Subcommittee on Innovation, Data, & Commerce
Hearing entitled "Addressing America's Data Privacy Shortfalls: How A National Standard Fills Gaps To Protect Americans' Personal Information"
[April 27, 2023]

Documents for the record

At the conclusion of the meeting, the chair asked and was given unanimous consent to include the following documents into the record:

1. A Washington Post article entitled, "Remote learning apps shared children's data at a 'dizzying scale,'" May 24, 2022, submitted by Representative Walberg.
2. A letter from the National Association of Federally-Insured Credit Unions, April 26, 2023, submitted by the Majority.
3. A letter from the California Privacy Protection Agency, April 26, 2023, submitted by the Minority.
4. A letter from Privacy for America, April 27, 2023, submitted by the Minority.
5. A letter from leading members of the U.S. startup ecosystem, April 27, 2023, submitted by the Minority.
6. A report from the Information Technology and Innovation Foundation entitled, "The Looming Cost of State Privacy Laws," January 2022, submitted by the Majority.
7. A letter from the Credit Union National Association, April 27, 2023, submitted by the Majority.
8. A statement for the record from U.S. PIRG, April 27, 2023, submitted by the Minority.
9. Written testimony from Mr. Edmund Mierzwinski to the Committee on Financial Services, February 26, 2019, submitted by the Minority.

The Washington Post
Democracy Dies in Darkness

TECHNOLOGY

Remote learning apps shared children's data at a 'dizzying scale'

The educational tools used by students during the pandemic shared their information with advertisers and data brokers that could track them around the Web, an international investigation found

By Drew Harwell

May 24, 2022 at 9:00 p.m. EDT

Millions of children had their online behaviors and personal information tracked by the apps and websites they used for school during the pandemic, according to an international investigation that raises concerns about the impact remote learning had on children's privacy online.

The educational tools were recommended by school districts and offered interactive math and reading lessons to children as young as prekindergarten. But many of them also collected students' information and shared it with marketers and data brokers, who could then build data profiles used to target the children with ads that follow them around the Web.

Those findings come from the most comprehensive study to date on the technology that children and parents relied on for nearly two years as basic education shifted from schools to homes.

Researchers with the advocacy group Human Rights Watch analyzed 164 educational apps and websites used in 49 countries, and they shared their findings with The Washington Post and 12 other news organizations around the world. The consortium, EdTech Exposed, was coordinated by the investigative nonprofit the Signals Network and conducted further reporting and technical review.

What the researchers found was alarming: nearly 90 percent of the educational tools were designed to send the information they collected to ad-technology companies, which could use it to estimate students' interests and predict what they might want to buy.

Researchers found that the tools sent information to nearly 200 ad-tech companies, but that few of the programs disclosed to parents how the companies would use it. Some apps hinted at the monitoring in technical terms in their privacy policies, the researchers said, while many others made no mention at all.

The websites, the researchers said, shared users' data with online ad giants including Facebook and Google. They also requested access to students' cameras, contacts or locations, even when it seemed unnecessary to their schoolwork. Some recorded students' keystrokes, even before they hit "submit."

The "dizzying scale" of the tracking, the researchers said, showed how the financial incentives of the data economy had exposed even the youngest Internet users to "inescapable" privacy risks — even as the companies benefited from a major revenue stream.

"Children," lead researcher Hye Jung Han wrote, were "just as likely to be surveilled in their virtual classrooms as adults shopping in the world's largest virtual malls."

School districts and the sites' creators defended their use, with some companies saying researchers had erred by including in their study homepages for the programs, which included tracking codes, instead of limiting their analysis to the internal student pages, which they said contained fewer or no trackers. The researchers defended the work by noting that students often had to sign in on the homepages before their lessons could begin.

The coronavirus pandemic abruptly upended the lives of children around the world, shuttering schools for more than 1.5 billion students within the span of just a few weeks. Though some classrooms have reopened, tens of millions of students remain remote, and many now depend on education apps for the bulk of their school days.

Yet there has been little public discussion of how the companies that provided the programs remote schooling depends on may have profited from the pandemic windfall of student data.

The learning app Schoology, for example, says it has more than 20 million users and is used by 60,000 schools across some of the United States' largest school districts. The study identified code in the app that would have allowed it to extract a unique identifier from the student's phone, known as an advertising ID, that marketers often use to track people across different apps and devices and to build a profile on what products they might want to buy.

A representative for PowerSchool, which developed the app, referred all questions to the company's privacy policy, which said it does not collect advertising IDs or provide student data to companies for marketing purposes. But the policy also says the company's website uses third-party tools to show targeted ads to users based on their "browsing history on other websites or on other devices." The policy did not say which third-party companies had received users' data.

The policy also said that it "does not knowingly collect any information from children under the age of 13," in keeping with the Children's Online Privacy Protection Act, or COPPA, the U.S. law that requires special restrictions on data collected from young children. The company's software, however, is marketed for classrooms as early as kindergarten, which for many children starts around age 4.

The investigation acknowledged that it could not determine exactly what student data would have been collected during real-world use. But the study did reveal how the software was designed to work, what data it had been programmed to seek access to, and where that data would have been sent.

School districts and public authorities that had recommended the tools, Han wrote, had "offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their fundamental rights to privacy."

The researchers said they found a number of trackers on websites common among U.S. schools. The website of ST Math, a "visual instructional program" for prekindergarten, elementary and middle school students, was shown to have shared user data with 19 third-party trackers, including Facebook, Google, Twitter and the e-commerce site Shopify.

Kelsey Skaggs, a spokeswoman for the California-based MIND Research Institute, which runs ST Math, said in a statement that the company does not "share any personally identifiable information in student records for the purposes of targeted advertising or other commercial purposes" and does not use the same trackers on its student platform as it does on its homepage.

But the researchers said they found trackers not just on ST Math's main site but on pages offering math games for prekindergarten and the first grade.

Google spokesperson Christa Muldoon said the company is investigating the researchers' claims and will take action if they find any violations of their data privacy rules, which include bans on personalized ads aimed at minors' accounts. A spokesperson for Facebook's parent company, Meta, said it restricts how businesses share children's data and how advertisers can target children and teens.

The study comes as concern grows over the privacy risks of the educational-technology industry. The Federal Trade Commission voted last week on a policy statement urging stronger enforcement of COPPA, with Chair Lina Khan arguing that the law should help "ensure that children can do their schoolwork without having to surrender to commercial surveillance practices."

COPPA requires apps and websites to get parents' consent before collecting children's data, but schools can consent on their behalf if the information is designated for educational use.

In an announcement, the FTC said it would work to "vigilantly enforce" provisions of the law, including bans against requiring children to provide more information than is needed and restrictions against using personal data for marketing purposes. Companies that break the law, it said, could face fines and civil penalties.

Clearly, the tools have wide impact. In Los Angeles, for example, more than 447,000 students are using Schoology and 79,000 are using ST Math. Roughly 70,000 students in Miami-Dade County Public Schools use Schoology.

Both districts said they've taken steps to limit privacy risks, with Los Angeles requiring software companies to submit a plan showing how student information will be protected while Miami-Dade said it had conducted a "thorough and extensive" evaluation process before bringing on Schoology last year.

The researchers said most school districts they examined had conducted no technical privacy evaluations before endorsing the educational tools. Because the companies' privacy policies often obscured the extent of their monitoring, the researchers said, district officials and parents often were left in the dark on how students' data would be collected or used.

Some popular apps reviewed by the researchers didn't track children at all, showing that it is possible to build an educational tool without sacrificing privacy. Apps such as Math Kids and African Storybook didn't serve ads to children, collect their identifying details, access their cameras, request more software permissions than necessary or send their data to ad-tech companies, the analysis found. They just offered simple learning lessons, the kind that students have relied on for decades.

Vivek Dave, a father of three in Texas whose company RV AppStudios makes Math Kids, said the company charges for in-app purchases on some word-search and puzzle games designed for adults and then uses that money to help build ad-free educational apps. Since launching an alphabet game seven years ago, the company has built 14 educational apps that have been installed 150 million times this year and are now available in more than 35 languages.

"If you have the passion and just try to understand them, you don't need to do all this level of tracking to be able to connect with kids," he said. "My first beta testers were my kids. And I didn't want that for my kids, period."

The researchers argued that governments should conduct data-privacy audits of children's apps, remove the most invasive, and help guide teachers, parents and children on how best to prevent data over-collection or misuse.

Companies, they said, should work to ensure that children's information is treated differently from everyone else's, including by being siloed away from ads and trackers. And lawmakers should encode these kinds of protections into regulation, so the companies aren't allowed to police themselves.

Bill Fitzgerald, a privacy researcher and former high school teacher who was not involved in the study, sees apps' tracking of students not only as a loss of privacy but as a lost opportunity to use the best of technology for their benefit. Instead of rehashing old ways to vacuum up user data, schools and software developers could have been pursuing fresher, more creative ideas to get children excited to learn.

"We have outsourced our collective imagination and our vision as to what innovation with technology could be to third-party product offerings that aren't remotely close to the classroom and don't have our best interests at heart," Fitzgerald said.

“The conversation the industry wants us to have is: What’s the harm?” he added. “The right conversation, the ethical conversation is: What’s the need? Why does a fourth-grader need to be tracked by a third-party vendor to learn math?”

Abby Rufer, a high school algebra teacher in Dallas, said she’s worked with a few of the tested apps and many others during a frustratingly complicated two years of remote education.

School districts felt pressured during the pandemic to quickly replace the classroom with online alternatives, she said, but most teachers didn’t have the time or technical ability to uncover how much data they gobbled up.

“If the school is telling you to use this app and you don’t have the knowledge that it might be recording your students’ information, that to me is a huge concern,” Rufer said.

Many of her students are immigrants from Latin America or refugees from Afghanistan, she said, and some are already fearful of how information on their locations and families could be used against them.

“They’re being expected to jump into a world that is all technological,” she said, “and for many of them it’s just another obstacle they’re expected to overcome.”

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

April 26, 2023

The Honorable Gus M. Bilirakis
Chairman
Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Janice D. Schakowsky
Ranking Member
Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"

Dear Chairman Bilirakis and Ranking Member Schakowsky:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) ahead of tomorrow's hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 135 million consumers with personal and small business financial service products. NAFCU and our members welcome the Subcommittee's review of this important issue.

As NAFCU has previously communicated to Congress, we believe there is an urgent need for comprehensive federal data privacy legislation that protects consumer data, establishes data safeguards, and recognizes the standards that have been in place for over two decades with the Gramm-Leach-Bliley Act (GLBA). In 2019, recognizing the importance of data privacy and the ongoing privacy debate, NAFCU issued a series of data privacy principles that calls for a comprehensive federal cybersecurity standard, the harmonization of existing federal data privacy laws, and the preemption of state privacy laws. As the Subcommittee works to develop much-needed comprehensive federal data privacy legislation, NAFCU recommends you include the following elements as key aspects in any such proposal:

- **A comprehensive federal cybersecurity standard covering all entities that collect and store consumer information.** Uniformly strong cybersecurity is necessary to ensure Americans' data is adequately protected across the economy. Existing strong federal cybersecurity standards, like that contained in the GLBA, should be extended to the activities of all data collectors and processors exceeding certain reasonable thresholds.

- **Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** The current patchwork of federal and state data privacy laws generates incredible consumer

confusion and significant compliance burdens while failing to address the most significant data privacy risks to Americans—those risks posed by unregulated or inconsistently regulated entities that collect, control, and process vast amounts of our data. Comprehensive federal data privacy legislation should responsibly build on the successes of robust, time-tested federal laws by extending the same robust data privacy standards across the economy and ensuring that already well-regulated entities, like credit unions, may confidently operate within their existing federal frameworks without fear of being subject to more than 50 different data privacy and security standards.

- **Delegation of enforcement authority to the appropriate sectoral regulator.** The National Credit Union Administration (NCUA) should be federal credit unions' sole data privacy and cybersecurity regulator. Allowing the NCUA, which is well-versed in the unique nature of federal credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers. Exposing credit unions and other already well-regulated entities to suits by states' attorneys general and private rights of action will dramatically increase compliance costs without providing a corresponding increase in consumer protection.

- **A safe harbor for businesses that take reasonable measures to comply with the privacy standards.** Comprehensive federal data privacy legislation should adopt principles-based requirements based on an organization's specific operations and risk profile and include a safe harbor for organizations that design and implement appropriate measures.

- **Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** Providing multiple data privacy disclosures and opt-out mechanisms across multiple channels creates consumer confusion and unreasonable burdens for subject entities. A new privacy law should avoid conflicting or duplicative disclosure requirements by incorporating easy to understand language, like that consistent with the GLBA's disclosure requirements.

- **Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** Actual damages to consumers are too difficult to establish by evidence, and statutory damages for violations are incredibly ripe for frivolous lawsuits. Sectoral regulators alone should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.

While NAFCU supports a national data security and privacy standard, we had some concerns about the American Data Protection and Privacy Act (ADPPA) that the Energy and Commerce Committee considered in the last Congress, including:

- *GLBA Exemption.* Through the GLBA, Congress defined robust federal data privacy and information security standards for the financial services industry and provided the NCUA and other federal financial regulators the means to create and maintain strong privacy and data safeguards. The ADPPA did not recognize these long-standing requirements by providing a GLBA exemption. Congress should recognize the strength and successes of the GLBA and other time-tested federal sectoral data privacy regulation, and the value of regulator-led regulation, by wholly exempting credit unions and other already closely-regulated entities.

- *Private Right of Action.* This legislation provided a private right of action which would allow individuals or states' attorneys generals to sue covered entities over potential violations allowing courts to determine the law. This means that different judicial interpretations will allow a consumer in California to have different privacy protections than a consumer in South Carolina, and credit unions will find themselves immediately and unnecessarily exposed to new and substantial compliance and legal risks.

- *Preemption of State Laws.* The ADDPA would preempt many state laws but then subsequently provided exceptions that undermine the preemption. This would perpetuate a patchwork of state and federal data privacy legislation and regulation. We believe Congress must leverage comprehensive federal data privacy legislation to expressly preempt all state data privacy legislation and regulation.

As your colleagues on the House Financial Services Committee tackle the Data Privacy Act, H.R. 1165, within its jurisdiction to improve the GLBA for financial services entities, we urge the Subcommittee to craft a workable GLBA expansion to those outside of financial services that may be handling consumer financial data. The GLBA has successfully served consumers, credit unions, and other covered financial institutions for nearly a quarter-century. Changes to the GLBA for those already covered by it must be viewed with a cautionary eye. While some modernization of the GLBA for financial institutions may be in store, the system has generally been a success and should be a model for other areas. Making the system work best means expanding financial data protection requirements outside of just financial services. Retailers, merchants, and others that handle financial data should be subject to new requirements similar to those standards adopted for financial institutions. We urge the Subcommittee to work with your counterparts on the House Financial Services Committee to ensure a balance that recognizes existing law and the concerns of credit unions as Congress tackles the important issue of privacy reform.

NAFCU looks forward to continuing to work with you to address these concerns with consumer privacy. On behalf of our nation's credit unions and their more than 135 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Lewis Plush NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2836 or lplush@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Innovation, Data, and Commerce

CALIFORNIA PRIVACY PROTECTION AGENCY
2101 Arena Blvd
Sacramento, CA 95834
www.cppa.ca.gov

April 26, 2023

The Honorable Gus Bilirakis, Chair
The Honorable Jan Schakowsky, Ranking Member
Innovation, Data, and Commerce Subcommittee
House Energy & Commerce Committee
United States House of Representatives
Washington, DC 20515

Re: Innovation, Data, and Commerce Subcommittee Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"

Dear Chair Bilirakis and Ranking Member Schakowsky:

The California Privacy Protection Agency (Agency)[1] writes to thank the Innovation, Data, and Commerce Subcommittee for highlighting the importance of protecting the privacy and security of personal information not currently covered by privacy laws in its hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."[2] But such protections should not come at the expense of existing rights. H.R. 8152, the American Data Privacy and Protection Act (ADPPA),[3] which the Agency opposes in its current form, seeks to significantly weaken the protections currently in place in the states, including safeguards Californians currently enjoy under the California Consumer Privacy Act, as amended (CCPA).[4] Instead, lawmakers should support legislation that sets a federal floor and encourages states to continue to take the lead to advance protections.

Supporting states' efforts to adopt legislation to address their own residents' needs is consistent with interoperability. For example, the CCPA directs the Agency to work with policymakers in other jurisdictions to ensure consistency in privacy protections.[5] And the Agency's CCPA regulations were carefully crafted to not contravene a business's compliance with other privacy laws, such as Europe's General Data Protection Regulation (GDPR) and consumer privacy laws recently passed in Colorado,

[1] Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians' consumer privacy. The Agency implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

[2] United States House of Representatives, Innovation, Data, and Commerce Subcommittee Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information" (April 27, 2023), https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information.

[3] H.R. 8152 (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[4] Cal. Civ. Code § 1798.100 et seq.

[5] *Id.* § 1798.199.40(i).

Virginia, Connecticut, and Utah.[6] In addition to working with other jurisdictions to ensure consistent protections, the Agency is also in regular contact with state, federal, and international regulators to help ensure consistent enforcement of the law.

Nearly all federal privacy laws already allow states to adopt stronger protections, which California has done. Such additional protections have not prevented California from becoming one of the world's leading economies.[7] For example, The Health Information Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA) all contain language that allow the states to adopt stronger protections.[8] The Telephone Consumer Protection Act (TCPA) and the Video Privacy Protection Act (VPPA) also allow for stronger state laws.[9] California has already adopted stronger protections in many of these areas, from the Confidentiality of Medical Information Act (CMIA), which is similar to, but broader than, HIPAA, and the California Financial Information Privacy Act (CFIPA), which was explicitly adopted to provide a higher standard of protections than GLBA.[10]

Furthermore, it's not clear that the ADPPA will create a single national standard, a purported justification for the bill's preemption language.[11] ADPPA seeks to preempt swaths of existing state privacy laws but allows covered businesses to develop their own compliance plans, to be submitted to the FTC for approval.[12] This safe harbor could lead to hundreds if not thousands of different compliance standards, causing confusion among consumers seeking to exercise their rights. This could be particularly harmful to members of underserved communities that do not have the resources to navigate these varying procedures.

The ADPPA could certainly weaken existing protections. For example, the CCPA gives Californians significant protections with respect to automated decision-making (ADM), including the right to access meaningful information about the logic involved in automated decisions and the right to opt out of automated decision-making.[13] This would enable California to help rein in algorithms, such as those used by social media apps popular with young adults and children that play a role in targeting harmful

[6] California Privacy Protection Agency, California Consumer Privacy Act Regulations, Notice of Proposed Rulemaking (July 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf.

[7] Office of Governor Gavin Newsom, *ICYMI: California Poised to Become World's 4th Biggest* Economy (Oct. 24, 2022), https://www.gov.ca.gov/2022/10/24/icymi-california-poised-to-become-worlds-4th-biggest-economy/.

[8] *See* 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807; 15 U.S.C. § 1681t.

[9] 47 U.S.C. § 227(f); 18 U.S.C. § 2710(f).

[10] Cal. Civ. Code § 56.10 et seq.; Cal. Fin. Code § 4051(b).

[11] Memo, from Committee Majority Staff, to Members, Subcommittee on Innovation, Data, and Commerce, re: Hearing Entitled "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information" (Apr. 25, 2023), https://d1dth6e84htgma.cloudfront.net/IDC_Memo_American_Data_Privacy_Hearing_2023_04_27_1_bda35f1b5d.pdf?updated_at=2023-04-25T21:40:51.125Z.

[12] *See* Sec. 303-4.

[13] Cal. Civ. Code § 1798.185(a)(16).

content,[14] or generative AI and Large Language Models that are growing in popularity at an astronomical rate, which ADPPA does not address.

The ADPPA also seeks to prevent the states from strengthening privacy protections in the future. ADPPA was introduced before the Dobbs decision created new urgency for meaningful privacy protections.[15] Since ADPPA was introduced, California has already adopted new laws to protect reproductive privacy, including a bill that, among other provisions, prevents out-of-state law enforcement entities from obtaining information from California businesses about an abortion that would be legal in California.[16] This year, the California legislature is also considering a bill to protect data collected by certain reproductive health apps by the CMIA[17] and a bill that would restrict the tracking of consumers near family planning centers, among others.[18] Washington State appears poised to advance HB 1155, a reproductive privacy law with sweeping protections over this sensitive data. In contrast, ADPPA has not been meaningfully amended to address new concerns with respect to reproductive privacy.

Ten state attorneys general, including those in Illinois and New Jersey, criticized ADPPA's preemption language, and "encourage[d] Congress to adopt legislation that sets a federal floor, not a ceiling, for critical privacy rights and respects the important work already undertaken by states to provide strong privacy protections for our residents."[19] California Governor Newsom, Attorney General Bonta, Assembly Speaker Anthony Rendon, and members of the California Senate have also raised concerns about preemption language in the ADPPA.[20]

ADPPA represents a false choice: that strong federal protections must come at the expense of the states. Americans deserve both, a federal floor that allows states to adopt stronger protections. We look forward to working with you to promote and safeguard these protections.

---

[14] Ben Smith, *How Tik Tok Reads Your Mind*, N.Y. Times (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html.

[15] *See, e.g.*, Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info in Pregnant People,* Politico (Aug. 1, 2022), https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988.

[16] 2022 Cal. Stat. 89 (AB 1242).

[17] AB 254 (2023).

[18] SB 345 (2023).

[19] Letter from Ten Attorneys General to Congressional Leaders (July 19, 2022), https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf.

[20] Letter from Governor Newsom, Attorney General Bonta, and the California Privacy Protection Agency to Congressional Leaders (Feb. 28, 2023), https://cppa.ca.gov/pdf/adppa_letter.pdf; Letter from California Assembly Speaker Rendon to U.S. House Speaker Nancy Pelosi (July 19, 2022), https://cppa.ca.gov/meetings/materials/20220728_item2_letter_assembly_speaker.pdf; Letter from Senator Tom Umberg et al. to U.S. House Speaker Nancy Pelosi (Aug. 9, 2022).

Sincerely,

Ashkan Soltani
Executive Director

Cc: The Honorable Cathy McMorris Rodgers, Chair
The Honorable Frank Pallone, Jr., Ranking Member
Members, House Energy & Commerce Committee

April 27, 2023

The Hon. Cathy McMorris Rodgers
Chair
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Frank Pallone
Ranking Member
House Energy & Commerce Committee
2322 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Gus Bilirakis
Chairman
House Energy & Commerce
Subcommittee on Innovation, Data, and Commerce
2306 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Jan Schakowsky
Ranking Member
House Energy & Commerce
Subcommittee on Innovation, Data, and Commerce
2408 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Rodgers, Chairman Bilirakis, Ranking Member Pallone, and Ranking Member Schakowsky:

Privacy for America is a coalition of trade organizations and companies representing a broad cross-section of the American economy. Our membership includes companies and trade associations in the advertising, travel, hospitality, media, financial services, data services, market research, and many other industries. We have long urged the creation of a single comprehensive, preemptive national standard for consumer privacy that supplements the existing set of sectoral and anti-discrimination laws already in effect in the United States.

As the House Energy and Commerce Committee Innovation, Data, and Commerce Subcommittee's ("Subcommittee") considers an approach to this type of comprehensive, preemptive law in its hearing on "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information," the Subcommittee should take a risk-based approach to such a law and balance consumer protection with the responsible use of data. This balance was absent from the American Data Privacy Protection Act ("ADPPA") as it stood at the end of the last Congress. We write to highlight several facts that we urge the Subcommittee to seriously consider during this hearing and its work going forward in an effort to appropriately calibrate a preemptive, comprehensive national privacy law for business and consumers across the United States.

- **Sectoral and anti-discrimination laws work to address data practices within their purview.** For decades the United States has maintained robust protections for data industries including health care, financial services, telecommunications, and education. It has also built up strong defenses against the misuse of data related to certain protected classes, including protections for children's data and protections against the use of data to discriminate against individuals in housing, credit, and employment based on characteristics

like race and gender. These long-standing laws, with long histories of enforcement and complex compliance programs within responsible companies, should not be left by the wayside as Congress assesses how to address the modern data-driven economy.

- **The Privacy for America Framework provides the model approach for privacy legislation.** The Subcommittee can look to the Privacy for America *Principles of Privacy Legislation* ("Framework") as an example of how to strike an appropriate balance for national data standards.[1] The Framework defines certain uses of personal information as reasonable and others as per se unreasonable and thus prohibited.[2] The Framework prioritizes consumer protection while also allowing consumers and businesses alike to derive immense value from reasonable uses of data and access to a vibrant online ecosystem.

- **Congress should set a national standard when addressing potential gaps in privacy protections and not abdicate that power to the Federal Trade Commission.** When the Subcommittee considers approaches to a comprehensive privacy law to supplement the sectoral laws, a bedrock principle of that work must be to set a true, preemptive national standard. The regulation of the modern data-driven economy is best left to the democratically accountable legislative branch, not individual states or executive branch agencies. Personal data is collected and processed almost exclusively in interstate commerce and, accordingly, should be subject to a single national standard, not a patchwork of differing state statutes. Data collection and processing, therefore, should be established once through the clear authority granted to Congress by the American people and the Constitution.

- **Private companies should follow the law, not create their own.** When Congress creates a true national framework for data practices, no company should be allowed to interfere in the legitimate, responsible, data practices Congress has authorized. Just because one entity maintains a market position as an intermediary between consumers and publishers does not give it the right to prevent otherwise legally permissible and responsible data processing. This concern is especially true when those private actors choose to obstruct reasonable data flows in order to further their own financial goals to the inevitable detriment of their competitors. A federal law should ban such meddling.

- **Responsible data-driven practices deliver over $30,000 in value to each consumer per year.** Any comprehensive national privacy law needs to balance the costs to consumers and businesses against the increased consumer protections such a law may offer. And the costs of overzealous regulation could be immense, as studies have found that companies' data-driven practices keep $30,000 per year in the pockets of each consumer in the United States thanks to free and discounted entertainment, information, and other services.[3] Congress

[1] Privacy for America, *Principles for Privacy Legislation* (2019) https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/.
[2] Framework at Part 1, Sec. 1(Y); Sec. 3: Sec 6(G)(c).
[3] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.

should not reach into consumer's bank accounts by imposing unreasonable restrictions on the data services companies that provide the backbone of many of these free and low-cost services that consumers desire. Consumers do not deserve a new $30,000 tax.

* * *

Thank you for your consideration of this letter on this important topic. We look forward to working with you as you continue to evaluate and develop approaches to preemptive, comprehensive, national privacy legislation that will properly balance consumer protection and the vital, efficient, and effective data-driven practices required for a growing and dynamic Unites States economy.

Sincerely,
Privacy for America

April 27, 2023

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Chair
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science,
and Transportation
254 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science,
and Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chair Rodgers, Ranking Member Pallone, Chair Cantwell and Ranking Member Cruz:

As leading members of the U.S. startup ecosystem—entrepreneurs, startup founders, incubators, investors, accelerators, and support organizations—located in 26 states that serve individuals, businesses, schools, and governments in every state across the country and throughout the world, we write to urge you to pass a uniform, consistently-enforced, comprehensive data privacy law to create certainty for us and provide baseline protections for our customers.

We are creating new ways for individuals to learn critical skills, helping people to advance in their careers, assisting businesses in reducing emissions, improving health outcomes for at-risk populations, among so many other innovative contributions to advance society. We care deeply about our users, customers, and clients, respect their privacy, and invest heavily in keeping their data safe.

Unfortunately, the rapidly shifting landscape of state privacy laws makes it difficult for us to be confident that we are compliant with the letter of each law and leads us to spend considerable time and resources navigating these disparate, complex frameworks. In fact, new research shows that we each spend hundreds of thousands and forgo up to 20% of revenue on often duplicative compliance activities.[1] A uniform federal privacy framework would create clarity for us, streamline these costs, allow us to better serve our customers, and improve our competitiveness all while ensuring that our customers in each state have the same privacy protections. The resources we save could be put toward hiring more workers to grow our businesses, investing in R&D to improve our products, and supporting our communities.

[1] *Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups,* Engine (Mar. 24, 2023), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf.

Last Congress you came closer than ever to passing a federal privacy law. We encourage you to build on that momentum this Congress while keeping in mind the needs of startups. We need federal privacy law that:

> **Creates uniformity**. Startups need a federal privacy law to preempt individual state privacy laws. Without preemption, a federal privacy law would merely be another law added to the patchwork and would not create certainty or ease compliance for us.
>
> **Limits bad faith litigation**. A federal privacy law should be consistently enforced by expert agencies and limit opportunities for bad actors to exploit the high cost of privacy litigation to extract settlements from startups by bringing lawsuits even when startups have not violated the law.
>
> **Respects the resources of startups**. Many of us have not yet raised formal funding rounds and instead rely on our personal savings or the revenue we generate. Even those of us that have raised outside capital have significantly fewer resources than our larger competitors. A federal privacy law must account for our resources and ability to comply.
>
> **Accounts for the tools startups use**. We use multiple tools and services to build our companies. As you formulate a federal privacy law, you should keep in mind the interconnectedness of the startup ecosystem.

The startup community supports your efforts to create a uniform, consistently-enforced federal privacy framework to create clarity and establish protections for all Americans. We thank you for considering our views.

Sincerely,

1Huddle
6AM City, Inc.
Abstract
Airpals Technologies Inc.
Ardian Group, Inc.
Availyst
Bims Laboratories, Inc.
Black & Brown Founders
Boolean Girl
Broadside Digital
Bryght Labs
Carefully
Center for American Entrepreneurship
CitiQuants Corp.
Connector Labs
Courtam, Inc. dba People Clerk
Cover
Cranberry Queues Corp.
DAF.Financial, Inc.
Denver Angels

Ecobot
Educreations
Engine
Eskuad
Event Vesta, Inc
Free From Market
FundBlackFounders
Gaussian Holdings
Global Response Systems
Globalfy, LLC
Green Tech Coast
Gust
Hacom
hobbyDB
Hush
Infiltron Software Suite
Innovare
Institute for Energy and Sustainability, Inc.
IronCore Labs, Inc.
Libib
Linktree
ListedB
LiteraSeed, Inc.
Lumo
M1PR, Inc.
Max Borges Agency
Maxwell
Onfleet, Inc.
PILOT Inc.
PIE
Polyhedra
Productions.com
RAVN
Raydiant Oximetry, Inc.
Red Cap Ventures
Refraction, Inc.
Renee
Right to Start
Signals
STY Holdings
TaxCredit.ai
TheraTec, Inc.
Tostie Productions, LLC
Venntive LLC
Voatz, Inc.
WePower Technologies LLC

cc: Honorable Members of the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation

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.

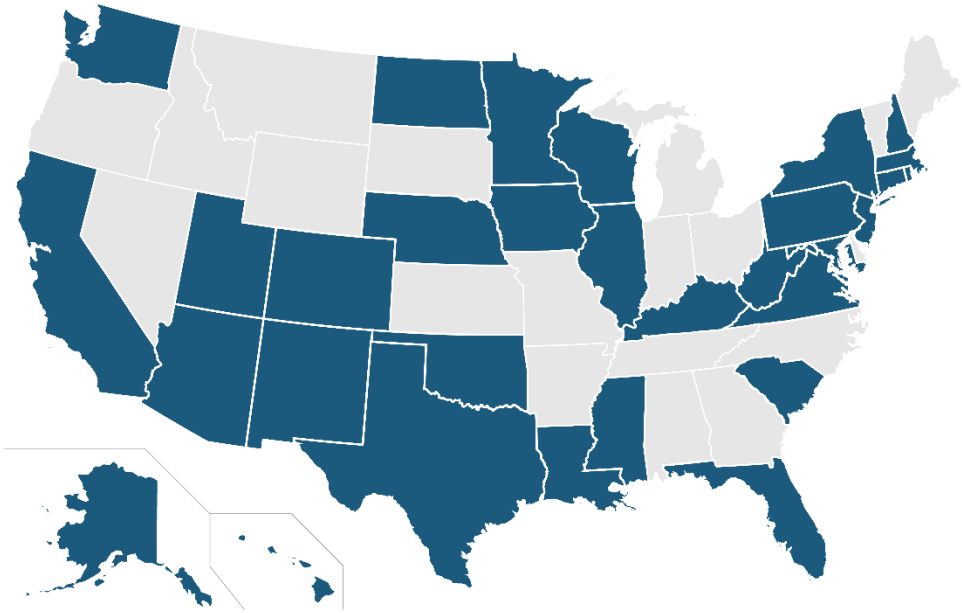
- **S. 2134, Data Protection Act of 2021:** Introduced by Sen. Kirsten Gillibrand (D-NY), this legislation would establish a new Data Protection Agency tasked with enforcing the nation's laws around the processing and use of personal data and preventing and remediating privacy harms. The bill would not 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.

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

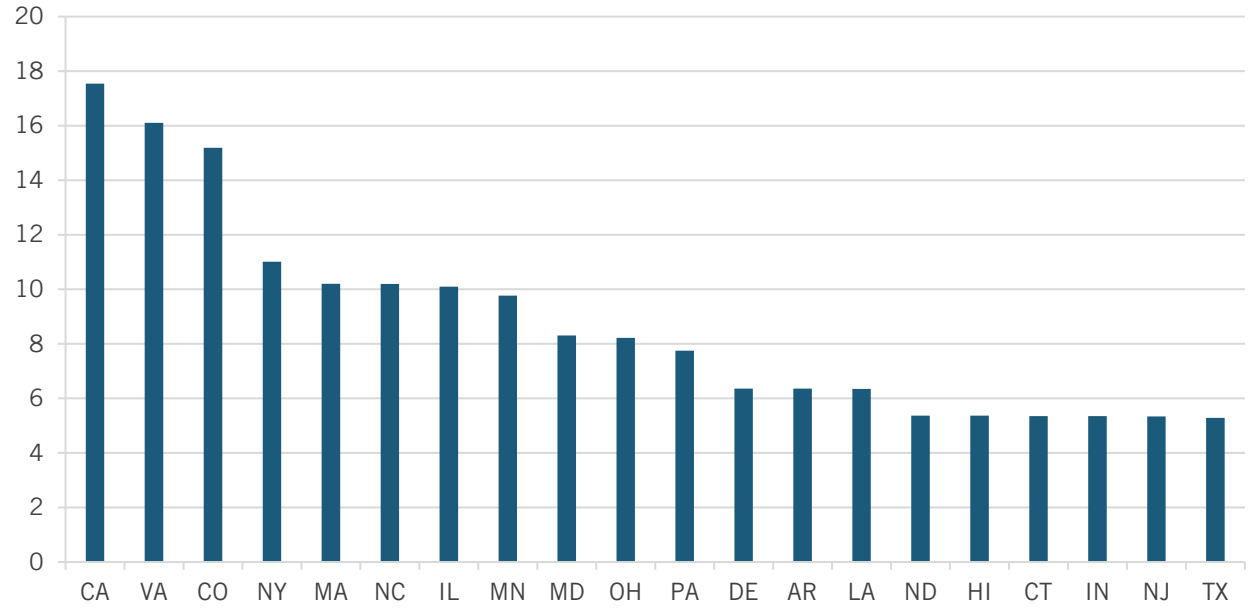
A state's deflator is the unweighted average of its share of U.S. GDP in the consumer products, consumer finance, and advertising industries. *d* is calculated using only 2019 data for all states and is applied to all years' calculations of SRS to control for issues of endogeneity. Data on a state's 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

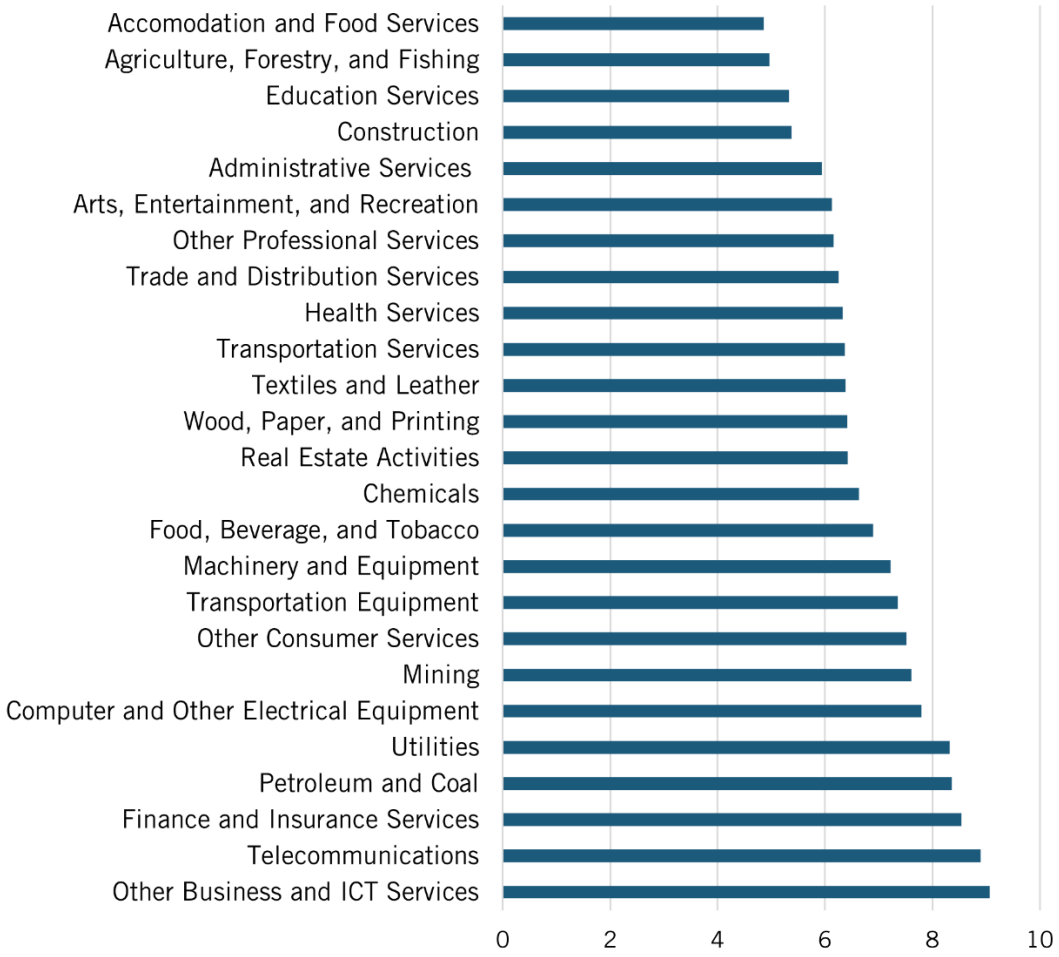


Data-Intensity Modifiers

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)



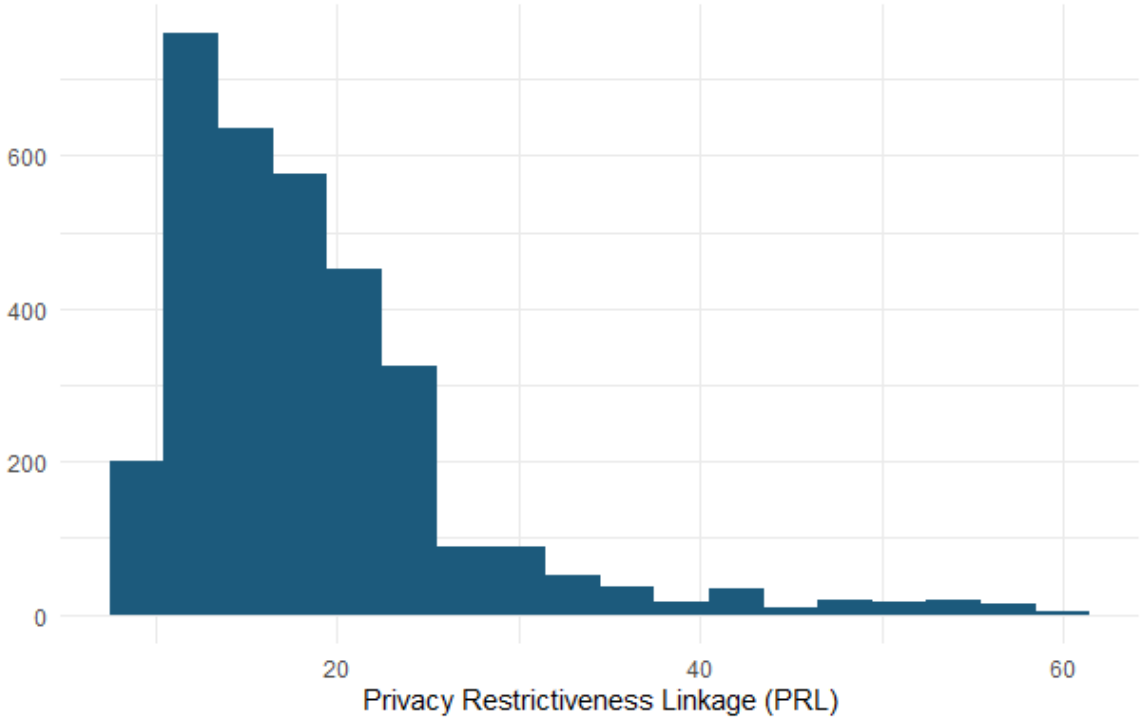
The proxies SRS by state and DIM by industry function as components of a composite index at the state-industry level. This composite index links the level of privacy restrictiveness within a state to the level of data reliance faced by an industry in order to provide measurement on the level of effective 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.

Credit Union National Association
CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

April 27, 2023

The Honorable Gus Bilirakis
Chairman
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of America's credit unions, I am writing about your hearing "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans Personal Information". CUNA represents America's credit unions and their more than 135 million members.

Credit unions strongly support the enactment of a national data security and data privacy law that includes robust security standards that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security. Securing and protecting consumer data is important not only for their individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches, exposing nearly 12 billion consumer records. These breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Stringent information security and privacy practices have long been part of the financial services industries' business practices and are necessary as financial institutions are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the Gramm Leach Bliley Act ("GLBA"). GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with the GLBA's requirements and robust enforcement for violations. Several of these significant regulatory requirements and internal safeguards include:

- Federal Requirements to Protect Information: Title V of the GLBA and its implementing rules and regulations require credit unions to protect the security, integrity, and confidentiality of consumer information.

- Federal Requirements to Notify Consumers: Credit unions are required to notify their members whenever there is a data breach where the misuse of member information has occurred or where it is reasonably likely that misuse will occur.

- Strong Federal Oversight and Examination: Under their broad-based statutory supervisory and examination authority, the National Credit Union Administration (NCUA) and the Consumer Financial Protection Bureau (CFPB) regularly examine credit unions for compliance with data protection, privacy, and notice requirements.

- Strong Federal Sanction Authority: Under numerous provisions of federal law, credit unions are subject to substantial sanctions and monetary penalties for failure to comply with statutory and regulatory requirements.

While this extensive legal and regulatory examination and enforcement framework ensures that credit unions robustly protect consumers' personal financial information, this safety net only extends to financial institutions. As consumers' personal information is disseminated to third parties, those protections end and credit unions and their members are adversely impacted by the lax data security standards at other businesses. These loopholes must end and a comprehensive data security and privacy framework that covers all entities that that collect consumer information and is preemptive of state laws must be established and this standard must hold those who jeopardize that data accountable through enforcement.

With that in mind, we ask the committee to consider the following data security and privacy principles for any comprehensive framework:

New Privacy and Data Security Laws Should Keep GLBA Intact: Congress should leave financial services' robust data and privacy requirements in place. Financial services and the healthcare industry are subject to federal data privacy laws. The GLBA and the Health Insurance Portability and Accountability Act (HIPAA) have protected American's PII for over two decades and should be left in place as financial services and healthcare and their respective regulators have developed regulations, guidance, and procedures for compliance.

Data Privacy and Data Security Are Hand in Glove: Any new privacy law should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured. Congress should enact robust data security standards to accompany and support data privacy standards.

Every Business Not Already Subject to Federal Law Should Follow the Same Rules: The new law should cover all businesses, institutions, and organizations. Consumers will lose if Congress focuses only on tech companies, credit-rating agencies, and other narrow sectors of the economy because any company that collects, uses, or shares personal data or information can misuse the data or lose the data through breach.

There Should Be One Rule for the Road: Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. We understand that some states have strong security and privacy requirements. Congress should carefully examine those requirements and take the best approaches from state law, as appropriate. A patchwork of state laws with a federal standard as a floor will only perpetuate a security system littered with weak links. The federal law should be the ceiling and the ceiling should be high. Just like moving away from the sector specific approach, the goal should be to create a strong national standard for all to follow.

Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy: Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement: The law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breach. Increasingly, courts are recognizing rights of action for individuals and companies (including credit unions). However, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to act against entities that violate the law.

Recognize This Issue For What It Is – A National Security Issue: More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding, and using PII do so with the security of the information of paramount concern. You simply cannot have data privacy unless there is data security.

On behalf of America's credit unions and their more than 135 million members, thank you for your consideration of our views and for holding this important hearing.

Sincerely,

Jim Nussle
President & CEO

April 27, 2023

The Hon. Gus Bilirakis
Chairman
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce
2306 Rayburn House Office Building Washington, D.C. 20515

The Hon. Jan Schakowsky
Ranking Member
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce
2408 Rayburn House Office Building Washington, D.C. 20515

Re: Hearing: “Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information”

Dear Chairman Bilirakis and Ranking Member Schakowsky:

Attached please find U.S. PIRG’s statement for the record for your hearing on “Addressing America's Data Privacy Shortfalls.”

It describes the inherent danger in preempting the states on page 2 in greater detail. We also believe it would be a mistake to exempt all entities covered by the Gramm -Leach-Bliley Act from your legislation and would be happy to discuss this further. Please let me know if you have any questions.

Sincerely,

Ed Mierzwinski
Senior Director, Federal Consumer Program, PIRG
edm@pirg.org

Testimony of
Edmund Mierzwinski

Senior Director, Federal Consumer Programs
U.S. Public Interest Research Group

At a Hearing On

Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System

Before the U.S. House of Representatives Committee on Financial Services

The Honorable Maxine Waters, Chairwoman

---

26 Feb 2019

Chairwoman Waters, Mr. McHenry, members of the committee. My name is Edmund Mierzwinski, Senior Director for Federal Consumer Programs at the U.S. Public Interest Research Group, which serves as the federation of state PIRGs, which are member-based, non-profit, non-partisan research and advocacy organizations around the country.

1. Summary

Thank you for the opportunity to testify today on the important matter of Fair Credit Reporting Act (FCRA) reform. The law was passed in 1970 and has been amended over the years. It regulates the activities of consumer reporting agencies (CRAs), commonly called credit bureaus. What is a CRA, or credit bureau? We like one court's description of the behemoth Experian as a "company that traffics in the reputations of ordinary people."[1]

We have prepared a rough timeline of some major consumer reporting problems that have led to state or federal policymaker reforms and enforcement actions by the Federal Trade Commission or Consumer Financial Protection Bureau. The list also includes enforcement actions by state attorneys general and consumer protection attorneys, who each play a critical role in reining in the CRAs. The timeline is attached as an appendix to this report. We hope it is helpful and I can answer questions about any of its items.

I first testified before this committee[2] on credit reporting mistakes in 1989, at a time when several states and the Federal Trade Commission (FTC) were conducting investigations and negotiating consent decrees with several large consumer reporting agencies[3] due to a troubling pattern of consumer complaints over both their mistakes and their recalcitrance and failure to correct the mistakes after consumers exercised FCRA-mandated dispute rights.

That 1989 hearing was the first real effort by Congress to rein in the credit bureaus since passage of the original act in 1970. Since then, Congress has continually conducted oversight and, in response to industry's indifference to the problems it causes for consumers seeking financial or employment opportunity, has enacted significant reforms in 1996, 2003 and 2010.

---

[1] See https://caselaw.findlaw.com/us-9th-circuit/1209375.html

[2] House Banking Committee, Subcommittee on Consumer Affairs and Coinage, Hearings on Fair Credit Reporting, 13 Sept 1989. (After the Gramm-Leach-Bliley Act of 1999, the full committee's name was changed to Financial Services Committee.)

[3] "Credit bureau" is a widely used colloquial term for Consumer Reporting Agencies regulated under the Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681 *et seq.* The so-called Big 3 bureaus, Equifax (formerly Retail Credit Company), Experian (formerly TRW) and TransUnion now qualify as Nationwide Consumer Reporting Agencies (15 U.S.C. § 1681a(p)) and face greater responsibilities under the act. Many other firms, including specialty CRAs offering check cashing and bounced check databases, employment background checks, tenant screening, medical insurance and other services are regulated under the act's definitions. However, the Big 3 continue to grow, with their recent acquisitions of competitors: for example, Experian acquiring Clarity Services, Equifax buying DataX and TransUnion buying FactorTrust, all in the last few years. The 3 smaller firms fashion themselves as alternative databases operating in the subprime space.

States Lead the Way

Critically, each federal reform was preceded by major accomplishments at the state level. A key part of my message today is that continued state leadership in all areas – from climate change to credit reporting and privacy and digital rights more broadly– is critical to the advancement of this nation's policies to improve consumer welfare, health and safety and liberty.

Numerous states emulated California's pioneering auto emissions rules, protecting the environment for us and future generations. As you know, those state rules are currently under administrative threat. The pioneering 2018 California Consumer Privacy Act is now under attack in the Commerce committees of both houses by a phalanx of powerful corporate interests led by Google, Facebook, Amazon and the telco/cable ISPs. If they win preemption of state laws, consumers and citizens lose, forever.

The big CRAs were early advocates of eliminating the right of states to protect their citizens. If the credit bureaus and banks had succeeded **in 1992** in their brazen House effort to reverse the FCRA's longstanding standard that the FCRA serve as a floor of protection, not a ceiling, and at that time 27 years ago successfully preempted all state laws related to credit reporting, we would not have nationwide free credit reports, we would not have access to our credit scores, we would not have identity theft protections, we would not have data breach notices, and we would not have the free nationwide credit freezes finally enacted in 2018.[4] Congress only acts to protect consumers after a disaster (cue 2008 financial collapse) or after several states act first. Industry's goal is to take state innovators and consumer cops off the credit bureau beat.

In this testimony, in addition to detailing the need for consumer reporting reform, we call on Congress to ensure that Equifax finally pays a price for its massive 2017 data breach affecting over 148 million consumers.

Finally, we offer our strong support to the two draft bills from Chairwoman Waters and other members, which are before the committee today. The first, a new version of the Chairwoman's Comprehensive Consumer Credit Reporting Reform Act, is a response to the problems posed to all consumers by the failure of the consumer reporting system. That system is dominated by its Big 3 members – Experian, Equifax, and TransUnion -- as self-appointed gatekeepers to financial and employment opportunity. Their lack of innovation and propensity toward mistakes perpetuates injustices and denies opportunity to many, especially lower-income consumers and people of color. The second bill, the "Protecting Innocent Consumers Affected by a Shutdown Act," will force the CRAs to lend a hand to the restoration of the financial lives of the government employees and contractors harmed by the recent extended shutdown. Since 1989, I have observed the arrogant attitude of the CRAs. They've always claimed that mistakes, let alone credit problems, aren't their fault; they simply report what they are told. It is literally the Bart Simpson defense: "It's not my fault." They won't change unless you make them. Passage of these two bills will make them change.

---

[4] In 1992, after Congressional consumer champions could not remove an amendment inserted in committee at the behest of the banks and CRAs, preempting all state laws under the FCRA, consideration of the Consumer Credit Reporting Reform Act of 1991, HR3596, was ended by a "House motion to rise" requested by consumer groups. See https://www.congress.gov/bill/102nd-congress/house-bill/3596

2. This Story Is About Consumers, Who Are Products, Not Customers, of the CRAs

This story is not simply about three big CRAs (credit bureaus) named Equifax, Experian and Trans Union. It is also about numerous specialty credit bureaus and also about numerous emerging companies that don't know or don't want to admit their products are consumer credit reports regulated under the FCRA.

It is also about the responsibilities of the creditors that voluntarily "furnish" information to CRAs.[5] Why do they do this? The theory is simple. If more credit files are available about more consumers and contain more trade lines (accounts) about consumer history, then the consumer reporting database will be more valuable to users. Most of the creditor-furnishers of information to the CRAs are also customer-users of the CRAs. The business customers gain the benefit of a larger database; they also have responsibilities as users of credit reports.

Yet, mostly it is about the plight of **consumers** whose financial and other histories are the subjects of credit reports, which are bought and sold without our consent. **We are not their customers; we are their product.** Note that this has not stopped the CRAs from developing a lucrative, multi-billion dollar marketing channel of subscription-based credit monitoring and identity theft protection products designed to play to our fears of low credit scores or imposters stealing our name.[6]

In reality those credit scores are low because the CRAs haven't been forced to do a better job protecting our files from misuse or to keep them accurate or to respond to us properly when we dispute the mistakes. Imposters prevail because of flaws in the credit granting system and debacles such as the Equifax breach that make financial DNA freely available. Instead of carrying out their statutory duties, the CRAs have persisted in ignoring them while simultaneously aggressively hawking a variety of over-priced self-help products.

In 2017, the CFPB fined Equifax $2.5 million; Transunion $3 million and Experian $3 million over deceptive marketing of credit monitoring products by offering deceptively marketing "educational" credit scoring products, not the scores actually used by lenders to make decisions. The CFPB also ordered Transunion to pay $13.8 million and Equifax to pay $3.8 million in consumer refunds for using bait and switch trial subscriptions.[7] If these products had the actual

---

[5] Furnishers did not have any duties until 1996 amendments. Duties to provide complete and accurate information are solely enforceable by regulators; private enforcement is available only when furnishers are notified of reinvestigation disputes (See FCRA Section 623, 15 USC 1681s-2).

[6] This lucrative channel includes identity theft protection and subscription credit scoring products. "The private research firm IBISWorld estimated that the U.S. market for identity theft services was about $3 billion in 2015 and 2016." See page 5, "Identity Theft Protection Services," U.S. GAO, March 2017, available at https://www.gao.gov/assets/690/683842.pdf.

[7] These enforcement actions were carried out under the first confirmed CFPB director, Richard Cordray. News release, CFPB, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 Jan 2017, see https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/ and News Release, CFPB, "CFPB Fines Experian $3 Million for Deceiving Consumers in Marketing Credit Scores," 23 March 2017, see https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-experian-3-million-deceiving-consumers-marketing-credit-scores/

value affixed to the price ($19.99/month and up), they would be sold as stand-alone products that would jump off the shelves.

3. What triggered passage of the 1970 Fair Credit Reporting Act?

In 1968 Representative Clement Zablocki (WI) offered an unsuccessful amendment to regulate credit reporting during consideration of the original Truth In Lending Act. Hearings were then held by the Senate and House by Sen. William Proxmire (WI) and Rep. Leonor Sullivan (MO). The complaints that triggered Congressional interest focused on a variety of deprivations by credit bureaus but a key driver of the hearings was complaints about the Retail Credit Company's abusive investigations of consumers applying for insurance policies. The Fair Credit Reporting Act was enacted in 1970 and in 1975, Retail Credit Company changed its name to Equifax.

While the original act restricted the sale of reports to limited purposes, provided certain rights for consumers and imposed responsibilities on credit bureaus and credit report users (but not yet on voluntary "furnishers of information"), some consumer advocates withdrew support when the final law included an industry-supported amendment providing qualified immunity from state defamation laws.

Early Consolidation Led to Mistake Patterns and Lack of Compliance That Continue Today; Sloppy Practices Also Lead to Identity Theft

Following passage of the act and the acceleration of industrial computerization, local and state credit bureaus began a first major wave of consolidation that resulted in 5, then 3 national CRAs by the early 1990s. A series of early 1990s reports by U.S. PIRG, Consumer Union (now Consumer Reports) and certain non-aligned CRAs confirmed widespread complaints.[8] U.S. PIRG, through FOIA requests, found credit bureau complaints led all others to the FTC in the early 1990s.[9] The consolidation of databases written in different programming languages and

[8] James Williams of Consolidated Information Services, a New York area retail mortgage credit reporting agency, in 1991 analyzed 1500 reports from the three big bureaus and found errors in 43 percent of the files. It and other smaller resellers of consumer credit reports are regulated by the FCRA; they are also customers of the Big 3, which are also known as data repositories. Over time, the number of these resellers, which in the 1980s and 1990s had an important role in conducting manual underwriting (line-by-line human review of consumer credit reports) has dwindled and their business models have changed, under pressure from the CRAs. But they have produced at least one other study of accuracy. See, for example, Consumer Federation of America and the National Credit Reporting Association, "Credit Score Accuracy and Implications for Consumers," 17 Dec 2002, at https://consumerfed.org/pdfs/121702CFA_NCRA_Credit_Score_Report_Final.pdf. This detailed study of credit scores derived from over 500,000 consumer credit files also provides a useful history of other studies of credit reporting accuracy and a discussion of the migration of credit and, especially, mortgage decision-making from manual to automated underwriting.

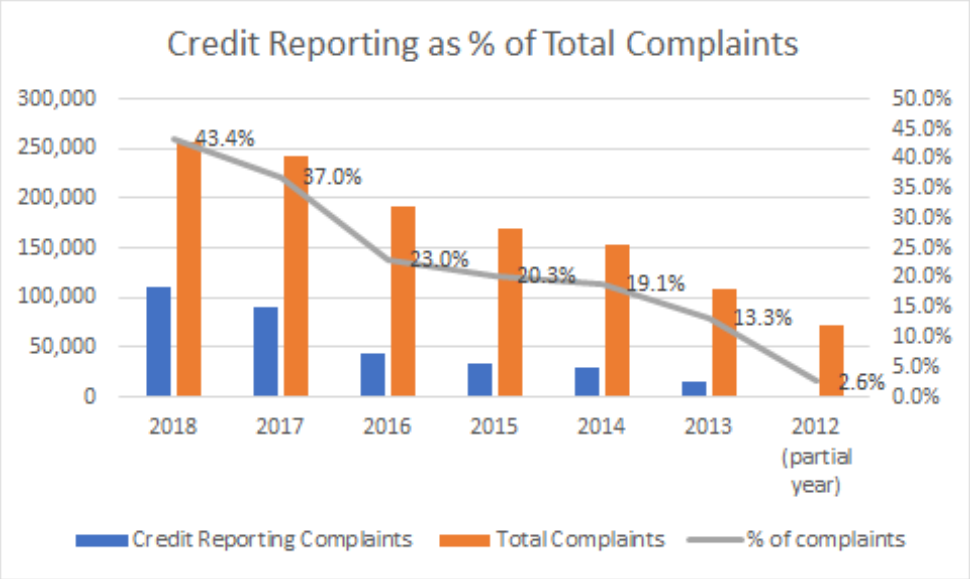
[9] See the following state PIRG reports: *Nightmare On Credit Street (Or How The Credit Bureau Ruined My Life): Case Studies Documenting Consumer Complaints and Recommendation For Amending the FCRA*, June 12, 1990; *Don't Call; Don't Write; We Don't Care,* 1991, which reviewed 156 consumer report complaints on file at the FTC and revealed that the average duration of complaints against a credit bureau was 22.5 weeks, or almost 6 months; and *Public Enemy #1 at the FTC,*" October 1993. Based on a Freedom of Information Act request, the 1993 report found that between 1990 and 1993, problems with credit bureaus was the leading cause of complaints to the FTC (30,901, 20.6%). *Public Enemy* also found

non-standard reporting formats – along with lax enforcement of the law – certainly contributed to the problems identified by the FTC, state attorneys general, Congress and consumer groups.

The mistakes and problems we found in the early 1990s continued. In the mid-1990s, we documented the rise of identity theft, which left more consumers struggling with the credit report dispute process.[10] ID theft was fueled by the easy availability of Social Security Numbers and a security flaw in the credit granting process. An identity thief doesn't need to obtain your credit report (which requires you to verify a lot of identifying information, try it). The thief simply applied for credit in your name, with your SSN and his/her address. The retailer or creditor, a trusted third party to the CRAs, obtains your credit report and issues credit in your name, to the imposter using your SSN, at the imposter's address.

In 2013, the Federal Trade Commission found that 26% of consumers had at least one mistake that "might affect their credit scores" in one of their credit reports and 5% of all consumers had "errors on one of their three major credit reports that could lead to them paying more for products such as auto loans and insurance."[11]

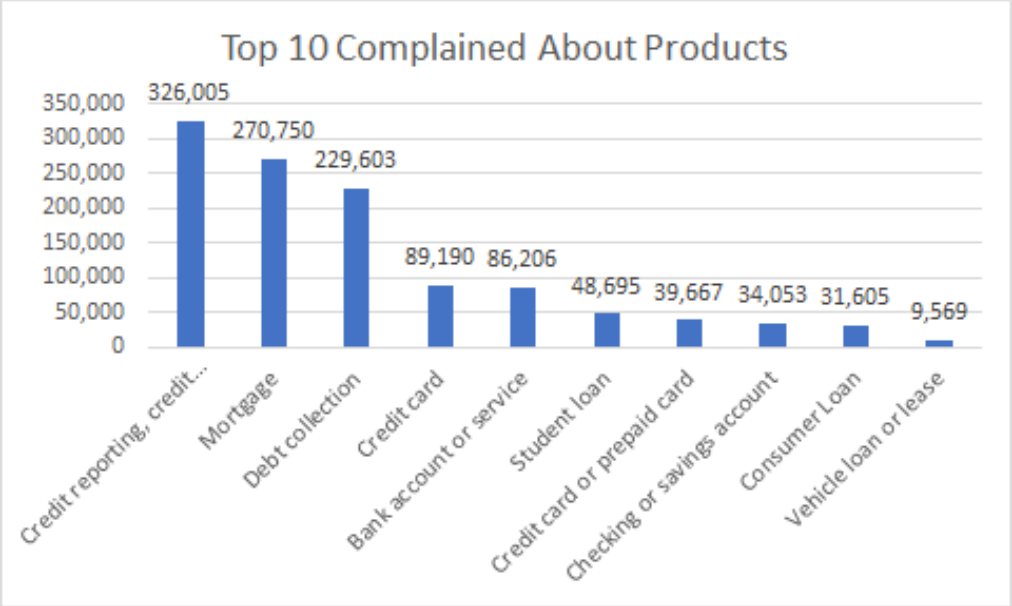
U.S. PIRG's regular reviews of the very important CFPB Public Consumer Complaint Database have most recently found the following, with 85% of all credit reporting complaints directed at Equifax, Experian and TransUnion:



that 44% of complaints concerned mixed files, and that among those, 64% involved the mixing of data with total strangers. We have published additional reports on consumer reporting errors, disputes and complaints in 1998, 2004 and 2014.

[10] See CALPIRG and U.S. PIRG, "Identity Theft: The Consumer X-Files," 1996, and "Identity Theft II: Return to the Consumer X-Files" and CALPIRG and the Privacy Rights Clearinghouse, "Nowhere to Turn: Stories from Identity Theft Victims," 2000.

[11] Federal Trade Commission, "In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans," 11 Feb 2013, see https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports



The public CFPB Consumer Complaint Database is a critical tool for consumers, academics and other researchers and even competitors to make consumer financial markets work better.[12] Efforts by special interest groups to kill it must be rejected.[13]

4. The Failures of the FTC To Bring the CRAs to Heel Over 40 Years

The Federal Trade Commission fought the credit bureaus with one hand tied behind its back from 1970-2010. The FTC had no or little rulemaking authority under the FCRA nor did it have supervisory or examination authority—the right to look inside the black box of CRA operations at any time to determine compliance and stop problems before the problems became worse.

Since 1970, we are only aware of one public civil penalty imposed by the FTC against the three CRAs for violating the FCRA. In 2000, in an action called Operational Busy Signal, the 3 were fined a total of $2.5 million for not having enough human staff to answer the complaint hotlines.[14] In 2007, under the FTC Act, not the FCRA, Experian subsidiaries were fined $300,000 for violating a consent decree issued in 2005 for deceptive marketing of its credit report monitoring subscription products.

[12] Since 2013, U.S. PIRG has released more than a dozen reports analyzing complaints in the database, on subjects including credit reports, and on categories of consumers, including the targeting of servicemembers by financial predators. See https://uspirg.org/page/usp/reports-cfpb-gets-results-consumers

[13] Our June 2018 report, "Shining A Light on Consumer Problems: The Case for Public Access to the CFPB Complaint Database," summarizes why the database must remain open. See https://uspirg.org/reports/usp/shining-light-consumer-problems

[14] In 2000, Experian and TransUnion were fined $1 Million and Equifax $500,000 for a total of $2,500,000 in the FTC's "Operation Busy Signal," for failing to comply withw a 1996 amendment to have adequate humans on hand to answer complaint calls.

Creation of the new Consumer Financial Protection Bureau, established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, largely remedied these deficiencies. The CFPB was given full rulemaking over 19 different consumer laws, including the FCRA.[15] The CFPB also has other authorities that the FTC lacks, including the right to impose penalties at any time[16] and supervisory or examination authority[17]—the right to look inside the black box of covered firms at any time to determine compliance and stop problems before the problems became worse.

The CFPB has exercised robust research,[18] examination and supervisory authority over the consumer reporting markets.[19] Yet, in one curious exception, with relevance to the Equifax breach, authority over CRA data security was retained by the FTC in Section 1031 of the Dodd-Frank Act. Title V of the Gramm-Leach-Bliley Act of 1999 had given the FTC authority to write rules establishing data security responsibilities for non-bank financial firms, including CRAs. Its data security rule is known as the "Safeguards Rule."[20] While the CFPB is reportedly pursuing an Equifax investigation and likely can defend its data security actions under its other authorities, it makes sense to transfer GLBA Title V authority to the CFPB, as recommended by the National Consumer Law Center in recent testimony before the committee.[21]

[15] The FTC retains joint authority over the FCRA, in addition, it retained a number of its own staff expert in the FCRA; annually the two agencies sign a Memorandum of Understanding concerning their shared FCRA duties.

[16] Although FTC can impose penalties for any violation of the FCRA or the Fair Debt Collection Practices Act, it can only impose civil penalties under either tits core authority under the FTC Act or its GLBA requirements after a firm is found to be in violation of an FTC-imposed consent decree.

[17] Congress gave the CFPB supervisory authority over banks > $10 Billion Dollars in asset size and over payday lenders, non-bank mortgage companies and private student lenders of any size. It also gave the Bureau, under Section 1024 of the Dodd-Frank Act, authority to write rules granting itself authority to supervise larger participants in other important financial markets. It has used the authority several times; notably, its first larger participant rule, in 2012, was over the consumer reporting markets. https://www.federalregister.gov/documents/2012/07/20/2012-17603/defining-larger-participants-of-the-consumer-reporting-market

[18] See "Key Dimensions and Processes in the U.S. Credit Reporting System: A review of how the nation's largest credit bureaus manage consumer data," December 2012, https://www.consumerfinance.gov/data-research/research-reports/key-dimensions-and-processes-in-the-u-s-credit-reporting-system/

[19] See "Supervisory Highlights: Consumer Reporting Special Edition," 2 March 2017 https://www.consumerfinance.gov/data-research/research-reports/supervisory-highlights-consumer-reporting-special-edition/

[20] See https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

[21] See page 8, Testimony of Chi Chi Wu, National Consumer Law Center, House Financial Services Committee "Continuation of Hearing Examining the Equifax Breach," 25 October 2017, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400866

5. Equifax Showed Gross Indifference to its Responsibilities to Protect Consumer Information; Its Data Breach Response Made Things Worse

Several Congressional committees have held hearings and/or issued staff reports detailing the Equifax breach. U.S. PIRG's own September 2018 report, "Equifax Breach One Year Later," summarized the following major problems:[22]

Had Equifax not been so careless, the breach may never have happened. Four months before the hacking, Equifax could have fixed a known security vulnerability in the widely-available and used Apache Struts open-source platform. Innumerable warnings from government security agencies and private experts were not acted on.

As explained in our report, the company also botched its response by:

- Delaying public notification for at least six weeks
- Setting up an online search tool that provided faulty results to those who used it about whether they were affected by the breach
- Initially understaffing its call center
- Initially including arbitration language that forced consumers to sign away their rights to a day in court
- Directing consumers to a fake website
- Failing to provide consumers full protection from new account identity theft -- which it still hasn't done. (See Appendix A for a summary of Equifax's offerings to consumers in response to the breach and how they fall short of protecting consumers.)

Despite all the outrage and media attention last year, Congress has done little except make security freezes free, and even then, done so in a manner favorable to Equifax and the other CRAs, by preempting the right of states to enact stronger freeze protections going forward. Of course, the idea of the freeze didn't come from Congress, it came from 50 state freeze laws passed between 2003 and 2018. The idea of the free freeze also was jump-started by several free freeze amendments to existing state laws passed after the 2017 Equifax breach but before Congress passed S2155 in May 2018. That law created several minor consumer protections—but both the preemptive free freeze right and a military credit monitoring "right without a remedy" if monitoring was not provided were imperfect efforts. The comprehensive Waters CCRRA reform will cure both these problems. Congress should never preempt the states, especially at the behest of powerful special interests.

Also, critically important, Equifax has neither been held accountable nor paid a price for its breach. Further, this sensitive information, including Social Security numbers and birth dates, is still out there, with the potential to wreak havoc for the majority of consumers in perpetuity.

6. It Is Critical to Pass the Two Bills Before the Committee Today

Finally, we offer our strong support to the two discussion drafts from Chairwoman Waters and her co-sponsors before the committee today. The first, the Comprehensive Consumer Credit

[22] Mike Litt, U.S. PIRG, "Equifax Breach: One Year Later: How to Protect Yourself Against ID Theft & Hold Equifax Accountable," 6 Sept 2018, available at https://uspirg.org/reports/usp/equifax-breach-one-year-later

Reporting Reform Act (CCRRA) of 2019, is a new version of the Chairwoman's longstanding effort to correct flaws in the consumer reporting system. It is a broad and thoughtful response to the problems posed to all consumers by the failure of the consumer reporting system, dominated by its Big 3 members as self-appointed gatekeepers to financial and employment opportunity. These firms have demonstrated for years that they lack the key incentives to do their jobs. Their failures perpetuate injustices that raise costs for nearly everyone and deny opportunity to many.

The second bill, the "Protecting Innocent Consumers Affected by a Shutdown Act," will force the CRAs to lend a hand to the restoration of the financial lives of the government employees and contractors harmed by the recent extended shutdown.

Since 1989, I have observed the bad attitude of the CRAs. They've always claimed that mistakes, let alone credit problems, aren't their fault; no, they claim "we simply report what we are told and if it is wrong, or negative, so what." They won't change unless you make them. The shutdown bill will make them take action to help people harmed through no fault of their own. The CCRRA addresses endemic problems in the consumer reporting system.

Title I of CCRRA: New Right of Appeal Critical to "Fixing the Dispute Process"

I will never forget the plea to the FTC by one of the consumers highlighted in U.S. PIRG's first report on credit bureau errors and failure to fix them. In 1990, the consumer asked: "It says "Item Remains, Confirmed By Source." What is this source!?"" A review of several narratives in the CFPB public consumer complaint database finds similar unanswered complaints from consumers continue today:

> "Experian states that the information remains…." [or] "Equifax completed the investigation yet this item still remains on my Equifax Credit Report...." [or] "According to TransUnion 's updated credit file on XX/XX/2017 (# XXXX), XXXX # XXXX ... .. should be removed XX/XX/2017. As of XX/XX/2017, this item remains…." [or] "their responsibility must consist of something more than merely parroting information received from other sources…" [or] "I have asked Experian to provide the name of the data furnisher or third party source who verified this information so that I can contact them directly. Experian refuses to provide this information…" [or] "I have disputed this account several times online and in writing with no resolution. This account still remains on my credit report…"

So, the dispute system, despite efforts in 1996 and 2003 to fix it, is still broken. Title I of the CCRRA makes significant improvements. Most notably, for the first time, it establishes a right to appeal disputes. Title I also includes new matching procedures and other requirements to prevent disputed information from being routinely reinserted into consumer reports. Until now, greater weight has been placed on the opinion of "the source" furnisher than the consumer and less weight has been placed on whether an actual reinvestigation ever occurred, or whether the furnisher and CRA computers simply agreed that they both contained the same data, even if it was wrong.

Title II of CCRRA Limits the Use of Consumer Reports for Most Employment Decisions

Several states, including California, Colorado, Maryland and Oregon, and cities such as Chicago and New York have restricted the use of consumer reports for employment decisions. Further, the industry has admitted in testimony that it cannot show a relationship between a consumer's credit report and job performance.

Further, should any consumer be denied employment opportunity in a difficult economy due to a disputed item, or even an actual late payment, on a credit card?[23] The problem is harshest on persons of color and lower income consumers with "thinner" credit reports. Historically, their credit opportunities have not been extended from the national firms that dominate the credit system. Should their job opportunities be similarly diminished by their credit reports?

Title III of CCRRA Improves Rights of Victims of Private Student Loan Borrowers

The title provides new protections for victims, including servicemembers and others, of unfair private student loan practices.

Title IV of CCRRA Makes a Variety of Changes to Rebalance the Reporting of Adverse Items

Credit scoring models prioritize the value of recent trade line information over much older information. Begrudgingly, under order by enforcement actions, the CRAs have also reduced the impact of non-predictive data, such as medical debt, and removed public records known to be full of misinformation. Yet, in general the CRAs have long resisted any changes to the types of information that they can collect or report or how long they can report it, even if it is now known to be non-predictive.

Title IV makes important changes to make reports more accurate and predictive. It shortens the reporting of certain bankruptcies from 10 to 7 years, eliminates reporting of certain public records and reduces the reporting of credit trade lines from 7 to 4 years, among other changes. It greatly reduces the impact of medical debt items, which are often mistaken due to bills that should be the responsibility of slow-pay insurance companies but are sent to collection under the consumer's name. Further, medical debt is the result of getting sick, or laid off, or losing insurance coverage, not due to a propensity toward "spending sprees." Both leading credit scoring models, FICO and VantageScore, a joint venture of the Big 3 CRAs, have already reduced or eliminated reliance on medical debt items.

Title IV also provides protection to victims of for-profit schools and other abusive practices.

Title V of CCRRA Establishes Oversight of Credit Scoring Models and the Use of Non-Traditional Data

Title V gives the Consumer Bureau clear authority to monitor and oversee the validity of credit scoring models to ensure that the often-opaque algorithms are accurate and predictive and do not

[23] See testimony of Chi Chi Wu, National Consumer Law Center, at a "Legislative Hearing on HR3149, the Equal Credit For All Act," Subcommittee on Financial Services and Consumer Credit, 23 Sept 2010, http://archives-financialservices.house.gov/Hearings/hearingDetails.aspx?NewsID=1355

introduce scoring factors that could violate the civil rights or fair lending laws. Further, Title V requires a Consumer Bureau study of the use of non-traditional data in consumer reporting. Alternative data is a shiny new toy you'll hear a lot about, but could have negative or unintended consequences, especially for some of the populations its proponents claim that it will assist.

Title VI of CCRRA Provides for Free Annual Credit Scores and Improves Requirements on Consumer Report User Firms to Promote Consumer Understanding of the Use of Reports and Scores

In the early 1990s the FTC proposed an interpretation that credit scores were, by definition, part of consumer credit reports that should be included in credit report disclosures[24] to consumers. Under an industry full-court press, it immediately reneged on this consumer-backed idea.

In 2000, following a joint campaign by realtors and consumer groups, California prohibited clauses in CRA contracts with users such as real estate agents that prevented them from showing credit scores to consumers. Since then, the veil over credit scores has gradually lifted. The CRAs have long-sought to monetize their disclosure, unfortunately also through deceptive marketing of "educational" scores, not the scores actually used by creditors.[25] It is past time to provide scores for free as part of the annual free report disclosure first required nationwide by the 2003 FACT Act. Section 604 of the CCRRA provides free credit scores in this and other circumstances.

Title VI also requires various users to provide consumers with additional information to improve their understanding of the consumer reporting system.

Title VII of CCRRA Bans Misleading and Unfair Consumer Reporting Practices

Even though we are not their customers, only their product, nothing has stopped the CRAs from developing a lucrative, multi-billion-dollar marketing channel of subscription-based consumer credit monitoring and identity theft protection products designed to play to our fears of low credit scores or imposters stealing our name.

Our credit scores are low because the CRAs haven't been forced to do a better job protecting our files from misuse or to keep them accurate or to respond to us properly when we dispute the mistakes. Instead of carrying out these statutory duties, the CRAs have persisted in aggressively hawking a variety of over-priced self-help products, often in an unfair or deceptive way.[26] Title

[24] The FTC did not have any rulemaking authority under the FCRA until limited authorities were granted in the 2003 FACT Act. In previous years, its views were described in often-amended "FCRA Interpretations" and through staff opinion letters.

[25] The CFPB used director Richard Cordray's bully pulpit very effectively to nudge more banks and credit unions to greatly expand the availability of free credit scores. Its most recent list is available: Skyricki, Irene, "A new list identifies more ways to access credit scores—for free," CFPB, 16 May 2018, at https://www.consumerfinance.gov/about-us/blog/new-list-identifies-more-ways-access-credit-scores-free/

[26] For deceptive marketing of subscription products by CRAs, see news release, CFPB, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 Jan 2017, at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/ and News Release, CFPB, "CFPB Fines Experian $3 Million for Deceiving Consumers in Marketing Credit Scores," 23

VII would provide a variety of new protections against unfair and deceptive marketing of these products. Low-value versions of these products are often provided free after a data breach but consumers face a barrage of online and televised ads extolling the supposed virtues of upgrading to a $19.99/month, or even higher-priced, products. Section 703 gives the Consumer Bureau authority to restrict the prices of the subscription products.

Title VII provides additional protections to consumers with limited English proficiency and mandates by law that shopping around, for example, for a good deal on a new car, is not treated in credit scores as multiple applications for credit with multiple "dings" to a credit score. Further Section 707 establishes, for the first time, national registration of national and specialty CRAs to make it easier for the Consumer Bureau, FTC and consumers to hold them accountable.

Highlights of Title VIII of CCRA, Which Provides Additional Consumer Protections

The CRAs have long-imposed barriers on consumers fighting identity theft. Section 801 makes clear that there are a variety of ways a consumer can file a lawful identity theft affidavit, even if their local police do not take identity theft complaints. Most don't.

Section 802 makes improvements to the rights of protected or incapacitated consumers.

Section 803 improves statutory fraud alert rights for both consumers and active duty military personnel.

Section 804 corrects a CRA-driven provision in 2018 amendments that established a free national credit freeze right, but preempted states from providing additional, stronger protections. Section 808 corrects a separate 2018 amendment that provided servicemembers with free credit monitoring, but did not give them a remedy if the services were not provided.[27]

Title IX makes certain other amendments to ensure that the CRAs and other firms act in the public interest and under the law and requires the Consumer Bureau to complete rulemaking under the CCRRA within two years of passage.

6. Conclusion

This testimony and the attached timeline make an effort to describe how consumer reporting agencies have no incentives to sell accurate credit reports, so they do not. We also concur with the detailed testimony of my consumer and civil rights colleagues on the panel today, as well as the statements for the record submitted by a number of other consumer and civil rights advocates.

To protect consumers and ensure that markets work fairly, a combination of strong federal laws enforced by strong federal agencies must be accompanied by the right of states to respond more quickly to new threats in the marketplace. Further, full enforcement rights by state Attorneys

March 2017, at https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-experian-3-million-deceiving-consumers-marketing-credit-scores/

[27] The provisions were included in S2155, a deregulatory proposal which became law as the Economic Growth, Regulatory Relief, and Consumer Protection Act (Public Law 115–174).

General and local officials and strong private rights of action so that consumer protection attorneys can act as private attorneys general are also needed. The message is clear. Congress cannot solve every problem. Federal agencies cannot go it alone.

Going forward, we also look forward to working with the committee on newer and emerging problems of consumer protection, privacy and digital rights in the financial marketplace. For example, a large class of nearly unregulated data brokers sells products that are virtually identical to consumer credit reports, but not sold for "credit, insurance or employment purposes," so remain outside the protections of the FCRA. So-called lead generators sell lists of consumers, including to predatory lenders, derived from tracking their Internet activities. Pre-approved marketing decisions are being made, in real time, based on unregulated "e-scores" and look-alike consumers. Since the reports are not about a particular consumer, the firms contend their products are not regulated consumer reports.

As we point out on our "Digital Data and Consumer Protection Page:[28]"

> "American consumers face new challenges and opportunities to their financial security as our economy is transformed by the convergence of digital media with "Big Data" technologies. Our use of mobile phones, social media, "apps," and other online tools have created new ways for us to spend, save and borrow money. Powerful forces are at work, however, that can undermine a consumer's ability to make the best choices and may place those already financially at risk even more vulnerable. The digital data-driven economy continually gathers vast amounts of information on individuals, online and offline, which is used to create a "profile" about our spending habits, behavior and our geo-location. These profiles can be "scored"—an invisible measure known only to the marketer and data brokers—that can determine whether we are offered high interest credit cards, payday and for-profit college loans and even what we may pay at retail and grocery stores. The uses of the information can be positive or, absent any regulation or meaningful protections, lead to discrimination, price manipulation or denied opportunity."

Thank you again for the opportunity to provide our views to the committee today. I look forward to your questions.

Appendix: Timeline of Significant Credit Reporting Events and Policymaker Responses

[28] See https://uspirgedfund.org/issues/usf/digital-data-and-consumer-protection-ensuring-fair-and-equitable-financial-marketplace

QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	**Problem/Policy**	**What Was the Problem; What was Response?**
Late '60s	**CRA Problem**	Complaints grow about Retail Credit Corporation (now Equifax) insurance consumer report scandal
1970	Federal Response	**Congress holds hearings on scandal; enacts Fair Credit Reporting Act to regulate companies selling consumer reports (called credit bureaus or CRAs)**
1980s	**CRA Problem**	First wave of consolidation of local/regional credit bureaus results in increase in errors in consumer credit reports
80s-early '90s	Both State/Federal Response	Responding to errors, investigations by state attorneys general and FTC result in CRAs brought under consent decrees, no fines
		-- TRW (now Experian) signs multi-state and FTC consent order in 1991
		-- Equifax signs consent orders with states (1992) and FTC (1996)
		-- Trans Union signs consent orders with states in 1992 and FTC in 1994
1989	Federal Response	House Banking Committee (now FSC) holds first hearings in years on credit bureau errors
1991	**CRA Problem**	TRW (now Experian) incorrectly reports all citizens (3,000) of Norwich, VT area had failed to pay their taxes.
1992 - today	**CRA Problem**	By early 1990s, consolidations result in powerful gatekeeper "Big 3" national CRAs which now continue to acquire specialty competitors
1992	**CRA Problem**	**Sponsors remove FCRA reform, HR3596, from floor action due to sweeping preemption provision demanded by banks/credit bureaus**
Early 1990s	CRA Problem & Bad Policy Response	Use of non-transparent credit scores grows, FTC proposes FCRA interpretation that scores are part of credit reports; under industry pressure, reverses itself.
1992-1996	State Response	**States led by Vermont and California enact comprehensive credit report reforms; 7 states provide annual free credit reports (VT, then CO, GA, MA, ME, MD, and NJ)**
1994-today	**CRA Problem**	Rise of instant credit, easy availability of SSNs, other financial DNA, fuel rise of identity theft
1995-present	**CRA Problem**	**Instead of improving compliance, CRAs respond to threat of errors/identity thieves by intensifying scare marketing of credit monitoring add-on products to consumers --now fueling a $3 Billion/year marketing channel per GAO**
1996	Federal Response	**Congress finally passes Consumer Credit Reform Act (largely 1992's HR3596), imposes first duties on furnishers [creditors and debt collectors that provide information to credit bureaus] among other reforms. Limited preemption, primarily for new furnisher (bank) duties, to sunset after 8 years.**
1998	Federal Response	Congress criminalizes identity theft, bureaus can now claim ID theft not our fault, "it's bad guys."

QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	**Problem/Policy**	**What Was the Problem; What was Response?**
2000	Federal Response	Big 3 CRAs fined total of $2.5M (Experian $1M; Equifax $500k; TransUnion $1M) in Operation Busy Signal for failing to comply w/ 1996 amendment to have adequate humans to answer complaint calls
1998-2000	State Response	**California realtors join consumer groups to win right for consumers to see their credit scores, previously prohibited by CRA contracts with user companies**
2002	State Response	**California enacts first data breach notice law**
2003	State Response	**California develops/enacts credit freeze protection right to deter identity thieves**
2003	Federal Response	**Congress passes FACT Act; limited bank preemption made permanent; annual free credit reports (but not free scores) included. Few identity theft fixes.**
2003-2018	State Response	**Following PIRG/Consumers Union model law, 50 states enact credit freeze and data breach notice laws to supplement omissions in FACTA.**
2003	Consumer Action	Consumer protection attorney wins first case against a creditor-furnisher for failing to comply with FCRA in dispute investigation
2005	**CRA Problem**	**Equifax spinoff ChoicePoint fined record $25M by FTC for selling credit reports to identity thieves**
2005-2007	**CRA Problem**	Experian subsidiaries deceptively market subscription-based credit monitoring products by intentionally confusing them w/ free credit report by law
2005-2007	Federal Response	**FTC places Experian under consent order in 2005 for deceptive marketing of subscription products, orders $300k penalty in 2007 for violating 2005 order under FTC Act**
1970-2010	**CRA Problem**	FTC's lack of tools to enforce FCRA leaves consumers at risk of credit and job denial and identity theft as credit bureaus run amuck
2010	Federal Response	**Dodd-Frank Act gives CFPB primary authority over FCRA and new tools to regulate/supervise/investigate/enforce violations of the FCRA**
2012	Federal Response	**In CFPB's first establishment of a "larger participant rule," agency begins examinations (supervision) of large Consumer Reporting Agencies**
2012	Federal Response	**Major FTC study finds 26% of consumers have errors on at least 1 report; 5% of consumers have a serious error that could cause denial of credit or higher costs for credit**
2013	Federal Response	CFPB supervision results in CRAs sharing full consumer complaint files instead of 2-digit summary codes, w/ furnisher creditors in disputes, which advocates contend 1996 amendments had required for over 15 years.
1995-present	**CRA Problem**	**Instead of improving compliance, CRAs respond to sloppy mistake-ridden reports/growth of identity theft by intensifying scare marketing of credit monitoring add-on products to consumers -- now fueling a $3 Billion marketing channel, per GAO, even though consumers are their products, not their customers**

QUICK TIMELINE OF SELECTED CREDIT BUREAU (or CRA) EVENTS 1960s-TODAY		
Date	**Problem/Policy**	**What Was the Problem; What was Response?**
2017	Federal Response	**CFPB fines Equifax $2.5 million; Transunion $3 million and Experian $3 million over deceptive marketing of credit monitoring products by offering "FAKO," not FICO-like, credit scoring products. Also orders Transunion to pay $13.8 million and Equifax to pay $3.8 million in consumer refunds for using bait & switch trial subscriptions**
2017	Consumer Action	Consumer protection attorneys win $60 Million jury verdict against TransUnion for falsely labeling 8,000 consumers as terrorists or drug traffickers.
2012-2017	Federal Response	CFPB releases "Key Dimensions report" and several "Supervisory Highlights" reports that document deficiencies in the Big Three CRAs' dispute systems, confirming findings in NCLC's 2009 Automated Injustice report
2014-2017	Both State/Federal Response	**CFPB supervisory actions and a 31-state Attorney General settlement eliminate tax liens and civil judgements (often posted with inaccurate identifying information) from reports, raising credit scores for 12 million; and reduce the negative impact of medical debt on scores.**
2015	**CRA Problem**	Data breach at Experian involving database used for T-Mobile customers affects 15 million consumers
2017	**CRA Problem**	**Equifax breach: sloppy data security makes SSNs, other sensitive information for 148 million consumers available to outsiders**
2019	Federal Response To Breaches	**Still Waiting…**
2019	Federal Response	**Chairwoman Maxine Waters of House FSC Holds Important Hearing To Review Equifax Breach Response and Discuss Necessary Improvements To FCRA**
Thanks to Chi Chi Wu of National Consumer Law Center for providing ideas.		
U.S. PIRG is responsible for any inaccuracies.		