ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Looming Cost of a Patchwork of State Privacy Laws

DANIEL CASTRO, LUKE DASCOLI, AND GILLIAN DIEBOLD | JANUARY 2022

In the absence of a federal privacy law, a growing patchwork of state laws burdens companies with multiple, duplicative compliance costs. The out-of-state costs from 50 such laws could exceed $1 trillion over 10 years, with at least $200 billion hitting small businesses.

KEY TAKEAWAYS

- Since 2018, 34 states have passed or introduced 72 privacy bills regulating the commercial collection and use of personal data.
- These laws create significant compliance costs for in-state businesses and confusion for consumers while also raising costs for out-of-state businesses that increasingly find themselves subject to multiple, duplicative rules.
- State privacy laws could impose out-of-state costs of between $98 billion and $112 billion annually. Over a 10-year period, these out-of-state costs would exceed $1 trillion.
- Small businesses would bear $20–23 billion of this out-of-state burden annually.
- Congress should pass federal privacy legislation that preempts states, protects consumers, and promotes innovation.

SUMMARY

In the absence of a comprehensive federal law, a handful of large states, including California, Colorado, and Virginia, have passed or begun to enact data privacy legislation. More states are likely to pass similar laws in the coming years, which would create a patchwork of different and sometimes conflicting state privacy laws regulating the commercial collection and use of personal data. Not only do these laws create significant costs for in-state businesses, both in terms of direct compliance costs and decreases in productivity, but they also raise costs for out-of-state businesses that can find themselves subject to multiple and duplicative rules and create confusion for consumers.

The Information Technology and Innovation Foundation (ITIF) has estimated that, in the absence of Congress passing privacy legislation, state privacy laws could impose out-of-state costs of $98 billion and $112 billion annually. Over a 10-year period, these costs would exceed $1 trillion. The burden on small businesses would be substantial, with U.S. small businesses bearing $20–23 billion annually.

ITIF's economic model also shows the impact of privacy laws on each state. For example, ITIF has estimated that California's privacy law will cost $78 billion annually, with California's economy bearing $46 billion and the rest of the U.S. economy bearing the other $32 billion. California small businesses will bear $9 billion of in-state costs, while out-of-state small businesses face $6 billion of costs.

These estimates highlight the high costs of states creating a patchwork of privacy laws and the need for Congress to move quickly to pass legislation to create a national privacy framework that streamlines regulation, preempts state laws, establishes basic consumer data rights, and minimizes the impact on innovation.

INTRODUCTION

Over the past few years in the United States, there has been a growing interest in establishing a new "omnibus" data protection law that would apply to a broad spectrum of organizations and go beyond the nation's many sectoral data protection laws. While members of Congress have introduced multiple proposals, none have yet to gather widespread bipartisan support. Without federal action, multiple states have proposed or enacted their own data protection laws. Unless Congress acts quickly, states will continue to erect a patchwork of potentially conflicting privacy laws that will not only confuse consumers but also impose significant costs on organizations, as they will have to comply with differing laws from multiple states.

In addition, many of the states advancing data protection legislation are modeling their proposals on the European Union's General Data Protection Regulation (GDPR)—one of the most restrictive data protection regimes in the world—which means businesses in the United States will be subject to significant regulatory costs that will ultimately be passed on to consumers. However, few of these states seem to understand that one of the primary purposes of the GDPR was to harmonize data protection laws across EU member states, and by enacting competing, and potentially contradictory, state data protection laws, state legislatures are creating the exact type of fragmentation in the United States that the EU created the GDPR to solve.

Congress should pass legislation to create a national privacy framework that streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation. Ideally, such legislation should protect and promote innovation by minimizing compliance costs and restrictions on data use, such as by allowing consumers to generally opt out of data collection (rather than requiring them to opt in) and avoiding data-minimization requirements, purpose-specification requirements, limitations on data retention, and privacy-by-design requirements. But even in the absence of such an optimal bill, two priorities stand out: First, Congress should preempt state data protection laws to ensure that there is one uniform national standard; and second, Congress should avoid creating a private right of action that would open a floodgate of expensive, and unnecessary, lawsuits against organizations subject to the new law. With President Biden signaling that his administration will be taking a more active role on data privacy, Congress may finally find the momentum it needs to move forward with comprehensive privacy legislation.[1]

BRIEF OVERVIEW OF PROPOSED U.S. DATA PRIVACY LAWS

Historically, the United States has embraced a light-touch regulatory approach to the digital economy. Rather than create a single data protection law, as the EU has done with the GDPR, the United States has a series of sectoral laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA) to regulate data in the health, financial, and educational sectors, respectively.

Over the past few years, federal and state lawmakers have proposed various privacy laws to regulate the collection and use of personal data. While these proposals have stalled in Congress, states have begun to enact new data protection laws that will have a significant impact on consumers and businesses, including those outside their respective states.

Federal Laws

Members of Congress introduced dozens of bills relating to privacy in 2021. While most of these bills addressed specific privacy issues, such as rules for contact tracing apps, vaccine passports, or social media, a handful of bills propose a broader federal privacy framework.[2] Some of these bills focus on businesses providing online services or engaging in e-commerce, while others include any organization processing personal data. Key bills introduced in 2021 include:

- **H.R. 1816, Information Transparency & Personal Data Control Act:** Introduced by Rep. DelBene (D-WA), this legislation directs the Federal Trade Commission (FTC) to establish requirements for how data controllers collect, transmit, store, process, and use sensitive personal information, including rules for obtaining affirmative consent, publishing an understandable privacy policy, and conducting regular privacy audits, as well as providing users with the ability to opt out of sharing nonsensitive information.[3] The legislation would preempt states from creating or enforcing their own competing privacy laws. The bill has 20 cosponsors and no companion bill in the Senate.
- **S. 113, BROWSER Act:** Introduced by Sen. Blackburn (R-TN), the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act requires broadband providers and online service providers to obtain opt-in consent from users to use or share their sensitive personal information and allows users to opt out of the use and sharing of nonsensitive

personal information.[4] This legislation would preempt states from creating or enforcing their own competing privacy laws. It has no cosponsors, but it does have a companion bill in the House with five cosponsors.[5]

- **S. 919, Data Care Act of 2021:** Introduced by Sen. Schatz (D-HI), the Data Care Act imposes specific obligations on online service providers, including a duty to secure information from unauthorized access, a duty to refrain from using data in ways that might harm end users, and a duty to not disclose data to a third party unless that third party is also bound by these same obligations.[6] This legislation would not preempt states from creating or enforcing their own privacy laws. It has 18 cosponsors and no companion bill in the House.

- **S. 1494, Consumer Data Privacy and Security Act of 2021:** Introduced by Sen. Moran (R-KS), the Consumer Data Privacy and Security Act requires most businesses and nonprofit organizations to follow certain rules when collecting and processing personal data, including adhering to notice and consent requirements, providing users with an easy-to-understand privacy policy, and offering users the ability to access, transfer, correct, or delete their personal data.[7] This legislation would preempt states from creating or enforcing their own competing privacy laws. It has no cosponsors and no companion bill in the House.

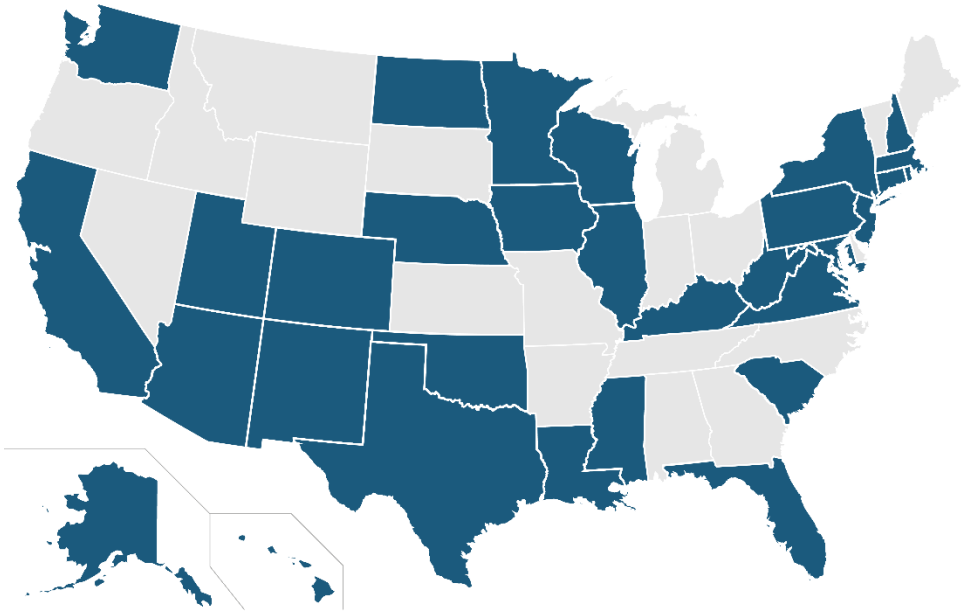
- **S. 2134, Data Protection Act of 2021:** Introduced by Sen. Kirsten Gillibrand (D-NY), this legislation would establish a new Data Protection Agency tasked with enforcing the nation's laws around the processing and use of personal data and preventing and remediating privacy harms. The bill would not preempt states from creating or enforcing their own privacy laws. It has one cosponsor and no companion bill in the House.

- **S. 2499, SAFE DATA Act:** Introduced by Sen. Wicker (R-MS), the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act requires most businesses and nonprofit organizations to implement a broad range of measures, including minimizing data collection, processing, and retention to what is reasonably necessary; conducting regular privacy impact assessments; appointing a data privacy officer and data security officer; and granting consumers the right to access, transfer, correct, or delete their data.[8] This legislation would preempt states from creating or enforcing their own competing privacy laws. It has one cosponsor and no companion bill in the House.

State Laws

States have passed a number of data privacy laws in recent years. Three states—California, Virginia, and Colorado—have passed comprehensive privacy legislation that gives consumers in those states new rights regarding the collection of their personal information and imposes new obligations on businesses. Many other states are looking to enact similar privacy laws. Since California passed its first law in 2018, the number of privacy bills introduced each year in state legislatures has increased. As shown in Figure 1, over the past three years, state legislatures have introduced 72 bills in a total of 34 states, with these bills reaching various stages of the legislative process.[9] This privacy patchwork will continue to expand unless federal lawmakers pass legislation that preempts state privacy laws.

Figure 1: States (in blue) that have passed or introduced privacy legislation, 2018–2021



Source: IAPP

States have also passed laws regulating specific data privacy issues. For example, the Illinois Biometric Information Privacy Act (BIPA) and the Texas Capture or Use of Biometric Identifier Act (CUBI) regulate the use of biometric data. BIPA is the more stringent of the laws, requiring written, informed consent for the collection and use of any biometric data and imposing serious penalties on companies that fail to comply with the rules. As of 2021, 5 states had biometric privacy laws modeled after the Illinois law, and 27 have similar legislation pending.[10]

The following summarizes key provisions of the comprehensive privacy laws that have passed in each of those three states.

California

The California Consumer Privacy Act (CCPA) is the most sweeping state privacy law in the United States. Legislators passed the law in June 2018, and it took effect in January 2020. The CCPA creates four new rights for California consumers: the right to know about the collection and use of personal information; the right to delete collected personal information; the right to opt-out of the sale of personal information; and the right to nondiscrimination for exercising CCPA rights.[11]

The CCPA applies to businesses operating in California or working with the data of California residents. To fall under the scope of the CCPA, a business must have a gross annual revenue greater than $25 million, buy or sell the personal information of more than 50,000 California residents, or derive more than 50 percent of its annual revenue from selling personal information.[12] It does not apply to nonprofit organizations or government agencies.

The California Property Rights Act (CPRA) is a ballot provision amending the CCPA that passed in November 2020. The provision, also known as Proposition 24, amends and expands on the rights and obligations of the CCPA. It establishes the California Privacy Protection Agency, a body specifically dedicated to privacy regulation enforcement. It creates a new definition of

"sensitive data" and expands data breach liability for businesses processing and collecting personal information. The CPRA also gives consumers the right to correct personal information held by a business, the right to obtain meaningful information about the logic used in automated decision-making technology, and the right to opt out of the use of their personal information in automated decision-making.

Virginia

Passed in March 2021, the Virginia Consumer Data Protection Act (CDPA) is another comprehensive state privacy law. The law applies to businesses both in and outside Virginia that target Virginia consumers, and it excludes nonprofits and small businesses. To be subject to the CDPA, a business must collect and process the data of over 100,000 consumers, or over 25,000 consumers if more than half the firm's revenue derives from data sales.[13] The CDPA sets a threshold for revenue and does not apply to businesses that only engage in data sales in a small way. Businesses must obtain consent before processing personal data and perform data impact assessments. The bill also creates new consumer rights: the right to access, correct, delete, and move data, along with the right to opt out of the processing of personal data for purposes of targeted advertising.[14]

Colorado

The Colorado Privacy Act (CPA) establishes rules for businesses operating in Colorado regarding the collection and use of personal data and creates a new set of rights for Colorado consumers, such as the rights of deletion and data portability. The CPA applies to Colorado businesses that produce or deliver products or services targeted at Colorado residents and control the personal data of at least 100,000 Colorado residents or control the data of 25,000 residents and derive revenue from the sale of that data.[15] These requirements cast a wider net than the CDPA does, but are narrower than California's criteria.

The CPA does not create a private right of action, a right of restriction, or a right to opt-out of automated decision-making.[16] Notably, Colorado is the first state to mandate an "easy to use" appeals process that can be used whenever a data controller denies a consumer request.[17] The CPA is also the only comprehensive state privacy law that does not exempt nonprofit organizations. Information maintained by state institutions, financial institutions covered by the Gramm-Leach-Bliley Act (GBLA), higher education institutions regulated by FERPA, and information covered by the Fair Credit Reporting Act (FCRA), HIPAA, and the Children's Online Privacy Protection Act (COPPA) is exempt if in compliance with federal law.

METHODOLOGY

Data protection laws impose costs on firms through both compliance costs and market inefficiencies. When firms are subject to multiple laws from more than one state, these costs can increase further as firms must comply with conflicting and overlapping regulations. Even when the laws are similar, small differences in definitions or scope, as well as divergent implementation of regulations, can create significant compliance costs as firms hire lawyers and engineers to ensure their systems comply fully with each state.

To estimate the economic impact state privacy laws have on businesses both within and outside those states, ITIF designed a model to observe empirical change in the earnings of a state's industries due to the passage of state-level privacy. While this type of econometric analysis can

only provide a rough cost projection and is limited by data availability, it helps illustrate the negative effects of creating a patchwork of 50 separate state privacy laws, as opposed to a single federal law, to regulate the collection and use of consumer data by firms.

The Economic Impact of a Patchwork of State Privacy Laws

ITIF's model calculates a composite index—the privacy restrictiveness linkage (PRL)—in order to quantify the extent a given industry is restricted by a particular state's privacy laws. Therefore, this model assumes that data-intensive industries are more impacted by privacy laws than non-data-intensive ones are. ITIF also conducted an econometric exercise to determine the relationship between industry earnings and the composite index scores of privacy restrictiveness. ITIF also produced estimates of aggregate costs for individual states' industries associated with privacy laws passed within those states, as well as the costs imposed on other states' economies due to passing such laws. For example, a privacy law in California would impact both California businesses as well as the many non-California businesses outside the state that wish to conduct business with California consumers.

ITIF's overall quantitative model aims to estimate the costs for each U.S. state, as well as the country at large, in the increasingly likely scenario of all 50 states establishing their own unique privacy laws. It is informed by ITIF's previous 2019 work on assessing the costs of privacy laws at the federal level.[18] This report differs from previous studies in that it incorporates econometric evidence on gross operating surplus (GOS), or earnings by industry, and uses such analysis to assess out-of-state costs associated with state privacy laws. Appendix A elaborates in greater detail on the data and methodology used.

State Restrictiveness Scores

ITIF established a scoring system to measure the extent of U.S. states' privacy restrictiveness over a period between 2003 to 2021. A higher state restrictiveness score (SRS) conveys a stricter privacy law set in that state in the given year. To quantify privacy restrictiveness, ITIF first recorded SRS as the unweighted cumulative sum of the number of unique privacy restrictions passed in a given state *x* observed in year *y*. ITIF used a combination of existing legislation trackers alongside state government sites to compile a list of 15 different privacy restrictions passed between 2003 and 2021.

However, SRS is a function of both in-state restrictions passed as well as out-of-state restrictions observed in other states. This model assumes that the larger a state's share of the nation's data-concerned industries is, the greater the impact of that state's privacy restrictions on businesses in other states. For example, California's privacy laws would expectedly impact businesses across the country far more than privacy laws set in a smaller-share state such as South Dakota would. Since there is no single decisive measurement of data-concerned industries, ITIF employs a proxy-calculation to supplement this measurement. To control for issues of endogeneity, a state's share of the nation's data-concerned industries is observed for the year 2019 and used as a constant in calculating SRS in all other years. The formula of the proxy calculation *d* for the share of the nation's data-concerned industries held by state *x* is below.

1. $$d_x = \frac{(Consumer\ Products\ Share_x + Consumer\ Finance\ Share_x + Advertisement\ Share_x)}{3}$$

A state's share *d* is observed as the unweighted mean of its share of national gross domestic product (GDP) in the consumer products, consumer finance, and advertising industries. We

obtained state shares for the consumer products and consumer finance GDP from the U.S. Bureau of Economic Analysis (BEA) and state shares of national advertising from Statista.[19] Using *d* as a state-specific coefficient to scale the relevance state privacy laws have on the rest of the country, the formula of SRS for state *x* in year *y* is below.

2. $SRS_{xy} = \sum_{n=2003}^{y}(State\ Privacy\ Restriction_{xn}) + \sum_{j \neq x} d_j * \sum_{n=2003}^{y}(State\ Privacy\ Restriction_{jn})$

This notation for the calculation of SRS reflects an in-state privacy restriction impacting all applicable business within that state, whereas an out-of-state privacy restriction impacts only a fraction of the applicable businesses, since not every business is a multi-state operation impacted by other states' restrictions on consumer data. Further, not every industry within a state is equally impacted by restrictions on consumer privacy. For example, the insurance and retail sectors are more reliant on consumer data than are agriculture and mining industries. To measure more precisely how state privacy laws impact downstream industries differently, ITIF calculates the data-intensity modifier (DIM) to measure how data intensive each industry is. Data intensity is approximated by measuring the software usage per worker in each U.S. industry. The model further controls for endogeneity by using national-level data in the base year 2013 to calculate DIM, as opposed to calculating state- and year-specific DIMs. This control, however, assumes equal technology among states and over time. The calculation of DIM for industry *z* is below.

3. $DIM_z = \ln\left(\frac{Intangible\ Software\ Expenditure_z}{Employment_z}\right)$

Data for intangible software expenditure per industry is taken as noncapitalized software expenditures listed in the 2013 U.S. Census Information and Communication Technology Survey. This data is divided by the number of workers in each corresponding industry as provided by the U.S. Bureau of Labor Statistics (BLS) for the same reference year of 2013. DIM is taken as a natural log to align with previous literature on factor intensity.

Privacy Restrictiveness Linkage

Data-intensive industries should be noted as being more susceptible to changes in privacy restrictions than non-data-intensive industries are. Therefore, this model provides a score of privacy restrictiveness for a given industry within a state by linking SRS values with DIM ratios. ITIF draws this linkage as the product of SRS for state *x* in year *y* with the DIM for industry *z* in order to calculate the PRL for that state's given industry. The formula for PRL of industry *z* in state *x* during year *y* is below.

1. $PRL_{xyz} = SRS_{xy} * DIM_z$

The Econometric Model

The composite index of state-industry-year privacy restrictiveness serves as the final independent variable to compare in econometric analysis how changes in state privacy laws impact in-state and out-of-state economies. The dependent variable chosen to measure economic costs incurred by states from state privacy laws is GOS, which is the total profit of enterprises in an industry minus intermediate costs and workers (GOS = Output – Intermediate Expenses – Compensation of Employees). GOS is selected as the dependent variable because it is a residual, meaning its value is the difference between an industry's output and costs. Therefore, a decrease in GOS can be caused by a loss in output or a rise in intermediate expenses or compensation of employees.

This makes GOS a highly useful variable in observing how privacy laws impact the economy, as change in GOS captures both compliance costs and market inefficiencies associated with increased privacy laws. For example, compliance costs from privacy laws requiring more data personnel or legal expenses would increase compensation and intermediate expenses, lowering GOS. Market inefficiencies due to privacy laws making data less usable and transferable would lower output, lowering GOS. Change in GOS would also be driven by privacy laws of multiple states incurring duplicative costs, and by in-state regulatory efforts distorting commerce out of state. Using the income approach to GDP, a loss in GOS is an equivalent loss in GDP. The final regression equation in the model is below.

1. $\widehat{GOS_{xyz}} = \hat{\beta}_0 + \hat{\beta}_1 * PRL_{xyz} + \hat{\beta}_2 * GDP_{xy} + \alpha_y + \gamma_z + \varepsilon_i$

This regression model adds controls via state-year GDP to control for differences in economic size, as well as controlling for fixed effects for both year and industry. Fixed effects control for the many unobservable factors that undoubtedly impact industry performance over time, such as various economic shocks and supply shortages. α_y represents year fixed effects, γ_z represents industry fixed-effects, and ε_i represents the error term. This model implements no time lag, as it aims to also capture how GOS changes due to firms anticipating new policies in the same year of a law's passing.

FINDINGS

The model described yields three primary insights:

- Without Congress passing privacy legislation, state privacy laws could impose out-of-state costs of $98 billion to $112 billion annually.
- Over a 10-year period, these out-of-state costs would exceed $1 trillion.
- The burden on small businesses would be substantial, with U.S. small businesses bearing $20 billion to $23 billion annually.

Each of these findings is discussed ahead in more detail.

The Economic Impact of Privacy Restrictions

The regression equation (formula 5) yields the regression table shown in figure 2. All coefficient estimates are found statistically significant above the 95 percent confidence level (all estimated p-values are less than 0.05). The independent variable of interest, PRL, has a significant negative relationship to GOS. Interpreting the model's negative coefficient estimate on PRL, an additional state privacy restriction (a 1.0 unit increase in PRL) is associated on average with a 0.39 percent decrease in GOS among its private industries.

Figure 2: Regression Table

	Coefficient Estimate	Standard Error	t-value	Pr(>|t|)
Intercept	13.27	0.10	132.8	< 2e-16
PRL	-0.00389	0.00115	-3.78	0.000737
GDP	1.025e-09	2.6e-11	39.4	< 2e-16

R-Squared: 0.734, Number of Observations: 3,984

To further test the validity of ITIF's econometric model in measuring the cost of state privacy laws, we consider the predicted cost of the CCPA. ITIF's list of state privacy laws between 2003 and 2021 (see appendix B) shows that the CCPA adds 10 new privacy restrictions for the State of California. Using the model's findings, the CCPA would convey nearly a 3.9 percent loss in California's $1.19 trillion 2020 GOS of private industry. Therefore, the CCPA's total costs between compliance costs and market inefficiencies borne in California would be approximately $46 billion annually. ITIF estimates an additional $32 billion a year in costs borne by businesses outside the state of California that seek to comply with the CCPA. In total, the CCPA will create a $78 billion annual economic burden on the U.S. economy.

ITIF's estimated in-state costs of $46 billion for the CCPA compare favorably to the cost estimate produced by Berkeley Economic Advising and Research, LLC in 2019.[20] The California Attorney General-sanctioned report found that the CCPA would cost the Californian economy upwards of $55 billion annually. Their methodology, however, focuses only on the cost impacts borne in California and considers no out-of-state effects in the analysis. It also relies heavily on survey data from firms required by law to self-report forecasted costs. The 2019 report also clarifies that their methodology yielding the final $55 billion in annual costs oversamples large-sized firms and thus overestimates costs faced by small firms, indicating that their $55 billion estimate in annual costs is likely overestimated in some small part. Comparing the two model estimates and their nuances, the fact that ITIF's estimate of California's in-state annual costs due to the CCPA is similar to findings from the California Attorney General's Office shows the accuracy of this report's econometric findings used to model the costs of state privacy laws.

Cost-Modeling a 50-State Scenario Over 15 Years

To understand the impact of states continuing to enact their own privacy laws in the absence of federal law, ITIF modeled a scenario in which all 50 states would enact their own privacy law. We assumed not all states would implement identical laws and early adopters would likely favor stricter policies, whereas laggard states would expectedly favor less-stringent consumer privacy laws. ITIF's 50-state scenario models a time horizon of 15 years, where over that time, all 50 states would enact their own state privacy law. The length of this time horizon was based on the rate at which all the states enacted their own data breach laws between 2003 and 2018. During this period, 32 states adopted data breach laws in the first 5 years, 13 states adopted between years 6 and 10, and the final 5 states passed laws between years 11 and 15. And since they are not assumed to have set equally stringent laws, states are modeled in this exercise to set one of

three possible levels of restrictiveness in privacy laws. At "high strictness," states' SRS = 10, at "medium strictness," states' SRS = 4, and at "low strictness," states' SRS = 2. Using regression findings quantifying the negative relationship between state privacy restrictions and GOS, this time-horizon model can estimate costs borne by each state over the 15-year span. Further, this model can discern between costs borne by each state incurred through its own state privacy laws as well as those incurred by privacy laws passed in other states.

Privacy laws can have a significant and detrimental impact on small businesses, which may be less able to weather the compliance burden. To understand the impact on small businesses (defined here as enterprises employing fewer than 50 workers), we further break down the state-by-state cost estimates for a 50-state patchwork of privacy laws. Using U.S. Census County Business Patterns payroll data on enterprises by size, the time-horizon model captures a state's share of total payroll paid from small businesses.[21] This share is used to proxy a state's share of GOS held by small businesses. Thus, we estimate costs of state privacy laws borne by small businesses as a state's share of GOS loss from small businesses.

Figure 3: Annual costs of a 50-state privacy law patchwork

	Year 5	Year 10	Year 15
Number of States with Privacy Laws	32	45	50
Total U.S. Economy Costs	$209B	$230B	$239B
In-State Costs	$112B	$122B	$127B
Out-of-State Costs	$98B	$107B	$112B
Total U.S. Small Business Costs	$43B	$48B	$50B
In-State Costs	$23B	$25B	$26B
Out-of-State Costs	$20B	$22B	$23B

*Note: Total costs in the table may not equal the sum of corresponding in-state and out-state costs due to rounding.

A state's privacy law has a significant impact outside that state. ITIF estimates that state privacy laws could impose out-of-state costs of $98 billion to $112 billion annually. As a point of comparison, the United States spends around $100 billion on police every year.[22] Over a 10-year period, these annual costs would exceed $1 trillion, cumulatively. U.S. small businesses would also face a heavy burden, paying $20 billion to $23 billion in annual costs from out-of-state privacy laws. For both the economy at large and small businesses, a 50-state privacy patchwork levies greater costs through a system of duplicative compliance and enforcement than through in-state costs alone. Below the national level, states vary in their economic burdens coming from in state or out of state based on economic size and restrictiveness. The table ahead elaborates each state's estimated costs from a 50-state privacy patchwork absent any one unifying federal policy on consumer privacy.

Figure 4: State-by-state costs of a 50-state privacy patchwork

State	Expected Privacy Law Strictness	Expected Year of Adoption	Total Costs of 50-State Privacy Laws	Costs of Out-of-State Privacy	Costs of In-State Privacy	Total Costs on Small Business	In-State Costs on Small Business	Out-of-State Costs on Small Business
Alabama	Low	15	$1.9B	$1.2B	$0.6B	$0.4B	$0.1B	$0.3B
Alaska	Low	10	$0.4B	$0.3B	$0.1B	$0.1B	$0.0B	$0.1B
Arizona	Low	5	$3.1B	$2.1B	$1.1B	$0.6B	$0.2B	$0.4B
Arkansas	Low	5	$1.1B	$0.7B	$0.4B	$0.2B	$0.1B	$0.2B
California	High	5	$58.9B	$12.5B	$46.4B	$11.8B	$9.3B	$2.5B
Colorado	High	5	$7.4B	$2.0B	$5.4B	$1.7B	$1.2B	$0.5B
Connecticut	Low	5	$2.5B	$1.7B	$0.9B	$0.5B	$0.2B	$0.3B
Delaware	Low	5	$0.9B	$0.6B	$0.3B	$0.2B	$0.1B	$0.1B
Florida	Low	15	$9.5B	$6.2B	$3.3B	$2.0B	$0.7B	$1.3B
Georgia	Low	5	$5.8B	$3.8B	$2.0B	$1.1B	$0.4B	$0.7B
Hawaii	Low	5	$0.7B	$0.4B	$0.2B	$0.2B	$0.1B	$0.1B
Idaho	Low	5	$0.7B	$0.5B	$0.3B	$0.2B	$0.1B	$0.1B
Illinois	Medium	5	$9.8B	$4.8B	$5.1B	$1.9B	$1.0B	$0.9B
Indiana	Low	5	$3.5B	$2.3B	$1.2B	$0.7B	$0.2B	$0.4B
Iowa	Low	10	$2.0B	$1.3B	$0.7B	$0.4B	$0.1B	$0.3B
Kansas	Low	5	$1.7B	$1.1B	$0.6B	$0.4B	$0.1B	$0.2B
Kentucky	Low	15	$1.8B	$1.2B	$0.6B	$0.3B	$0.1B	$0.2B
Louisiana	Low	5	$2.2B	$1.5B	$0.8B	$0.5B	$0.2B	$0.3B
Maine	Low	5	$0.5B	$0.4B	$0.2B	$0.2B	$0.1B	$0.1B
Maryland	Medium	10	$4.2B	$2.1B	$2.1B	$0.9B	$0.5B	$0.5B
Massachusetts	Medium	5	$6.4B	$3.1B	$3.3B	$1.2B	$0.6B	$0.6B
Michigan	Low	5	$4.4B	$2.9B	$1.5B	$0.9B	$0.3B	$0.6B
Minnesota	Medium	5	$4.3B	$2.1B	$2.2B	$0.8B	$0.4B	$0.4B
Mississippi	Low	10	$0.9B	$0.6B	$0.3B	$0.2B	$0.1B	$0.1B
Missouri	Low	10	$2.8B	$1.8B	$0.9B	$0.5B	$0.2B	$0.4B
Montana	Low	5	$0.5B	$0.3B	$0.2B	$0.2B	$0.1B	$0.1B
Nebraska	Low	5	$1.4B	$0.9B	$0.5B	$0.3B	$0.1B	$0.2B
Nevada	Low	10	$1.5B	$1.0B	$0.5B	$0.3B	$0.1B	$0.2B
New Hampshire	Low	5	$0.7B	$0.5B	$0.2B	$0.2B	$0.1B	$0.1B
New Jersey	Low	5	$5.1B	$3.4B	$1.7B	$1.1B	$0.4B	$0.7B
New Mexico	Low	15	$0.7B	$0.5B	$0.2B	$0.2B	$0.1B	$0.1B
New York	Medium	5	$21.2B	$9.8B	$11.4B	$4.1B	$2.2B	$1.9B
North Carolina	Medium	10	$7.1B	$3.4B	$3.6B	$1.4B	$0.7B	$0.7B
North Dakota	Low	5	$0.5B	$0.3B	$0.2B	$0.1B	$0.0B	$0.1B
Ohio	Medium	5	$8.1B	$3.9B	$4.2B	$1.5B	$0.8B	$0.7B

Oklahoma	Low	10	$1.6B	$1.0B	$0.5B	$0.4B	$0.1B	$0.2B
Oregon	Low	5	$2.1B	$1.4B	$0.7B	$0.5B	$0.2B	$0.3B
Pennsylvania	Medium	5	$8.9B	$4.3B	$4.6B	$1.7B	$0.9B	$0.8B
Rhode Island	Low	5	$0.5B	$0.3B	$0.2B	$0.1B	$0.0B	$0.1B
South Carolina	Low	10	$2.0B	$1.3B	$0.7B	$0.4B	$0.1B	$0.3B
South Dakota	Low	15	$0.6B	$0.4B	$0.2B	$0.2B	$0.1B	$0.1B
Tennessee	Low	5	$3.3B	$2.2B	$1.1B	$0.6B	$0.2B	$0.4B
Texas	Low	10	$15.3B	$10.0B	$5.3B	$2.9B	$1.0B	$1.9B
Utah	Low	5	$1.8B	$1.2B	$0.6B	$0.4B	$0.1B	$0.2B
Vermont	Low	10	$0.2B	$0.2B	$0.1B	$0.1B	$0.0B	$0.0B
Virginia	High	10	$9.6B	$2.6B	$7.0B	$3.1B	$2.3B	$0.8B
Washington	Low	5	$5.3B	$3.5B	$1.8B	$1.1B	$0.4B	$0.7B
West Virginia	Low	10	$0.6B	$0.4B	$0.2B	$0.1B	$0.0B	$0.1B
Wisconsin	Low	5	$2.8B	$1.9B	$1.0B	$0.6B	$0.2B	$0.4B
Wyoming	Low	5	$0.3B	$0.2B	$0.1B	$0.1B	$0.0B	$0.0B
USA	--	--	$239.3B	$112.2B	$127.1B	$49.5B	$26.4B	$23.1B

DIRECT AND INDIRECT COSTS OF STATE PRIVACY LAWS

The prior analysis shows the magnitude of the potential economic impact of a patchwork of 50 different state privacy laws. However, it is also important to understand the sources of many of these costs. This section discusses some of the primary ways privacy laws impose costs on firms either directly through compliance costs or indirectly by creating market inefficiencies. Notably, duplicative state privacy laws create redundant costs, which means firms spend more on compliance and are subject to additional market inefficiencies while not increasing privacy safeguards for consumers.

Compliance Costs

There are several compliance costs associated with data privacy legislation, including hiring data protection officers, conducting privacy audits, and building and maintaining information systems to facilitate various user rights (e.g., data access, deletion, portability, and correction). Firms must devote resources to regulatory compliance, either by reducing investment in existing products and services or by passing on some of the costs to consumers. While initial compliance costs may be highest, because of certain fixed costs, as this report shows, many of the compliance costs are recurring expenses. Moreover, the costs associated with data privacy laws adversely affect small businesses, often more so than their larger counterparts, because the high costs represent a larger proportion of their revenue. Larger firms are also more likely to have in-house regulatory expertise and to be in compliance with privacy laws outside the United States.

Data Protection Officers

Some data privacy laws require organizations to designate a data protection officer, data privacy officer, or information security officer to be responsible for compliance. For most organizations, this requirement would compel them to hire additional personnel to handle data protection

compliance issues, retain a law firm or similar service provider to handle this responsibility, or divert existing staff to reallocate their time away from other activities.

The GDPR, which many states have cited as a model for their own privacy laws, requires businesses of all sizes and sectors to have a dedicated data protection officer to guarantee compliance with the law.[23] For a small business, hiring a data protection officer would be a significant endeavor likely involving a trade-off between hiring for compliance purposes and hiring for expanding a business's product or service.[24]

Privacy Audits

Some privacy laws require organizations to submit to periodic compliance audits, administered by either their organization or a third party. The GDPR requires some organizations to participate in periodic audits, and even direct inspections by data protection authorities.[25] Similarly, HIPAA requires covered entities to meet certain requirements, which they must prove through periodic audits. These audits create both direct costs and costs of employee time and range in scope depending on the types of data collected and the protections required. According to the health care compliance company Datica, a full HIPAA audit costs between $30,000 and $60,000 in both employee and direct costs.[26]

Data Impact Assessments

Some state privacy legislation requires businesses to perform risk assessments similar to the data protection impact assessments (DPIA) required by the GDPR. These assessments examine the costs and benefits to both the business and user of collecting personal data. While the specific conditions for assessment vary from state to state, they typically apply to the processing of sensitive data. Because these obligations are similar to the GDPR's DPIA requirements, larger companies are more likely to be familiar with the process and complete routine assessments.

Consumer Privacy Rights

State privacy laws often establish new consumers rights over their personal data. Examples of common rights include the right to access personal data stored by an organization, the right to move their personal data to other services, the right to delete their personal data, and the right to correct their personal data. State privacy laws obligate firms to respond to consumer requests, so in order to comply with these requests, firms must account for three types of costs. First, companies must build and maintain information systems that allow them to store, find, delete, and update requested personal information. These are often fixed costs on the back end to allow them to respond to such queries in a timely manner. It may involve, for example, linking multiple disparate systems together so that all consumer data can be queried from a single interface. Second, businesses must create mechanisms and processes to authenticate and document when consumers make those requests. Without sufficient authentication protocols in place, firms may inadvertently expose personal data to bad actors seeking to exploit privacy rights in order to gain access to consumer data.[27] Authentication tools can range in complexity from something as simple as requiring a username and password to access an online service to requiring users to submit government identification that a third-party authentication service reviews to verify an individual's identity. Costs vary depending on complexity, but they can be quite significant. For smaller businesses, the additional requirement of costly authentication tools can quickly add up. Lastly, each new privacy right comes with processing costs that vary depending on the number and types of requests they receive. Although many of these requests come through digital portals,

businesses still need some type of human processing, which can significantly increase labor costs.

Differences in state laws can also create confusion among consumers about their individual data privacy rights. For example, consumers may not understand why firms must process their data one way if they are a resident of one state and another way if they are a resident of another one. These differences between states can also make it harder for businesses, the media, and others to educate consumers about their data rights because they have to tailor their messages to people depending on where they live. Similarly, since different state privacy laws may have unique provisions or require specific disclosures, businesses have to create different privacy policies for each state. With a patchwork of state privacy laws, privacy policies and related notices on apps and websites will likely become even longer, more complex, and harder for consumers to understand.

Market Inefficiencies and Lawsuits

While privacy laws come with clear compliance costs, they also include several indirect costs that adversely impact innovation and limit an organization's ability to do business in a given locale. A patchwork of multiple state privacy laws exacerbates these market inefficiencies because businesses must navigate competing regulations, which can limit their ability to use data effectively. ITIF previously estimated that overly restrictive privacy regulations in the United States could generate $104 billion in market inefficiencies, which would manifest as higher costs, lower productivity (for both organizations and consumers), and decreased innovation.

Privacy laws can constrain businesses from collecting and using data, thereby limiting data-driven innovation and adversely affecting consumers. For example, some biometric laws have prevented businesses from selling certain products and services in those jurisdictions.[28] Other privacy rules, such as data minimization requirements, can prevent firms from collecting more data than necessary for a particular service, even though businesses often do not know what insights they might derive from data until after they have had an opportunity to analyze it. Likewise, purpose specification requirements, found in many privacy laws, mandate that businesses both inform users why they are collecting their personal information and not use that data for any other reason. These restrictions prohibit firms from using the data they have for new purposes, thereby limiting innovation.

Privacy legislation that inhibits the collection and use of personal data can reduce the effectiveness of targeted advertising, thereby hurting not only advertisers that can no longer efficiently access specific audiences, but also app developers, media companies, and content creators that obtain revenue from targeted ads. For consumers, this means a worse Internet experience with less-relevant ads, lower-quality online content and services, and more paywalls.[29]

Beyond general market inefficiencies from less-efficient use of data, a patchwork of state privacy laws also opens the door to inefficiencies from litigation on multiple fronts, especially if some states create a private right of action that allows individuals to file lawsuits against companies for potential violations. Privacy litigation has grown rapidly in recent years, with certain laws clearing the way for a proliferation of class action lawsuits. A patchwork of state laws with varying definitions and standards creates a complex regulatory minefield for businesses to navigate, especially if potential violations risk costly litigation.

BIPA, for example, demonstrates the potential for costly litigation. It was designed to regulate the collection of biometric data by companies operating in a given state or whose products reach consumers in that state. The state privacy law includes a private right of action that allows both consumer class action lawsuits and employer lawsuits. Although BIPA passed into law in 2008, most lawsuits have occurred more recently after the Illinois Supreme Court held in 2019 that individuals are not required to show harm and instead can file lawsuits even when there has only been a technical violation of BIPA.[30] Likewise, a ruling by the U.S. Court of Appeals for the Ninth Circuit found that plaintiffs had legal standing for filing lawsuits alleging technical violations of BIPA.[31] Since then, a definitive trend has taken hold, as the Illinois courts have ruled in favor of plaintiffs in most class action suits.

Since 2019, the number of BIPA lawsuits has skyrocketed, with many high-profile cases. In March 2021, Facebook paid $650 million in a case filed over the social media platform's use of facial recognition technology for tagging in photos.[32] As a result, almost 1.6 million Illinois residents will receive $345 or more.[33] Similarly, in April 2021, security company ADP paid a $25 million settlement for supplying equipment and support to employers that required workers to scan their fingerprints. Over 40,000 residents filed claims.

There have also been BIPA lawsuits against employers. Walmart settled for $10 million in June 2021 due to the company's use of palm-scanning technology.[34] Over 20,000 employees were involved in the case—which stemmed from Walmart giving employees that needed to take out their cash-register drawers at the end of their shifts the option of using a biometric scanner, rather than entering a PIN code, to verify their identities—due to their use of the technology without giving written consent, although no actual injury was involved. Walmart subsequently deleted all data and ended the scanning option in Illinois.

The number of lawsuits filed under BIPA has grown over time. In 2019, there were around 300 lawsuits, and the number of cases referencing BIPA doubled in 2020.[35] The legal specifics, such as the private right of action and the grounds for standing make taking legal action for biometric data collection all too easy in Illinois. The consequences of BIPA have implications not only for Illinois but other states considering stringent biometrics laws as well. As there is currently no such federal data privacy law, states must consider the collective cost of class action litigation on their economies. Some companies, such as Clearview AI, have pulled out of Illinois altogether, while others limit the technology available to consumers.[36] For example, Nest (smart home devices) will not include facial recognition features for Illinois consumers. Similarly, Google never released its Arts and Culture app outright in Illinois due to BIPA-compliance concerns.

BIPA is not alone in creating a wave of privacy litigation. As the standard for privacy legislation in the United States, the CCPA has been the focus of over 190 lawsuits since it was enacted in 2020.[37] Regulating any firm that "does business in California," the law even applies to those without a physical presence in the state. With a private right of action for those wherein consumer information "is subject to an unauthorized access and exfiltration, theft, or disclosure," many cases have emerged that argue businesses have failed to maintain necessary security procedures. The number of cases increases each year, with 125 claims filed in 2021.[38]

Class action lawsuits can lead to major settlements, thereby threatening the viability of smaller businesses. Even if a business can prevail in a lawsuit, the costs of the lawsuit are often significant, especially in state courts that are often more favorable for plaintiffs in class action

litigation compared with federal courts and allow for expensive discovery processes, such as requesting documents and witness interviews, that can drive up the costs of litigation very quickly.

CONCLUSION

Poorly designed data privacy laws can impose a substantial toll on the economy through both direct compliance costs and indirect costs from lower productivity and constraints on innovation; and when multiple states subject businesses to conflicting privacy laws, they increase these costs. To avoid conflicting laws and unnecessary costs, Congress should act swiftly to pass comprehensive privacy legislation that preempts state laws, streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation (e.g., by avoiding requirements for data minimization, universal opt-in, purpose specification, limitations on data retention, or privacy-by-design). This legislation should not include a private right of action and instead rely on federal and state regulators for enforcement. Establishing a comprehensive federal privacy law would also simplify compliance for businesses, especially small businesses working across multiple U.S. jurisdictions, as well as help consumers better understand their privacy rights and avoid the confusion resulting from a patchwork of state laws.

APPENDIX A: DETAILED METHODOLOGY

This analysis is informed by best practices in modeling the effects of data regulation between nations as demonstrated by the Organization for Economic Cooperation and Development (OECD) and the European Center for International Political Economy (ECIPE).[39]

State Restrictiveness Scores

SRSs are calculated as a function *f* of both in-state and out-of-state privacy restrictions on consumer data.

$$SRS = f(\text{in-state restriction, out-state restriction})$$

The table on state privacy laws shown in appendix B is the source document referenced in calculating SRS. States occupying larger shares of national data-concerned industries are assumed to be of greater weight in the composition of a state's contribution of SRS resulting from out of state. Since all applicable businesses within a state would require direct compliance with their own state's laws, in-state restrictions are taken as unweighted. Out-of-state restrictions would only impact multistate operations complying in those other states, which would be a smaller fraction than all businesses based within the state. To provide a weight to the contribution of out-of-state restrictions into the calculation of SRS, ITIF's model uses deflator *d* as a state-specific coefficient for out-of-state restrictions. The equation for deflator *d* of state *x* is below.

$$d_x = \frac{(Consumer\ Products\ Share_x + Consumer\ Finance\ Share_x + Advertisement\ Share_x)}{3}$$

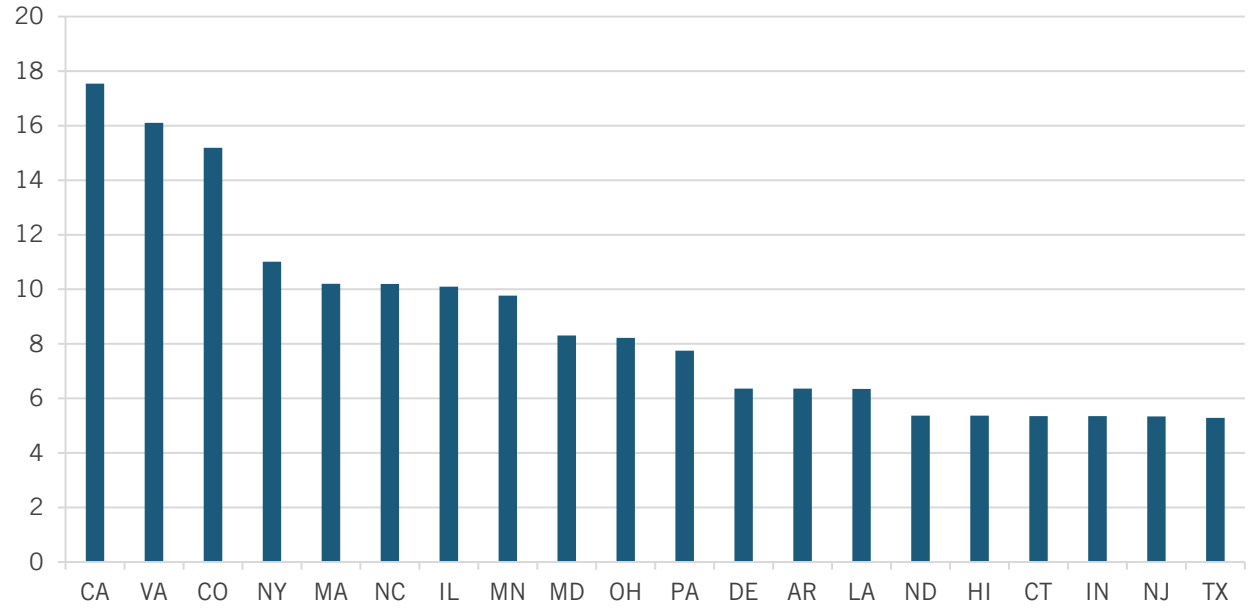
A state's deflator is the unweighted average of its share of U.S. GDP in the consumer products, consumer finance, and advertising industries. *d* is calculated using only 2019 data for all states and is applied to all years' calculations of SRS to control for issues of endogeneity. Data on a state's share of the national consumer products industry is taken from BEA's Regional Data table on retail trade as a percentage of the U.S. industry's GDP. Data on a state's share of the national consumer finance industry is taken from BEA's Regional Data table on finance and insurance as the state's percentage of the U.S. industry's GDP. Lastly, data on a state's share of national advertising spending is taken from a 2019 Statista dataset and study of U.S. total advertisement spending. Using *d* to deflate the value of out-of-state laws in the calculation of SRS, the equation for SRS of state *x* during year *y* is below.

$$SRS_{xy} = \sum_{n=2003}^{y} (State\ Privacy\ Restriction_{xn}) + \sum_{j \neq x} d_j * \sum_{n=2003}^{y} (State\ Privacy\ Restriction_{jn})$$

SRS is equal to the unweighted cumulative sum of state privacy restrictions passed up to year *y* in state *x*, plus the cumulative sum of deflated state privacy restrictions across states other than *x* passed up to year *y*. These scores provide a common quantitative scale to measure the level of restrictiveness imposed onto a state's consumer data, wherein higher SRS means stricter compliance/enforcement regarding data privacy. While some privacy restrictions are undoubtedly of higher economic cost than others (e.g., laws requiring rights to access, deletion, data portability, and rectification would levy higher compliance costs than laws requiring privacy

audits would), this model provides no weighting to the value of state privacy restrictions in the calculation, in order to simplify methodology.

Figure 5: Highest SRSs in 2021

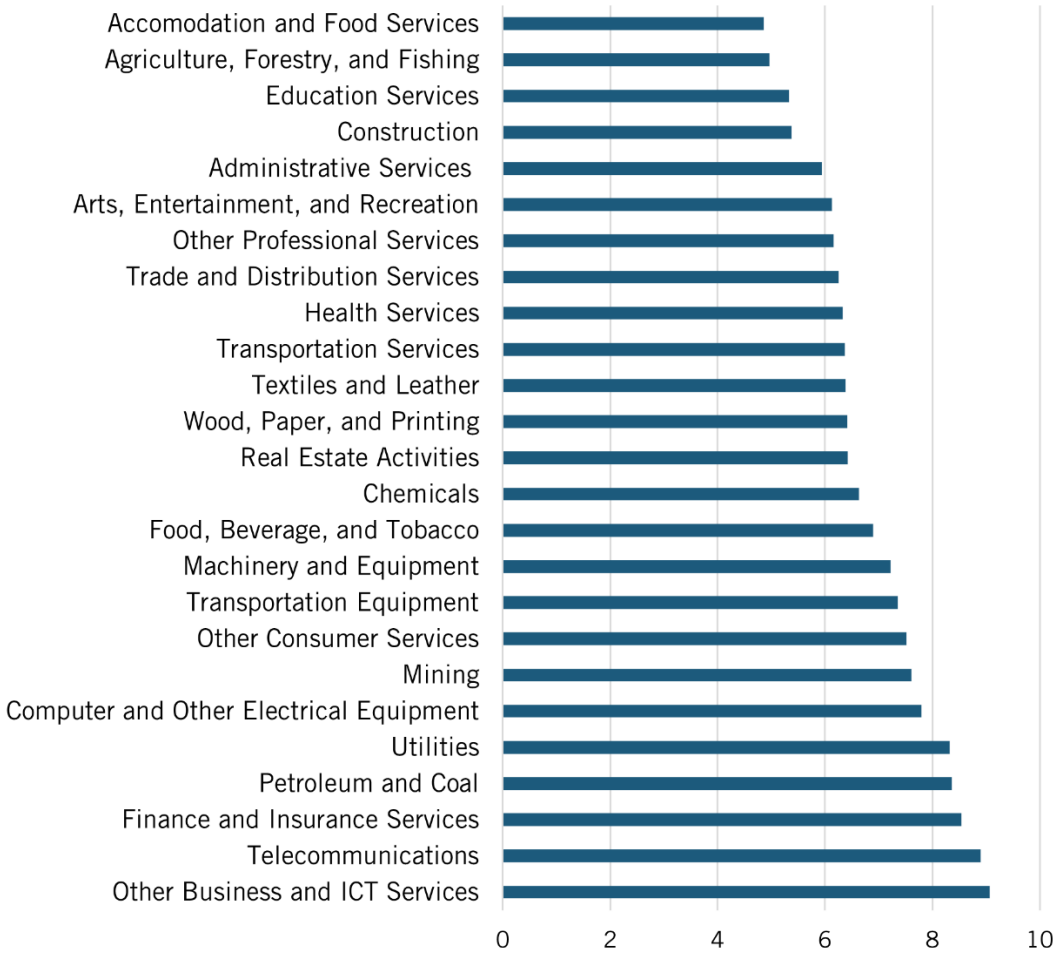


Data-Intensity Modifiers

ITIF's model assumes that restrictions on consumer data have greater effects on industries that are more reliant on data and data-related tools and services. To best weigh state-level measurements of SRS at the precision of industry-specific scores, a DIM is calculated to help correct for bias in the proxy SRS by weighting each downstream industry's linkage with state privacy restrictiveness for every industry within the North American Industry Classification System (NAICS) categorization. Furthermore, this model selects U.S. national data as a reference in a given baseline year for computing industry-specific measurements of DIM to be applied to states in the sample. However, this approach assumes that all U.S. states have technologies equal to the national estimated for the United States. U.S. Census ICT 2013 Survey data on intangible software expenditure and BLS data of employment by industry in the same year are gathered to compute the ratios of data-related service expenditures per worker in each industry. ITIF's methodology for calculating DIM is based on best practice as demonstrated by ECIPE's studies on data localization. Employment is recorded in number of workers employed, and noncapitalized software expenditure is recorded in millions of U.S. Dollars. DIM is taken as a natural log to align with previous literature on factor intensity.

$$DIM_z = \ln\left(\frac{Intangible\ Software\ Expenditure_z}{Employment_z}\right)$$

Figure 6: Data intensity by Industry (as a log of noncapitalized software expenditures per worker)



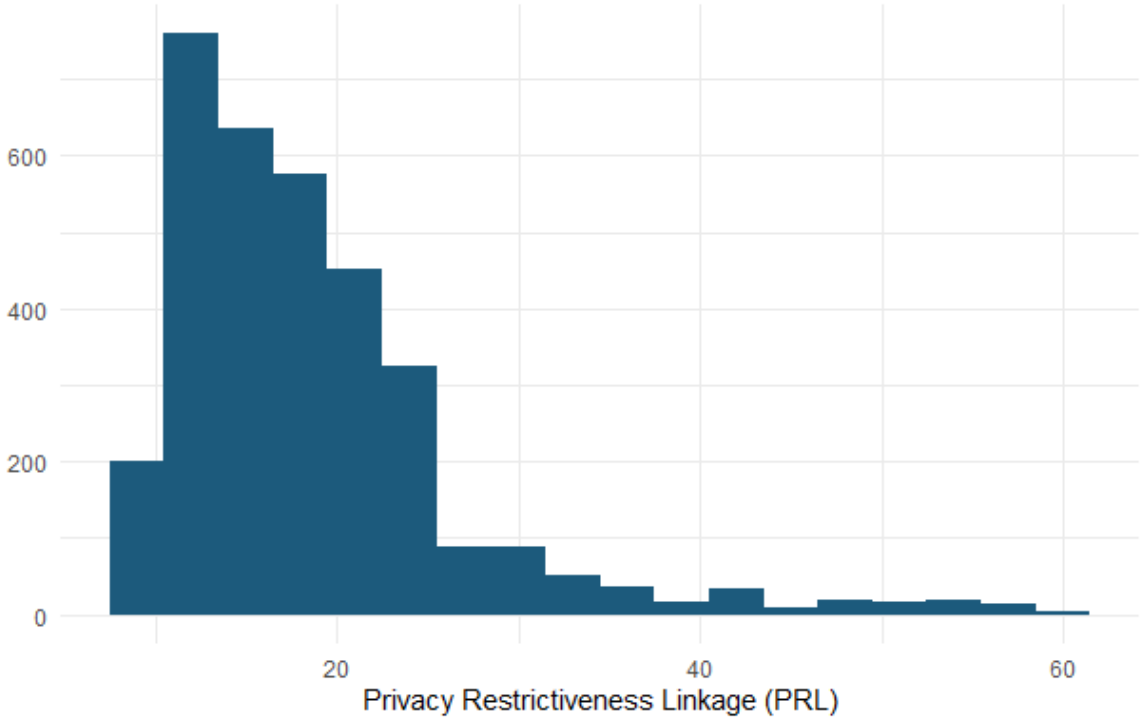
The proxies SRS by state and DIM by industry function as components of a composite index at the state-industry level. This composite index links the level of privacy restrictiveness within a state to the level of data reliance faced by an industry in order to provide measurement on the level of effective restrictiveness faced by a state's industries due to privacy restrictions passed by that state. This PRL is the composite index and final independent variable observed to analyze the economic impact of privacy laws on industries. Conducting this analysis at the level of state-industry-year rather than just state-year provides greater precision in identifying a statistical relationship between privacy laws and economic performance. Since not every industry relies on data equally, not every industry within a state will be equally impacted by its privacy law changes. The product of a state's SRS with an industry's DIM gives the PRL of that industry within the state. The equation for PRL of state-year-industry x, y, and z is below.

$$PRL_{xyz} = SRS_{xy} * DIM_{z}$$

PRL is recorded over a panel between years 2003 to 2021 for 50 U.S. states among 25 NAICS industries included by the U.S. BEA's Regional Data tables on industry GDP in order to be compatible with response variable data. Note that total number of observations will not equal the

total number of entries recorded for PRL due to missing responses and control variables. Since most states so far do not impose privacy laws to similar levels of stringency found in California, most PRL in early years in the panel data is accounted for by out-of-state restrictions in the calculation of SRS. Further, since most states have not yet determined their privacy law, distribution of PRL will be skewed by early actors. As a result, the distribution of PRL in years 2018 and on yield the following histogram. The distribution of PRL is positively skewed above the normal. While still skewed and dealing with imperfect data, correcting for variation in data intensity among industries helps normalize the predictor variable, whereas a vector of SRS values would otherwise be irregularly distributed and thus less suitable for regression.

Figure 7: Distribution of PRL



This econometric exercise is informed by best econometric practices in modeling the effects of data regulation between nations as demonstrated by OECD and ECIPE.[40] ITIF's econometric model selects GOS as its main response variable based on economic theory and statistical convenience. GOS is the residual earnings among corporations within an industry after subtracting their total intermediate expenses and compensation of employees. GOS can therefore be understood as a measurement of an industry's net economic performance. This makes GOS a fitting response variable since this model's purpose is to examine how a state's industry earnings are impacted by a rise in state privacy laws adopted across 50 U.S. states.

Further, GOS has direct implications for GDP. GDP can be calculated by three main approaches, and while it is chiefly calculated by the production approach (the sum of all domestically created goods and services), the income approach to GDP relies in part on GOS to calculate GDP. The income approach calculates GDP as the sum of total incomes, including total net corporate earnings. Net corporate earnings are often represented in this calculation with GOS, meaning

that a change to a state's GOS, by the income approach to GPD, marks an equivalent change in GDP.

The composition of GOS makes it doubly useful in capturing costs associated with privacy law restrictions. Privacy laws impose explicit costs on firms through added forms of compliance that cost more to satisfy. Privacy laws also impose effective costs on firms by limiting the utility and usability of data. If consumer data is rendered less transferrable or has its range of uses limited, then that data becomes less monetizable and thus less valuable. These kinds of restrictions create market inefficiencies that lower firms' total output, effectively imposing additional costs on firms impacted by such laws. GOS can be broadly represented by the equation below.

$$GOS = Total\ Output - Intermediate\ Expenses\ - Compensation\ of\ Employees$$

Higher compliance costs result in higher intermediate expenses or higher compensation of employees, thus lowering GOS. Higher costs due to market inefficiencies lower total output, which also lowers GOS. Therefore, GOS should capture both kinds of costs associated with privacy laws. Additionally, an industry containing many multistate operations would report lower GOS due to duplicative costs of compliance with other states and the operational costs (captured by intermediate expenses and further compensation of employees) associated with discerning a patchwork system of 50 different privacy laws in place of one unifying federal law on consumer data.

Despite the advantages of GOS, ITIF's model still draws compromises due to issues in data availability. A key statistic of use for this model is industry-level trade data, in both goods and services, between U.S. states; however, to our knowledge, there is no freely available public dataset on this matter. Further, in economic census datasets collected by the U.S. Census, there is currently no publicly available data on the share of enterprises in each state that are multistate operations. For these reasons, we resort to proxies in calculating the final composite index PRL that serves as the model's predictor variable.

Regression Model

The purpose of this regression modeling is to measure the statistical relationship between the index of a state-year-industry's PRL and its GOS. This report constructs a multivariate linear regression model using the ordinary least squares (OLS) method of linear regression. The lead regression model detailing this relationship is below.

$$ln(\widehat{GOS})_{xyz} = \hat{\beta}_0 + \hat{\beta}_1 * PRL_{xyz} + \hat{\beta}_2 * GDP_{xy} + \alpha_y + \gamma_z + \varepsilon_{xyz}$$

$ln(\widehat{GOS})_{xyz}$ represents the response variable GOS as a natural log. GOS is taken as a natural log in order to model a log-linear relationship and help normalize the distribution of GOS for a data frame better suited for regression. This regression model, with results summarized in the following table, regresses a log-linear relationship by the OLS method in order to estimate the percentage change in GOS associated with a 1-unit change in the predictor variable, PRL. $\hat{\beta}_0$represents the y-intercept estimate. $\hat{\beta}_1$ represents the coefficient estimate on the predictor variable PRL. $\hat{\beta}_2$ represents the coefficient estimate on the control variable state GDP. $\alpha_y$represents yearly fixed-effects in which the model assumes errors in residuals are in part owed to unobservable variation within data between years but is constant between states and industries (e.g., national economic shocks that change between years but are of common impact

on states and industries). γ_z represents industry fixed effects in which the model assumes errors in residuals are also owed to unobservable variation within data across different industries, as there are many factors that determine industry-specific performance that are together not easily captured by other controls. Lastly, ε_{xyz} represents residual error that varies for each fitted value.

Table 1: Regression Table

	Coefficient Estimate	Standard Error	t-value	Pr(>|t|)
Intercept	13.27	0.10	132.8	< 2e-16
PRL	-0.00389	0.00115	-3.78	0.000737
GDP	1.025e-09	2.6e-11	39.4	< 2e-16

R-Squared: 0.734, Number of Observations: 3,984

Comparisons to Bottom-Up Modeling

This model differs from previous work from ITIF and others on modeling the costs of state privacy laws in that it employs econometric analysis. It is a top-down model whereby looking at a high-level residual in industry economic performance over time captures an aggregated change of multiple factors (compliance costs, market inefficiencies, duplicative costs, etc.). The top-down model gives strong insight into a total change in performance via loss in GOS, which estimates a total cost/economic burden incurred on states through the adoption of additional state privacy laws; however, since GOS is made of multiple components, ITIF's model is not able to discern exactly which components comprising GOS are changing and by how much. A model capable of identifying separate cost components with greater specificity can be better thought of instead as a bottom-up model. This is because a model like this would be identifying separate costs associated with added privacy laws and summing them up to derive a total cost borne by states. While data-constraints are present in the top-down model, a bottom-up model is especially constrained by the availability of data. A top-down model requires analyzing a response variable that encompasses multiple relevant factors in order to identify a statistical relationship, whereas a bottom-up model needs a unique dataset to identify costs for each line item included in the model. For example, increased legal costs through more lawsuits is captured in GOS due to increased intermediate expenses of legal services, which would incur a loss in GOS. However, there would be no way to identify what portion of a loss in GOS would be due to increased legal costs. In a bottom-up model, one would need a separate dataset capable of targeting increased legal costs associated with more lawsuits incurred by a change in a state's privacy laws, but such a model would be capable of identifying specific costs with greater precision. But given the lack of free and publicly available costs around specific economic burdens created by additional privacy law restrictions, a bottom-up model is less feasible. To address holes in a bottom-up model's demand for data, modelers would need to supplement their methodology with either survey data or suitable proxies. Survey data on self-reported costs on different restrictions induced by a change in state privacy law could help obtain information that is otherwise private; however, that data is only as effective as its survey. A 2019 Berkeley Economic Advising and Research report sanctioned by the Office of the California Attorney General conducts a similarly

structure bottom-up model, supplementing holes in data with robust survey data taken from California firms reporting costs. Given the challenges inherent to conducting an effective and accurate survey, ITIF declines to supplement a bottom-up model with survey data. A bottom-up model also faces the challenge of identifying a state's costs for its businesses to comply with privacy laws set in other states. This model's main purpose is to quantify the cost of compliance with multiple states' privacy laws, and to model a hypothetical scenario wherein all 50 states have established their own privacy law, which is made possible by the calculation of SRS as a function of both in-state laws and (to a lesser degree by the deflator equation *d*) out-of-state laws. Capturing the costs associated with a system of multistate compliance in a bottom-up model would require information on the value of trade from businesses in state *a* to purchasers in state *b (*and to purchasers in state *c,* and so on*)*. There is currently no dataset, to our knowledge, that covers this exchange to the specificity of NAICS industries. Therefore, without survey-data or access to a privately held database on industry-level trade between states, a bottom-up model lacks the ability to capture the cost effect imposed on firms by having to navigate a multistate system of divergent privacy laws. For these reasons, ITIF instead conducts the elaborated top-down econometric model presented in this report.

Nevertheless, a state's costs incurred by its own in-state privacy laws estimated by the top-down model in this report can be compared with a bottom-up model calculating only a state's costs due to in-state privacy laws (excluding out-of-state effects). ITIF constructs an example bottom-up model in order to compare its national estimate on the cost of in-state privacy laws against the estimates of the costs of in-state privacy laws projected by this report's top-down model. The methodology for this example of a bottom-up model follows ITIF's 2019 report "The Costs of Unnecessarily Stringent Federal Data Privacy Law," except it excludes the line item for data protection officers (DPOs), since a rule on DPOs was ultimately kept out of the CCPA. All calculations are based on both the number of enterprises by size in a state, the actual privacy laws passed in a state, and a state's share of national data-concerned industries.

Table 2: Comparing sample estimates of a bottom-up model

Line Item	Annual National Cost (Totaled among U.S. States) in 2020	Methodology
State Audit Costs	$189 million	0.5 percent of firms are estimated to be audited annually. Small enterprises (fewer than 20 employees) and nonprofits have estimated audit costs equal to $10,000. Medium-sized enterprises (between 20 and 500 employees) have estimated audit costs equal to $30,000. Large enterprises (more than 500 employees) have estimated audit costs equal to $60,000. Each state's total costs are calculated based on the number of firms by size and their number of in-state restrictions on privacy laws during 2021. National cost is taken as the sum of all state costs.
Cost of Database Administrators (Requirements on Updating and Maintaining Data Infrastructure)	$18.5 billion	Additional database administrators (DAs) would be needed to comply with requirements on updating and maintaining data infrastructures. Annual cost of a database administrator salary is $91,000. Small firms and nonprofits would require additional hiring on average of 0.05 new DAs, medium-sized firms on average would hire an additional 0.1 new DAs, and large firms would on average hire an additional 1 new DA. Each state's total costs are calculated based on the number of firms by size and their number of in-state restrictions on privacy laws during 2021. National cost is taken as the sum of all state costs.
Cost of Legal Enforcement (Lawsuits)	$1.4 billion	Due to the challenge of acquiring and preparing legal data between national and state agencies, this line item is proxied using ITIF's 2019 report estimate on the cost of lawsuits throughout the country due to enforcing data privacy laws. ITIF estimated a national cost of $2.7 billion due to a federal law applying to all states equally strict as CCPA. This statistic of $2.7 billion is scaled down to account for the actual number of privacy law restrictions in place within each state during 2021. Rescaling this statistic, in which state costs are scaled based on actual privacy laws rather than privacy laws equal to CCPA, gives a new sum across states equal to $1.4 billion.
Right to Access, Deletion, Data Portability, and Rectification	$3.5 billion	ITIF's 2019 report estimates data access, deletion, portability, and rectification requirements would cost the United States $7.2 billion, which assumes all states would enact state laws equally strict to California's CCPA. This estimate is rescaled based on the actual laws passed by states through 2021, which gives a new estimate of $3.5 billion.
Productivity Loss in Online Services	$935 million	ITIF's 2019 report estimates the productivity loss in online services incurred by all states with equal privacy laws to CCPA would equal $1.9 billion nationally. This estimate is rescaled by each state's share of online services in the United States (proxied by national advertising share) and by their actual state privacy laws passed as of 2021, which gives a new estimate of $935 million.
Losses Due to Inefficiencies of Less Data	$32.8 billion	ITIF's 2019 report estimates the national cost of economic losses due to market inefficiencies created by privacy laws restricting data would equal $71 billion. This estimate assumes that each U.S. state would have privacy laws equal to CCPA. This estimate is rescaled by each state's share of data-concerned industries and by their actual state privacy laws passed, giving each state a new estimated cost. The sum of rescaled estimated costs among states equals $33 billion.

Losses Due to Inefficiencies in Advertising	$22.5 billion	ITIF's 2019 report estimates a national cost of $33 billion in economic value lost due to less-effective advertising inhibited by increased privacy laws. The $33 billion is scaled up relative to the growth in total advertising between 2018 and 2021, estimating a $46 billion loss nationally. However, this $46 billion estimate assumes all states have privacy laws equal to California's. State estimates on their share of loss due to ineffective advertising are rescaled based on their shares of the national advertising industry and by their actual set of passed state privacy laws as of 2021. The sum of rescaled state estimates for 2021 is equal to $22.5 billion.
Annual Total Cost of In-State Privacy Laws in 2021 (Bottom-Up Model)	$79.9 billion	Sum of all other line items in this sample bottom-up model.
Annual Total Cost of In-State Privacy Laws in 2021 (Top-Down Model)	$95.3 billion	Using regression coefficients estimated from the econometric model in this report on PRL, each state's actual GOS loss due to PRL in 2021 is estimated, and out-state costs are subtracted from each state's total estimated GOS loss. The sum total of state costs due to in-state privacy laws estimated by the top-down model is equal to $95 billion.
Difference in Estimates (Bottom-Up – Top-Down)	- $15.4 billion	The estimate on in-state costs from the bottom-up model is approximately $15 billion less than what is estimated by the top-down model.

This sample methodology on bottom-up costs helps provide, with greater specificity, estimates for economic burdens faced by states from their own in-state privacy laws. There is a notable discrepancy between these two estimates because a bottom-up model requires complete and accurate information regarding the factors influenced by privacy laws, which is nearly impossible given the complexity of the issue. As a result, costly line items concerning matters of compliance costs, both direct and indirect, and of market inefficiencies are likely to be missed or underestimated, explaining the difference in estimates. Regardless, the previous table helps demonstrate where, due to an increase in a state's own passed privacy law restrictions, some of the actual costs that amount to a loss in GOS come from and what they could amount to.

Time Horizon Model

Now that a statistical relationship is estimated between a state's change in PRL by 1 unit against a percentage loss in its GOS, ITIF's model can be extended to a scenario in which all states are assumed to pass some version of their own state privacy laws. States would adopt their own laws at different times, as some states would be less quick to adopt legislative changes than others. To model the time horizon over which each state would be estimated to determine their own set state privacy laws, ITIF uses the case study of data breach laws adopted by U.S. states. Each of the 50 states has its own version of data breach laws, but they have adopted those laws in different times. In total, between the first and last state to enact their own data breach laws, 15 years passed (between 2003 to 2018). From this example, ITIF constructs a time horizon model in which all 50 states enact (and settle) their own state privacy laws over 15 years. In that span, states are modeled to have passed their own laws during either the first five years (years 1–5), the second five-year span (years 6–10), or the last five years (years 11–15). If a state has already passed and settled its own state privacy laws as of 2021, then it is automatically modeled to have passed its privacy laws during the first five years. To simplify estimates over this time horizon of 15 years, states are modeled to adopt one of three possible levels of strictness in data

privacy: high (in-state privacy laws = 10 [for calculation of SRS scores]), medium (in-state privacy laws = 4), and low (in-state privacy laws = 2). Using these totals for a state's number of in-state privacy laws, each state's SRS (and therefore PRL values) can be calculated over this hypothetical 15-year period. The following table demonstrates each U.S. state's estimated cost of a 50-state privacy law patchwork over the 15-year time horizon.

Table 3: Annual state total costs of a 50-state privacy patchwork

			Years 1-5			Years 6-10			Years 11-15		
State	Estimated Strictness of Privacy Law	Latest Year of Adoption	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws
AL	Low	15	$1.1B	$0.0B	$1.1B	$1.2B	$0.0B	$1.2B	$1.9B	$0.6B	$1.2B
AK	Low	10	$0.2B	$0.0B	$0.2B	$0.4B	$0.1B	$0.3B	$0.4B	$0.1B	$0.3B
AZ	Low	5	$2.9B	$1.1B	$1.8B	$3.1B	$1.1B	$2.0B	$3.1B	$1.1B	$2.1B
AR	Low	5	$1.0B	$0.4B	$0.6B	$1.0B	$0.4B	$0.7B	$1.1B	$0.4B	$0.7B
CA	High	5	$56.6B	$46.4B	$10.3B	$58.2B	$46.4B	$11.8B	$58.9B	$46.4B	$12.5B
CO	High	5	$7.2B	$5.4B	$1.8B	$7.3B	$5.4B	$1.9B	$7.4B	$5.4B	$2.0B
CT	Low	5	$2.3B	$0.9B	$1.5B	$2.5B	$0.9B	$1.6B	$2.5B	$0.9B	$1.7B
DE	Low	5	$0.8B	$0.3B	$0.5B	$0.8B	$0.3B	$0.5B	$0.9B	$0.3B	$0.6B
FL	Low	15	$5.6B	$0.0B	$5.6B	$6.1B	$0.0B	$6.1B	$9.5B	$3.3B	$6.2B
GA	Low	5	$5.3B	$2.0B	$3.4B	$5.7B	$2.0B	$3.7B	$5.8B	$2.0B	$3.8B
HI	Low	5	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B	$0.7B	$0.2B	$0.4B
ID	Low	5	$0.7B	$0.3B	$0.4B	$0.7B	$0.3B	$0.5B	$0.7B	$0.3B	$0.5B
IL	Medium	5	$9.2B	$5.1B	$4.1B	$9.6B	$5.1B	$4.5B	$9.8B	$5.1B	$4.8B
IN	Low	5	$3.3B	$1.2B	$2.0B	$3.5B	$1.2B	$2.2B	$3.5B	$1.2B	$2.3B
IA	Low	10	$1.1B	$0.0B	$1.1B	$1.9B	$0.7B	$1.2B	$2.0B	$0.7B	$1.3B
KS	Low	5	$1.5B	$0.6B	$1.0B	$1.6B	$0.6B	$1.0B	$1.7B	$0.6B	$1.1B
KY	Low	15	$1.0B	$0.0B	$1.0B	$1.1B	$0.0B	$1.1B	$1.8B	$0.6B	$1.2B
LA	Low	5	$2.0B	$0.8B	$1.3B	$2.2B	$0.8B	$1.4B	$2.2B	$0.8B	$1.5B
ME	Low	5	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.4B
MD	Medium	10	$4.0B	$2.1B	$1.8B	$4.1B	$2.1B	$2.0B	$4.2B	$2.1B	$2.1B
MA	Medium	5	$6.0B	$3.3B	$2.7B	$6.3B	$3.3B	$3.0B	$6.4B	$3.3B	$3.1B
MI	Low	5	$4.0B	$1.5B	$2.5B	$4.3B	$1.5B	$2.8B	$4.4B	$1.5B	$2.9B
MN	Medium	5	$4.0B	$2.2B	$1.8B	$4.2B	$2.2B	$2.0B	$4.3B	$2.2B	$2.1B
MS	Low	10	$0.5B	$0.0B	$0.5B	$0.9B	$0.3B	$0.6B	$0.9B	$0.3B	$0.6B
MO	Low	10	$1.6B	$0.0B	$1.6B	$2.7B	$0.9B	$1.7B	$2.8B	$0.9B	$1.8B
MT	Low	5	$0.4B	$0.2B	$0.3B	$0.4B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
NE	Low	5	$1.2B	$0.5B	$0.8B	$1.3B	$0.5B	$0.9B	$1.4B	$0.5B	$0.9B
NV	Low	10	$0.9B	$0.0B	$0.9B	$1.5B	$0.5B	$1.0B	$1.5B	$0.5B	$1.0B
NH	Low	5	$0.6B	$0.2B	$0.4B	$0.7B	$0.2B	$0.4B	$0.7B	$0.2B	$0.5B
NJ	Low	5	$4.7B	$1.7B	$2.9B	$5.0B	$1.7B	$3.2B	$5.1B	$1.7B	$3.4B
NM	Low	15	$0.4B	$0.0B	$0.4B	$0.5B	$0.0B	$0.5B	$0.7B	$0.2B	$0.5B
NY	Medium	5	$19.8B	$11.4B	$8.4B	$20.8B	$11.4B	$9.4B	$21.2B	$11.4B	$9.8B
NC	Medium	10	$3.1B	$0.0B	$3.1B	$6.9B	$3.6B	$3.3B	$7.1B	$3.6B	$3.4B
ND	Low	5	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
OH	Medium	5	$7.6B	$4.2B	$3.4B	$7.9B	$4.2B	$3.8B	$8.1B	$4.2B	$3.9B

OK	Low	10	$0.9B	$0.0B	$0.9B	$1.5B	$0.5B	$1.0B	$1.6B	$0.5B	$1.0B
OR	Low	5	$1.9B	$0.7B	$1.2B	$2.0B	$0.7B	$1.3B	$2.1B	$0.7B	$1.4B
PA	Medium	5	$8.3B	$4.6B	$3.8B	$8.7B	$4.6B	$4.1B	$8.9B	$4.6B	$4.3B
RI	Low	5	$0.4B	$0.2B	$0.3B	$0.4B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
SC	Low	10	$1.2B	$0.0B	$1.2B	$2.0B	$0.7B	$1.3B	$2.0B	$0.7B	$1.3B
SD	Low	15	$0.3B	$0.0B	$0.3B	$0.4B	$0.0B	$0.4B	$0.6B	$0.2B	$0.4B
TN	Low	5	$3.1B	$1.1B	$1.9B	$3.3B	$1.1B	$2.1B	$3.3B	$1.1B	$2.2B
TX	Low	10	$11.6B	$2.7B	$8.9B	$14.9B	$5.3B	$9.6B	$15.3B	$5.3B	$10.0B
UT	Low	5	$1.7B	$0.6B	$1.1B	$1.8B	$0.6B	$1.2B	$1.8B	$0.6B	$1.2B
VT	Low	10	$0.1B	$0.0B	$0.1B	$0.2B	$0.1B	$0.2B	$0.2B	$0.1B	$0.2B
VA	High	10	$9.3B	$7.0B	$2.3B	$9.5B	$7.0B	$2.5B	$9.6B	$7.0B	$2.6B
WA	Low	5	$4.9B	$1.8B	$3.0B	$5.2B	$1.8B	$3.3B	$5.3B	$1.8B	$3.5B
WV	Low	10	$0.4B	$0.0B	$0.4B	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B
WI	Low	5	$2.6B	$1.0B	$1.6B	$2.7B	$1.0B	$1.8B	$2.8B	$1.0B	$1.9B
WY	Low	5	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B
US	--	--	$209.3B	$111.8B	$97.5B	$229.6B	$122.1B	$107.5B	$239.3B	$127.1B	$112.2B

Small Business Estimates

ITIF estimates the costs that this 50-state privacy law patchwork would impose on small businesses by using the above annual costs per state over the 15-year time horizon. To do this, ITIF estimates the share of GOS loss in each state that would be borne by small businesses. For this extended exercise, small businesses are simplified as enterprises employing fewer than 50 people. This process requires the US. Census Statistics on U.S. Businesses tables, among which is the 2021 SUSB table "The Number of Firms and Establishments, Employment, and Annual Payroll by State, Industry, and Enterprise Employment Size: 2018." This source data provides both the number of enterprises by size for each state as well as the amount of payroll paid out from enterprises by size. Using this data, ITIF calculates the share of each state's total payroll paid out by small businesses. These shares serve as a proxy for each state's total GOS earned by small businesses. When the time horizon estimates a loss in GOS, small businesses are modeled to bear a loss equal to the proxy small business share of GOS times the total loss in GOS (equation below for state *x* during year *y*).

$$.Small\ Business\ Cost_{xy} = \left(\frac{Small\ business\ Payroll_x}{Total\ Payroll_x}\right) * GOS\ Loss_{xy}$$

However, this method of calculating the cost borne by small businesses assumes that estimated losses in GOS fall proportionally along firms by size as they would comprise total GOS. Burdens may fall disproportionately greater on small or large businesses depending on the specificities of laws enacted, which are not able to modeled in the time horizon model since the scenario assumed is hypothetical. Ahead is a time horizon of the annual costs by state borne by small businesses due to the 50-state privacy law scenario.

Table 4: Annual state small business costs due to a 50-state privacy patchwork

		Years 1-5			Years 6-10			Years 11-15		
State	Estimated Small Business Share of GOS	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws	Total Costs	Costs Due to In-State Laws	Costs Due to Out-of-State Laws
AL	21.4%	$0.2B	$0.0B	$0.2B	$0.3B	$0.0B	$0.3B	$0.4B	$0.1B	$0.3B
AK	26.7%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B
AZ	19.1%	$0.5B	$0.2B	$0.3B	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B
AR	21.7%	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.2B
CA	20.0%	$11.3B	$9.3B	$2.0B	$11.6B	$9.3B	$2.4B	$11.8B	$9.3B	$2.5B
CO	22.8%	$1.6B	$1.2B	$0.4B	$1.7B	$1.2B	$0.4B	$1.7B	$1.2B	$0.5B
CT	20.2%	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
DE	21.3%	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
FL	20.7%	$1.2B	$0.0B	$1.2B	$1.3B	$0.0B	$1.3B	$2.0B	$0.7B	$1.3B
GA	18.7%	$1.0B	$0.4B	$0.6B	$1.1B	$0.4B	$0.7B	$1.1B	$0.4B	$0.7B
HI	23.2%	$0.1B	$0.1B	$0.1B	$0.1B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
ID	28.9%	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
IL	19.3%	$1.8B	$1.0B	$0.8B	$1.9B	$1.0B	$0.9B	$1.9B	$1.0B	$0.9B
IN	18.7%	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B	$0.7B	$0.2B	$0.4B
IA	20.5%	$0.2B	$0.0B	$0.2B	$0.4B	$0.1B	$0.3B	$0.4B	$0.1B	$0.3B
KS	21.5%	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B	$0.4B	$0.1B	$0.2B
KY	19.1%	$0.2B	$0.0B	$0.2B	$0.2B	$0.0B	$0.2B	$0.3B	$0.1B	$0.2B
LA	23.5%	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
ME	28.2%	$0.1B	$0.1B	$0.1B	$0.1B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
MD	22.3%	$0.9B	$0.5B	$0.4B	$0.9B	$0.5B	$0.4B	$0.9B	$0.5B	$0.5B
MA	18.5%	$1.1B	$0.6B	$0.5B	$1.2B	$0.6B	$0.6B	$1.2B	$0.6B	$0.6B
MI	21.2%	$0.9B	$0.3B	$0.5B	$0.9B	$0.3B	$0.6B	$0.9B	$0.3B	$0.6B
MN	18.5%	$0.7B	$0.4B	$0.3B	$0.8B	$0.4B	$0.4B	$0.8B	$0.4B	$0.4B
MS	22.4%	$0.1B	$0.0B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
MO	19.4%	$0.3B	$0.0B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.4B
MT	36.8%	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
NE	22.6%	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B
NV	22.1%	$0.2B	$0.0B	$0.2B	$0.3B	$0.1B	$0.2B	$0.3B	$0.1B	$0.2B
NH	24.8%	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B	$0.2B	$0.1B	$0.1B
NJ	21.1%	$1.0B	$0.4B	$0.6B	$1.0B	$0.4B	$0.7B	$1.1B	$0.4B	$0.7B
NM	26.6%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.2B	$0.1B	$0.1B
NY	19.3%	$3.8B	$2.2B	$1.6B	$4.0B	$2.2B	$1.8B	$4.1B	$2.2B	$1.9B
NC	20.0%	$0.6B	$0.0B	$0.6B	$1.4B	$0.7B	$0.7B	$1.4B	$0.7B	$0.7B
ND	26.3%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B
OH	18.6%	$1.4B	$0.8B	$0.6B	$1.5B	$0.8B	$0.7B	$1.5B	$0.8B	$0.7B
OK	23.3%	$0.2B	$0.0B	$0.2B	$0.4B	$0.1B	$0.2B	$0.4B	$0.1B	$0.2B
OR	24.7%	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B	$0.5B	$0.2B	$0.3B
PA	19.4%	$1.6B	$0.9B	$0.7B	$1.7B	$0.9B	$0.8B	$1.7B	$0.9B	$0.8B

RI	24.9%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B
SC	20.9%	$0.2B	$0.0B	$0.2B	$0.4B	$0.1B	$0.3B	$0.4B	$0.1B	$0.3B
SD	27.3%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.2B	$0.1B	$0.1B
TN	19.0%	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B
TX	19.2%	$2.2B	$0.5B	$1.7B	$2.9B	$1.0B	$1.8B	$2.9B	$1.0B	$1.9B
UT	20.3%	$0.3B	$0.1B	$0.2B	$0.4B	$0.1B	$0.2B	$0.4B	$0.1B	$0.2B
VT	20.9%	$0.0B	$0.0B	$0.0B	$0.1B	$0.0B	$0.0B	$0.1B	$0.0B	$0.0B
VA	32.2%	$3.0B	$2.3B	$0.7B	$3.1B	$2.3B	$0.8B	$3.1B	$2.3B	$0.8B
WA	19.8%	$1.0B	$0.4B	$0.6B	$1.0B	$0.4B	$0.7B	$1.1B	$0.4B	$0.7B
WV	20.6%	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B	$0.1B	$0.0B	$0.1B
WI	21.5%	$0.6B	$0.2B	$0.3B	$0.6B	$0.2B	$0.4B	$0.6B	$0.2B	$0.4B
WY	19.9%	$0.1B	$0.0B	$0.0B	$0.1B	$0.0B	$0.0B	$0.1B	$0.0B	$0.0B
US	--	$43.3B	$23.3B	$20.1B	$47.5B	$25.4B	$22.1B	$49.5B	$26.4B	$23.1B

APPENDIX B: LIST OF PASSED STATE PRIVACY LAWS

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
AL	Alabama SB 318	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
AK	Alaska Stat. § 45.48.010 et seq.	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
AZ	Ariz. Rev. Stat. § 18-551 et seq	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
AZ	HB 2154	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
AR	Ark. Code §§ 4-110-101 et seq.	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
AR	Personal Information Protection Act	2019	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1
CA	S.B. 1386	2003	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	S.B 24	2012	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	SB 46	2014	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	AB 1710	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	AB 964, SB 570, SB 34	2016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	AB 1130	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CA	California Consumer Privacy Act	2018	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	0
CA	California Privacy Rights Act	2020	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
CO	HB 1119	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CO	HB 18-1128	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CO	SB 190	2021	0	1	1	1	0	1	1	1	0	1	1	1	1	1	0	0
CT	SB 650	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CT	HB 6001	2012	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CT	SB 949	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CT	SB 472	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CT	HB 5310	2021	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
CT	SB 1108 (Task force on consumer privacy)	2020	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DE	HB 116	2005	0	0		0	0	0	0	0	0	0	0	0	0	0	0	1
DE	HB 247	2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
DE	House Substitute 1 for HB 180	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
DE	Insurance Data Security Law HB 174	2019	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1
FL	SB 1524	2014	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
FL	SB 1526	2014	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
GA	SB 230	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
GA	SB 236	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
HI	SB 2290	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
HI	SB 2402	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
HI	HCR 225	2019	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ID	SB 1374	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ID	HB 556	2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IL	HB 1633	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IL	HB 3025	2012	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IL	HB 1260	2017	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IL	Biometric Information Protection Act	2008	0	0	0	1	0	0	1		1	0	1	0	0	1	1	0
IL	SB 1624	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IN	SB 503	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IN	HEA No. 1197	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IN	HEA No. 1121	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IN	HB 2189	2020	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
IA	2007 S.F. 2308	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IA	2014 S.F. 2259	2014	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IA	2018 S.F. 2177	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
KS	Kan. Stat. § 50-7a01 et seq. SB 196	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
KY	HB 232	2014	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
KY	HB 5	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
LA	SB 205	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
LA	SB 361	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LA	Insurance Data Security Law	2020	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
LA	HR 249	2019	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ME	LD 1671	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ME	HP 672	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ME	LD 696	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	HB 208	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	HB 974	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	SB 30	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	SB 693/HB 1154	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	Personal Information Protection Act	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MD	Labor and Employment - Use of Facial Recognition Services - Prohibition	2020	0	0	0	0	0	0	1	1	0	0	1	0	0	0	1	0
MA	HB 4144	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MA	H 4806	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MI	SB 309	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MI	SB 223	2011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MI	HB 6406	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MI	Insurance Data Security Law	2021	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MN	Minn. Stat. § 325E.61 and 325E.64 HB 2121	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MS	Miss. Code § 75-24-29 HB 582	2011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MO	Mo. Rev. Stat. § 407.1500 HB 62	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MT	HB 732	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
MT	HB 74	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NE	LB 876	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NE	LB 835	2016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
NV	SB 347	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NV	SB 186	2011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NV	AB 179	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NH	N.H. Rev. Stat. § 359-C:19 et seq. HB 1660	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NH	Insurance Data Security Law	2021	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NJ	A 4001	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NJ	SB 52	2019	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
NM	N.M. Stat. 57-12C-1 et seq. HB 15	2017	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NY	AB 4254	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NY	S 2605-D	2013	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
NY	Stop Hacks and Improve Electronic Data Security (SHIELD) Act	2019	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1
NC	SB 1017	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ND	SB 2251	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ND	HB 1435, SB 2214	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ND	HB 1485	2019	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OH	HB 104	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OH	Insurance Data Security Law	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OK	24 Okla. Stat. § 161 et seq., § 74-3113.1 HB 2245	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OR	SB 583	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OR	SB 574	2013	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OR	SB 601	2016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OR	SB 1551	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OR	SB 684	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
PA	73 Pa. Stat. § 2301 et seq. SB 712	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
RI	HB 6191	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
RI	SB 0134	2016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
SC	SB 453	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
SC	HB 3248	2013	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
SD	S.D. CODE 22-40-20 et seq. SB 62	2018	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TN	HB 2170	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TN	SB 2005	2016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TN	SB 547	2017	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	Acts 2007, 80th Leg., ch. 885, § 2.01. Amended by Acts 2009, 81st Leg., ch. 419, § 3.	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	Acts 2011, 82nd Leg., ch. 1126, § 14 (H.B. No. 300).	2012	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	SB 1610	2013	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	HB 4390	2020	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	HB 3529	2021	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
TX	HB 3746	2021	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
UT	SB 693/HB 1154	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
UT	SB 208	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
UT	SB 193	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VT	S 284, H 254	2012	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VT	H 513	2013	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VT	S 73	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VT	S 110	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VA	Va Code § 18.2-186.6	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VA	§ 32.1-127.1:05	2011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VA	HB 2113	2017	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
VA	HB 2396	2019	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

State	Statute	Year	Reg. 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VA	Consumer Data Protection Act	2021	0	1	1	1	0	1	1	1	0	1	1	1	1	1	1	0
WA	SB 6043	2005	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WA	HB 1149	2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WA	HB 1078	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WA	HB 1071	2020	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WV	W. VA. Code § 46A-2A-101 et seq. SB 340	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WI	Wis. Stat. § 134.98 SB 164	2006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WY	Wyo. Stat. § 40-12-501 et seq.	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
WY	SF No. 35, 36	2015	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Table Key

Reg. 1	Creates privacy review body	Reg. 9	Private right of action
Reg. 2	Right of access	Reg. 10	Opt-in requirement age
Reg. 3	Right of rectification	Reg. 11	Notice/transparency requirement
Reg. 4	Right of deletion	Reg. 12	Risk assessments
Reg. 5	Right of restriction	Reg. 13	Prohibition on discrimination
Reg. 6	Right of portability	Reg. 14	Purpose/processing limitation
Reg. 7	Right of opt-out	Reg. 15	Biometric data collection restriction
Reg. 8	Right against automated decision-making	Reg. 16	Data breach law
Reg.## = 0	Law does not include restriction	Reg.## = 1	Law includes restriction

Acknowledgments

This report was made possible in part through financial support from TechNet. ITIF maintains complete editorial independence for all of its work. All opinions, findings, and recommendations are those of ITIF and do not necessarily reflect the views of its supporters. Any errors and omissions are the authors' alone.

About the Author

Daniel Castro (@CastroTech) is vice president at ITIF and director of its Center for Data Innovation. He writes and speaks on a variety of issues related to information technology and Internet policy, including privacy, security, intellectual property, Internet governance, e-government, and accessibility for people with disabilities.

Luke Dascoli is an economic & technology policy research assistant at ITIF. He was previously a Research Assistant in the MDI Scholars Program at the McCourt School of Public Policy's Massive Data Institute. He holds a B.A. in Political Economy from Georgetown University.

Gillian Diebold (@g1lliandiebold) is a digital media specialist and policy analyst at ITIF's Center for Data Innovation. She holds a B.A. from the University of Pennsylvania, where she studied Communication and Political Science.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit itif.org.

ENDNOTES

1. Margaret Harding McGill, "Biden administration makes first move on data privacy," *Axios*, November 30, 2021, https://www.axios.com/biden-administration-data-privacy-commerce-department-65c99433-f7ac-49a8-88ce-b377e7e72382.html.
2. Müge Fazlioglu, "Privacy Bills in the 117th Congress," Privacy Tracker, August 24, 2021, https://iapp.org/news/a/privacy-bills-in-the-117th-congress/.
3. Information Transparency & Personal Data Control Act, H.R. 1816, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/house-bill/1816.
4. BROWSER Act of 2021, S.133, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/senate-bill/113/text.
5. BROWSER Act of 2021, H.R. 4659, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/house-bill/4659.
6. Data Care Act of 2021, S. 919, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/senate-bill/919.
7. Consumer Data Privacy and Security Act of 2021, S.1494, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1494/.
8. SAFE DATA Act, S.2499, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/senate-bill/2499.
9. "The Growth of State Privacy Legislation," IAPP, last modified November 2021, https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/.
10. Christopher Ward and Kelsey C. Boehm, "Developments in Biometric Information Privacy Laws," Foley & Lardner, LLP, accessed December 2021, https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws.
11. State of California Department of Justice, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa.
12. State of California Department of Justice, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20requires%20business%20privacy,the%20Right%20to%20Non%2DDiscrimination.
13. Virginia Consumer Data Protection Act, H.B. 2307, https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2307.
14. Virginia Consumer Data Protection Act, SB 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392.
15. Colorado Privacy Act, SB21-190, https://leg.colorado.gov/bills/sb21-190.
16. "US State Privacy Legislation Tracker," IAPP, last modified January 3, 2022, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.
17. "Colorado Privacy Act becomes law," The Privacy Advisor, July 8, 2021, https://iapp.org/news/a/colorado-privacy-act-becomes-law/.
18. Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (ITIF, August 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

19. Bureau of Economic Analysis, Regional Data (GDP and Personal Income; accessed November 2021), https://apps.bea.gov/itable/iTable.cfm?ReqID=70&step=1&acrdn=1; "Advertising spending in the United States from 2010 to 2019, by state," Statista, 2015, https://www.statista.com/statistics/652235/ad-spend-state-usa/.
20. Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018," September 2019, https://iapp.org/media/pdf/resource_center/standardized_regulatory_impact_assessment_CCPA.pdf.
21. 2018 SUSB Annual Data Tables by Establishment Industry (census.gov).
22. David Cloud, "On Life Support"; "Rethinking The Blues: How We Police in The U.S. And at What Cost," Justice Policy Institute, 2012, https://justicepolicy.org/wp-content/uploads/justicepolicy/documents/rethinkingtheblues_executive_summary.pdf.
23. "Data Protection Officer," European Data Protection Supervisor, n.d., https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en.
24. "How startups can ensure CCPA and GDPR compliance in 2021," *TechCrunch*, April 15, 2021, https://techcrunch.com/2021/04/15/how-startups-can-ensure-ccpa-and-gdpr-compliance-in-2021/.
25. "Processor," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 28, https://gdpr-info.eu/art-28- gdpr/.
26. Travis Good, "What is the Cost of a HIPAA Audit?" Datica, January 23, 2019, accessed July 23, 2019, https://datica.com/blog/what-is-the-cost-of-a-hipaa-audit/.
27. Alec Stapp, "Against Privacy Fundamentalism in the United States" (Niskanen Center, November 2018), accessed July 23, 2019, https://niskanencenter.org/blog/against-privacy-fundamentalism-in-the-united-states/.
28. "Privacy Law Prevents Illinoisans From Using Google App's Selfie Art Feature," Illinois Policy, January 23, 2018, https://www.illinoispolicy.org/privacy-law-prevents-illinoisans-from-using-google-apps-selfie-art-feature/.
29. Benjamin Mueller and Daniel Castro, "The Value of Personalized Advertising in Europe" (Center for Data Innovation, November 22, 2021), https://www2.datainnovation.org/2021-value-personalized-ads-europe.pdf.
30. "The BIPA Litigation Landscape and What Lies Ahead," Woodruff Sawyer, April 1, 2021, https://woodruffsawyer.com/cyber-liability/bipa-litigation-landscape/.
31. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), https://cdn.ca9.uscourts.gov/datastore/opinions/2019/08/08/18-15982.pdf.
32. "Judge approves $650 million settlement of Facebook privacy lawsuit linked to facial photo tagging," *Business Insider*, February 27, 2021, https://www.businessinsider.com/facebook-settlement-pay-650-million-privacy-lawsuit-biometrics-face-tagging-2021-2.
33. "Facebook privacy settlement approved: Nearly 1.6 million Illinois users will 'expeditiously' get at least $345," *Chicago Tribune*, February 26, 2021, https://www.chicagotribune.com/business/ct-biz-facebook-privacy-settlement-approval-20210227-okljqhsiargl7ijvzzfcotpyby-story.html.
34. "Nearly 22,000 Illinois Walmart workers could get share of $10 million privacy settlement," *Chicago Tribune*, January 19, 2021, https://www.chicagotribune.com/business/ct-biz-walmart-biometric-palm-scan-lawsuit-20210119-parcawurhzcshir2naurw5pccu-story.html.

35. "Illinois Supreme Court Finds Insurer Has Duty to Defend BIPA Suit," *Bloomberg Law*, June 18, 2021, https://news.bloomberglaw.com/privacy-and-data-security/illinois-supreme-court-finds-insurer-has-duty-to-defend-bipa-suit.

36. "Clearview AI Has Promised To Cancel All Relationships With Private Companies," *BuzzFeed News*, May 7, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

37. "CCPA Litigation Tracker, Updated as of December 2021," Perkin Coie, n.d., https://www.perkinscoie.com/en/ccpa-litigation-tracker.html (accessed January 10, 2022).

38. "2021 Year in Review: CCPA Litigation," *The National Law Review*, December 31, 2021, https://www.natlawreview.com/article/2021-year-review-ccpa-litigation.

39. Martina F. Ferracane and Erik van der Marel, "Do Data Policy Restrictions Inhibit Trade in Services?" (ECIPE), https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/; Martina F. Ferracane and Erik van der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" (ECIPE), https://ecipe.org/publications/do-data-policyrestrictions-impact-the-productivity-performance-of-firms-and-industries/; "The 2018 edition of the OECD PMR indicators and database: Methodological improvements and policy insights" (OECD, March 23, 2020), https://www.oecd-ilibrary.org/economics/the-2018-edition-of-the-oecd-pmr-indicators-and-database-methodological-improvements-and-policy-insights_2cfb622f-en; "Trade and cross-border data flows" (OECD, December 21, 2018), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En.

40. Ibid.