would receive between 100-190 requests per million consumer records in a given year. Data from Gartner suggests the cost of processing is around $1,406 per request.[73] Multiplied together, the cost per request and expected requests per year present an estimated compliance cost for covered companies.

For consumer requests to access, delete, correct, or opt-out of personal information, the compliance cost for a single business is estimated to be between $140,000 and $275,000 annually due to a consumer data privacy law.

Data Security Safeguards

Given the alarming growth of data breaches in recent years,[74] data security provisions have formed a core part of consumer data privacy legislation. From Virginia to California, consumer data privacy laws require covered companies to implement reasonable security measures to prevent the illegal access, use, or theft of a consumer's personal information. California's CCPA goes even further by allowing any consumer whose nonencrypted or nonredacted personal information is exfiltrated or stolen to institute a civil action against covered companies.[75] Following other states, Florida included legislative provisions that aimed to bolster data security for consumer information.[76] For these reasons, it can be expected that as part of any aggregate compliance cost, companies would incur a cost from implementing reasonable data security measures.

Data security measures can vary in scope and price, ranging from smaller cybersecurity risk assessments to more sophisticated protection systems. Furthermore, there may be lower data security costs for companies that have extensive experience handling sensitive personal information, such as in the healthcare or financial sectors. Given the variability, to proxy the compliance cost for companies, the analysis references findings from a Cisco cybersecurity report that studied data security costs for different sized firms.[77] The report found that 46 percent of mid-market organizations (250-999 employees) spent less than $250,000 on data security and 43 percent spent between $250,000 and $999,999. For enterprise organizations (1,000-9,999 employees), more than 57 percent reported spending between $250,000 and $999,000 for security safeguards.[78] As a rough benchmark, the analysis assumes Florida companies will spend between $200,000 and $500,000 to comply with data security requirements.

71 DataGrail, Early CCPA Trends Shaping the Privacy Landscape, Apr. 2020.

72 DataGrail, The State of CCPA: Benchmarking CCPA Trends Across Consumer (B2C) Brands, Mar. 2021

73 Gartner, "4 Key Trends in the Gartner Hype Cycle for Legal and Compliance Technologies, 2020," Sept. 21, 2020.

74 Forbes, "Alarming Cybersecurity Stats: What You Need to Know for 2021," Mar. 2, 2021.

75 California Legislative Information, "SB-1121 California Consumer Privacy Act of 2018," Accessed Sept. 7, 2021.

76 Florida Senate, CS/CS/SB 1734: Consumer Data Privacy Bill Text, Last Action: Apr. 28, 2021. Florida House of Representatives, CS/CS/CS/HB 969: Consumer Data Privacy Bill Text, Last Action: Apr. 30, 2021. Accessed Sept. 7, 2021.

77 Cisco Cybersecurity Series, The Security Bottom Line: How much security is enough?, Oct. 2019.

78 Ibid.

For implementing reasonable data security measures to protect consumers' personal information, the compliance cost for a single business is estimated to be between $200,000 and $500,000 annually due to a consumer data privacy law.[79]

Total Cost of Compliance

Based on the different cost components explored throughout this section—staffing, IT infrastructure, consumer responses, and data security—the cost of initial compliance ranges from $732,500 to nearly $2.5 million for each Florida company covered under a consumer data privacy law (See Table 3). In a 2021 consumer data privacy benchmark study by Cisco, the report found that consumer data privacy budgets for compliance averaged $2.4 million—comparable to the upper-bound estimate in the present analysis.[80]

Table 3. Per-Firm Cost of Initial Compliance Due to Consumer Data Privacy

Description	Lower Bound	Upper Bound
Staffing and Training	$138,865	$393,848
IT Infrastructure and Systems	$253,660	$1,300,000
Responses to Consumer Requests	$140,000	$275,000
Data Security Safeguards	$200,000	$500,000
Total, All Categories	**$732,525**	**$2,468,848**

Source: Florida TaxWatch[81]

Businesses that must comply with consumer data privacy are likely to experience a higher cost of compliance at the beginning due to the preparation and development required before a data law's effective date. Even though these costs may taper off over time, covered businesses would still experience ongoing compliance costs from employing data privacy professionals, responding to consumer requests, and keeping data warehouses secure. The per-firm cost of ongoing compliance is comparable to the previous table; however, the cost to develop IT infrastructure is lower in this calculation since development costs are presumed to be primarily front-loaded. Nonetheless, companies may still incur an ongoing cost for maintenance to IT infrastructure. As such, costs are assumed to be 25 percent of the initial compliance cost for the IT infrastructure category.[82] Based on the different cost components explored throughout this section, the cost of ongoing compliance would range between $542,000 and nearly $1.5 million for each covered business (See Table 4).

Table 4. Per-Firm Cost of Ongoing Compliance Due to Consumer Data Privacy

Description	Lower Bound	Upper Bound
Staffing and Training	$138,865	$393,848
IT Infrastructure and Systems	$63,415	$325,000
Responses to Consumer Requests	$140,000	$275,000
Data Security Safeguards	$200,000	$500,000
Total, All Categories	**$542,280**	**$1,493,848**

Source: Florida TaxWatch[83]

To estimate the aggregate cost of initial and ongoing compliance to the state of Florida, the report estimates how many covered businesses would likely fall under a consumer data privacy law. Threshold requirements largely dictate how many businesses would be affected, with higher thresholds minimizing the exposure to small and mid-sized businesses. In the previous Florida TaxWatch brief, the compliance estimate assumed the consumer data privacy law would affect most businesses in Florida, even those with fewer than 20 employees. To update these numbers and reflect Florida legislative attempts to raise thresholds (thereby capturing fewer small businesses) the present analysis incorporates firm data from the 2018 Statistics of US Businesses (SUSB) program.[84]

79 The analysis assumes these costs are recurring each year as companies want to ensure data security precautions are in place to maintain proper compliance.

80 Cisco, 2021 Data Privacy Benchmark Study – Forged by the Pandemic: The Age of Privacy, Jan. 26, 2021.

81 The numbers presented in this table reflect various sources mentioned throughout the report section.

82 In reality, maintenance costs may be exponentially higher than is presently estimated. However, absent any concrete data about what the average cost is per company, the current analysis provides a conservative estimate of 25%.

83 The numbers presented in this table reflect various sources mentioned throughout the report section.

84 U.S. Census Bureau, 2018 SUSB Annual Data Tables by Establishment Industry, Released May 2021. The data from 2018 is the latest available data from the U.S. Census.

Table 5. Number of Florida Firms

Firm Employment Size	Upper Bound
<20 employees	420,822
20-99 employees	31,816
100-499 employees	7,111
500+ employees	4,938
Total	**464,687**

Source: 2018 Statistics of U.S. Businesses

Based on the data from the U.S. Census, there are 464,687 firms in Florida (See Table 5); however, not all businesses would be covered under a consumer data privacy law.[85] The current analysis assumes all firms with 500+ employees will incur the compliance costs outlined in the previous sections, and 50 percent of firms with 100-499 employees will face similar costs. These assumptions are modeled on similar assumptions made in the economic impact assessment for California's CCPA implementation.[86] Additionally, the assumptions reflects the fact that since the first iteration of consumer data privacy legislation in Florida, there have been substantive efforts to raise the thresholds and reduce the number of smaller businesses affected.

As observed in Virginia, efforts to raise business thresholds have minimized the scope of the VCDPA and lowered overall compliance costs. This experience differs from the EU's work with the GDPR which lacks any threshold requirements and disproportionately affects smaller to mid-sized businesses, raising total compliance costs. Absent any concrete data, these assumptions are conservative estimates that will differ depending on the final thresholds adopted in any Florida legislation. For the present analysis, there are at least 8,493 Florida businesses projected to fall under a consumer data privacy law.[87] It should also be pointed out, some of these businesses may already fall under consumer data privacy laws in other states like California or Virginia.

For the state of Florida, the total cost of initial compliance from implementing data privacy is estimated to be between $6,221,334,825 and $20,967,926,064.[88] This range depends on the cost estimates presented previously and the potential number of firms affected. Any such changes to the per-firm compliance cost (e.g., more or fewer obligations) or to the number of covered businesses (e.g. raising or lowering thresholds) will influence the ultimate outcome. Additionally, if many of the covered businesses have already implemented similar compliance features for other states, the resulting cost would likely be on the lower range. If on the other hand a Florida data privacy law were to induce wholly new compliance activities for companies, the aggregate cost would be on the higher end of the range. Overall, the aggregate cost estimates represent an approximate range that may serve as a benchmark for ex-post compliance analysis.

For the state of Florida, the total cost of ongoing compliance from implementing consumer data privacy is estimated to be between $4,605,584,040 and $12,687,251,064 annually.[89] Once again, this estimated range depends on how many firms are ultimately affected and how much each company must pay each year to stay in compliance. Having more consumer requests every year, for example, would cause companies to have an ongoing compliance cost on the higher end of the estimated range. Efforts to streamline processes would conceivably lower ongoing compliance costs over time.

Non-Quantifiable Components and Secondary Effects

Consumer data privacy legislation would generate certain direct costs for businesses in Florida. Yet beyond the cost categories already mentioned, certain compliance elements are inherently difficult to quantify and raise concerns about non-compliance. Additionally, how compliance obligations indirectly affect other businesses is another remaining question. Although not exclusive, the considerations presented in this section offer a

85 U.S. Census Bureau, 2018 SUSB Annual Data Tables by Establishment Industry, Released May 2021.

86 Berkeley Economic Advising and Research, LLC (Prepared for State of California Department of Justice), Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, Aug. 2019.

87 Total Firms = 4938 + (0.50 x 7111) = 8493.5.

88 Reference Table 3. Lower Bound Estimate = 8,493 * $732,525 = $6,221,334,825 /// Upper Bound Estimate = 8,493 * $2,468,848 = $20.967,926,064.

89 Reference Table 4. Lower Bound Estimate = 8,493 * $542,280 = $4,605,584,040 /// Upper Bound Estimate = 8,493 * $1,493,848 = $12,687,251,064.

starting point to consider some non-quantifiable difficulties with consumer data privacy.

Secondary Effects on Small to Mid-Sized Businesses

Although small and mid-sized businesses are not primarily targeted by consumer data privacy legislation due to higher threshold requirements, these businesses could still experience indirect outcomes from any consumer data privacy law. To stay economically competitive, smaller businesses may have to follow trends set by larger firms, such as offering delivery services or maintaining a website. Extending to consumer data privacy, even though small to mid-sized businesses would not be mandated to comply in most cases, they may still feel compelled to adopt consumer data privacy measures to remain competitive. In other words, there may be a market expectation for smaller firms to protect consumer information in the same way as large companies, or else consumers may opt for larger competitors. The result is an economic pressure for smaller businesses to implement consumer data privacy without the sufficient financial resources to do so. Calculating this secondary, downstream effect on small to mid-sized businesses is difficult to achieve without actual data; however, experiences in Europe with GDPR suggest the costs may be disproportionately high.[90]

Unintended Competitive Advantages for Large Businesses

Consumer data privacy legislation is ordinarily crafted to focus regulatory efforts on large technology-oriented companies that deal with personal information daily. As discussed in the previous point, this orientation can still affect smaller businesses. For larger businesses, however, consumer data privacy legislation may create a competitive advantage over smaller and medium-sized firms. Larger firms are more likely to have prior experience coming into compliance with consumer data privacy laws around the world in places like Europe and California. Further, these larger businesses have significant in-house engineering, legal, and administrative resources to make compliance less burdensome. Since large technology companies are often the target of consumer data privacy laws, they attract data privacy professionals with technical expertise, potentially attracting privacy experts away from other businesses in different industries. The competitive advantage that larger businesses may experience is not easily quantifiable, but it signifies a potential disequilibrium in the economy.

Inferences and Probabilistic Identifiers

"Personal information" is a large encompassing term that can refer to many different identifiers often spelled out in legislation. Certain identifiers, such as social security numbers and names, are obvious pieces of personal information. Yet less apparent are inferences and probabilistic identifiers which may indirectly identify a consumer based on other data points. Constructed consumer profiles may reflect information about an individual's preferences, predispositions, or psychological trends. Probabilistic identifiers may link a consumer to a degree of certainty of more than 50 percent based on other categories. California's CCPA includes express business obligations that deal with inferential or probabilistic personal information—a feature that has led to some practical difficulties for companies. Virginia's VCDPA and Colorado's CPA, on the other hand, do not have any provisions regarding inferential profiles or probabilistic identifiers, making compliance easier.

Similar to California's CCPA, some provisions within Florida's proposed consumer data privacy legislation deal with inferences drawn from consumers and probabilistic identifiers.[91] There are certain compliance issues, however, for companies to respond to consumer requests regarding inferential profiles or probabilistic identifiers. For example, a consumer who requests to delete all personal information would require a company to delete all connected data points, even if tangentially related to the constructed profile. For some businesses, the IT architecture to respond to such a request simply does not exist. And for other companies, to comply with such a request would require significant reconstructing or an overhaul of business models. Either way, there is a substantial risk of non-compliance that leads to enforcement and litigation costs. Even though California's CCPA includes rules about inferential and probabilistic data, the CCPA does not allow citizens to bring a private right of action against non-compliant businesses. The

90 GDPR.EU, "Millions of small businesses aren't GDPR compliant, our survey finds," Accessed Sept. 8, 2021.

91 Florida House of Representatives, CS/CS/CS/HB 969: Consumer Data Privacy Bill Text, Last Action: Apr. 30, 2021. Accessed Sept. 8, 2021.

inclusion of a private right of action in Florida legislation would make this present difficulty more than just a compliance issue but also a litigation consideration.

Estimated Cost of Litigation in Florida

Enforcement is often seen as a core part of consumer data privacy legislation, enabling regulators to oversee implementation and ensuring accountability when rules are ignored. In California, Virginia, and Colorado, the Attorney General possesses the power to notify companies of alleged violations and initiate enforcement actions if needed after some specified cure period (typically 30 days). Of the three states that have already passed consumer data privacy laws, California's enforcement mechanism is the most expansive due to the CCPA's private right of action. Under the CCPA, consumers can sue companies directly for civil penalties under the private right of action provision when nonencrypted or nonredacted personal information is breached or stolen.[92] Regarding damages, CCPA consumers can seek statutory damages between $100-$750, or actual damages, depending on the data incident.[93]

If not reasonably constructed, enforcement mechanisms can produce duplicative enforcement efforts and create disproportionate litigation costs for organizations. Allowing both government regulators and private citizens to pursue litigation, for example, can lead to sizeable legal fees and result in a negative economic impact. Other than litigation data related to the CCPA, there are scant data points about how a private right of action would induce civil lawsuits in a particular state.

Nevertheless, this section seeks to project the number of private cause of action cases, and accompanying litigation costs, if a consumer data privacy bill were to pass in Florida.

The analysis uses class-action data under the CCPA as a reference.

To project the potential number of consumer data privacy class-action lawsuits in Florida, this analysis uses class-action CCPA data as a reference point and U.S. Census data detailing the number of businesses in each state. Between January 2020 and July 2021, there were 141 class-action lawsuits filed under the CCPA's private right of action section.[94] According to U.S. Census data, there are around 779,825 businesses in California.[95] When considered together, the two figures suggest there have been 18.08 consumer data privacy class-action lawsuits per 100,000 California businesses since January 2020.[96] In Florida, there are some 464,687 total businesses in the state.[97] Applying the class-action rate found above, this report projects there to be roughly 84 class-action lawsuits in Florida due to consumer data privacy (See Table 6).[98]

Table 6. Consumer Data Privacy Private Right of Action Lawsuits

State	Firms	Lawsuits	Lawsuits Per 1,000 Firms
California	779,825	141	18.08
Florida	464,687	84*	18.08*

Source: 2018 Statistics of U.S. Businesses;
*= Estimated (See Calculations Above)

It should be emphasized, these Florida-specific projections are dependent on the inclusion of a private right of action in any Florida consumer data privacy legislation. The CCPA's private right of action is written to focus solely on data breach incidents; however, potential legislation in Florida would extend this private right of action to other non-compliance issues. Authorizing consumers to sue companies for issues beyond just data security would increase the estimated number of class-action cases in Florida, thereby raising potential litigation costs.

92 JD Supra, "Preparing for the CCPA Private Right of Action for Certain Security Incidents," Jan. 6, 2020.

93 International Association of Privacy Professionals (IAPP), "CCPA litigation: Shaping the contours of the private right of action," Jun. 8, 2020.

94 Perkins Coie, CCPA Litigation Tracker, Updated As of July 2021, Accessed on Sept. 9, 2021.

95 U.S. Census Bureau, 2018 SUSB Annual Data Tables by Establishment Industry, Released May 2021.

96 To find this number, TaxWatch took the number of class-action lawsuits (141) and divided it by the number of firms in California (779,825). 141/779,825 = 0.00018081. Finally, the product is multiplied by 100,000 to get a rate per 100,000 firms. 0.00018081 * 100,000 = 18.08.

97 U.S. Census Bureau, 2018 SUSB Annual Data Tables by Establishment Industry, Released May 2021.

98 To find this number, TaxWatch took the rate of 18.08 per 100,000 firms (18.08/100,000) and multiplied it by the number of firms in Florida (464,687). The result is (18.08/100,000) * 464,687 = 84.02.

Ascribing a litigation cost for each particular lawsuit is difficult given the myriad factors, including attorney's fees, court fees, and legal consultations that businesses may experience. Complicating estimates further, the number of consumers who sign onto these class-action lawsuits would also affect the aggregate cost. In 2020, defense spending on class-action lawsuits reached a new high of $2.9 billion and is anticipated to exceed $3 billion in 2021. A past survey from Duke Law School found that the average outside litigation cost per respondent was $115 million, an amount that has risen in recent years.[99] Given the variability and uncertainty of the numerous components that comprise litigation costs, the analysis conservatively estimates that each class-action lawsuit would cost organizations more than $50 million. In a comparable report by Information Technology & Innovation Foundation, the study used a similar per-case cost estimate to determine economic impacts.[100]

For the state of Florida, the potential cost of litigation from implementing consumer data privacy is estimated to be more than $4.2 billion over subsequent years.[101] The estimation incorporates the assumptions that a Florida consumer data privacy law would include a private right of action provision and would produce similar legal trends following CCPA implementation. Even without a private right of action, however, firms are still expected to incur a legal cost to maintain in-house experts or consult external firms. These lawyers would likely provide advice on how to comply with consumer data privacy provisions and how to respond to an Attorney General's enforcement decision. Because the $4.2 billion cost estimate is based on observations from California's CCPA, the resulting litigation cost may far exceed (or be under) the approximate projection presented in this analysis.

Conclusion

In response to a growing data economy that underpins most consumer products and services, governments around the world have sought to grant individuals rights to control their personal information. In the U.S., the absence of federal consumer data privacy laws has generated a patchwork of state consumer data privacy laws with varying provisions. To date, California, Virginia, and Colorado are the only three states that have passed comprehensive data privacy laws, but legislative activity in other states suggests consumer data privacy may soon follow elsewhere across the nation.

To calculate the potential economic outcomes of passing consumer data privacy in Florida, this report analyzed the respective compliance and litigation costs stemming from implementation. Based on various cost elements, the report estimated the total cost of initial compliance to be between $6.2 and $21.0 billion for the state of Florida. Two key variables in determining the actual cost will be the number of firms affected and the size of the respective firms. When considering the ongoing costs of compliance, such as staffing needs and responses to consumer requests, the total cost of ongoing compliance is projected to be between $4.6 and $12.7 billion annually for Florida. Finally, there is a litigation risk that arises when companies are not compliant with the law. Assuming the inclusion of a private right of action, there is a potential litigation cost of more than $4.2 billion in the state of Florida.

Consumer data privacy is a tradeoff between the economic value and privacy rights for consumers and the potential economic costs that arise due to compliance and litigation. Given COVID-19's ongoing economic, the development of any consumer data privacy in Florida should be considered in conjunction with the potential economic outcomes that such a law would produce. Ultimately, the action that would yield the most consumer benefits while minimizing the adverse costs of implementation is passing a comprehensive federal consumer data privacy law that unifies regulatory frameworks across the fifty states.

99 Duke Law School, "Litigation Cost Survey of Major Companies," Presented by Lawyers for Criminal Justice, Civil Justice Reform Group, and U.S. Chamber Institute for Legal Reform," May 2010, Accessed Sept. 2021. Respondents included Fortune 200 companies.

100 Information Technology & Innovation Foundation, The Costs of an Unnecessarily Stringent Federal Data Privacy Law, Aug. 5, 2019.

101 To find this number, TaxWatch multiplied the projected number of class-action lawsuits (84) and the cost per case ($50 million). Litigation Cost = 84 * $50,000,000 = $4,200,000,000 ($4.2 billion). Given the fact some lawsuits take a long time to settle, it is unclear whether these costs would be absorbed on an annual basis or over a specified period of time. The analysis does not endeavor to estimate the time table for litigation costs.

Recommendations

As discussed in great detail throughout this report, consumer data privacy would create certain compliance and litigation costs for Florida companies in exchange for greater consumer control over personal information. In an effort to maintain a proper balance while mitigating potential economic costs, Florida TaxWatch makes the following recommendations:

Recommendation 1

Delay consumer data privacy implementation until July 1, 2024, or later to provide covered businesses ample time to come into compliance with new regulations.

If a consumer data privacy law were to pass in Florida, businesses would need to construct new IT infrastructure and processes to be compliant. In addition to the technical needs, there would also be a need for adequate training among staff to ensure proper preparation. Delaying a consumer data privacy law's effective date allows companies more time to understand their unique complexities and address challenges beforehand, thereby reducing the risk of non-compliance when the law goes into effect. Reducing the risk of non-compliance would have the added benefit of mitigating the risk of litigation. Virginia and Colorado's consumer data privacy laws have both been praised in their respective states for providing businesses more time to prepare for full implementation. Both data laws (the VCDPA and CPA) are set to go into effect in 2023.[102]

Recommendation 2

Omit a private right of action provision from consumer data privacy legislation to minimize litigation costs.

Enforcement is a key part of consumer data privacy legislation, without which there would be little incentive to comply with a consumer data privacy law. Duplicative enforcement, however, is a costly outcome. As this report finds, including a private right of action can potentially lead to litigation costs of more than $4.2 billion in Florida over subsequent years. Currently, California is the only U.S. state to offer a limited private right of action, and over a year and a half, there have been more than 141 class-action lawsuits filed citing the CCPA.[103]

Exposing covered businesses to heightened legal risk has the unintentional consequence of detracting resources away from compliance activities that would, in the end, do more to protect consumer personal information.[104] Agency enforcement is a far more effective method that avoids excessive judicial costs and allows companies to identify and remedy compliance issues through a robust, consistent process.

Recommendation 3

Urge Florida's congressional delegation to push for passage of a comprehensive federal consumer data privacy law—rather than a state-by-state standard—that would standardize consumer rights, business obligations, and enforcement mechanisms across all 50 states.

Currently, the U.S. lacks a comprehensive consumer data privacy law, opting instead for a patchwork of sectoral or data-specific federal regulations (e.g., GLBA and HIPAA) that govern the use of personal information in areas like healthcare and financial information.[105] In recent years, state governments have taken an active role to pass consumer data privacy laws, at the expense of consistency and uniformity across the nation. Without a common set of compliance regulations, however, businesses will face greater difficulty adapting to different state consumer data privacy laws and experience even higher compliance costs. A vast array of state laws would inevitably lead to inconsistent treatment of personal information, endangering consumers in the process.

102 National Conference of State Legislatures, "State Laws Related to Digital Privacy," July 22, 2021.

103 Perkins Coie, CCPA Litigation Tracker, Updated As of July 2021, Accessed on Sept. 9, 2021.

104 U.S. Chamber Institute for Legal Reform, Ill-Suited: Private Rights of Action and Privacy Claims, July 2019.

105 New York Times, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," Sept. 6, 2021.

ABOUT FLORIDA TAXWATCH

As an independent, nonpartisan, nonprofit taxpayer research institute and government watchdog, it is the mission of Florida TaxWatch to provide the citizens of Florida and public officials with high quality, independent research and analysis of issues related to state and local government taxation, expenditures, policies, and programs. Florida TaxWatch works to improve the productivity and accountability of Florida government. Its research recommends productivity enhancements and explains the statewide impact of fiscal and economic policies and practices on citizens and businesses.

Florida TaxWatch is supported by voluntary, tax-deductible donations and private grants, and does not accept government funding. Donations provide a solid, lasting foundation that has enabled Florida TaxWatch to bring about a more effective, responsive government that is accountable to the citizens it serves since 1979.

RESEARCH PROJECT TEAM

Tony Carvajal	Executive Vice President	
Jonathan Guarine	Research Economist	*Lead Researcher & Author*
Chris Barry	Vice President of Comms. & External Affairs	*Design, Layout, Publication*

All Florida TaxWatch research done under the direction of Dominic M. Calabro, President, CEO, Publisher & Editor.

The findings in this Report are based on the data and sources referenced. Florida TaxWatch research is conducted with every reasonable attempt to verify the accuracy and reliability of the data, and the calculations and assumptions made herein. Please feel free to contact us if you feel that this paper is factually inaccurate.

The research findings and recommendations of Florida TaxWatch do not necessarily reflect the view of its members, staff, Executive Committee, or Board of Trustees; and are not influenced by the individuals or organizations who may have sponsored the research.

Florida TaxWatch

Stay Informed

floridataxwatch.org

@floridataxwatch

@floridataxwatch

@fltaxwatch

Florida TaxWatch
106 N. Bronough St.
Tallahassee, FL 32301

o: 850.222.5052
f: 850.222.7476