ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

# Maintaining a Light-Touch Approach to Data Protection in the United States

ASHLEY JOHNSON AND DANIEL CASTRO I AUGUST 2022

Data privacy regulations impose significant costs on businesses and the economy. Effective, targeted federal legislation would address actual privacy harms while reducing costs that hinder productivity and innovation.

## KEY TAKEAWAYS

- Privacy regulations carry two sets of costs: compliance costs imposed directly on businesses and "hidden costs" that affect the entire economy.
- Proponents of an approach that mimics the General Data Protection Regulation (GDPR) in the United States ignore the significant costs of such a law and the impact of higher compliance costs on businesses and consumers.
- A GDPR-style law would cost the U.S. $122 billion per year, including $106 billion in hidden costs. A more targeted, but still effective law would cost $6 billion per year, 95 percent less.
- Congress should pass federal data privacy legislation that preempts state laws, addresses specific privacy-related harms, distinguishes between sensitive and nonsensitve personal data, and does not contain a private right of action.

## INTRODUCTION

Comprehensive data privacy legislation has been on the congressional to-do list for years. As partisan debates and an unwillingness to compromise have stalled movement on the issue at a federal level, five states—California, Virginia, Colorado, Utah, and Connecticut—have passed their own laws, setting a trend that many more states are likely to follow.[1] Meanwhile, Europe's privacy regulation, the General Data Protection Regulation (GDPR) marked its sixth anniversary this year.

Congress is failing to meet the need for federal leadership on this critical issue for the digital economy, and in doing so, it is risking a state of play wherein organizations that handle personal data must comply with a patchwork of state legislation, driving up costs and creating confusion among consumers.[2] Congress only recently introduced a comprehensive, bipartisan privacy bill, the American Data Privacy and Protection Act (ADPPA), which in its current form is still not likely to pass given a lack of agreement on multiple key issues and crucially does not preempt all state privacy laws.[3] Furthermore, the longer Congress delays, the more difficult it will be to reach a compromise on data privacy because privacy activists will demand a federal law that does not preempt stricter state laws—or if it does, to model a federal law after California's overly broad and costly privacy law, the California Consumer Privacy Act (CCPA), which itself took inspiration from the GDPR.[4] Both of these outcomes would lead to much higher compliance costs for organizations that handle personal data, costs organizations would likely pass onto consumers.

**Overly broad privacy legislation would come with both significant compliance costs and enormous hidden costs, whereas a more targeted law that still protects consumer privacy would be far less burdensome on organizations, consumers, and the economy.**

Proponents of a GDPR-style data privacy law in the United States argue that, by subjecting organizations to the same rules they must adhere to in the European Union, such a law would reduce compliance costs. There are two problems with this argument. First, there are variable compliance costs, and therefore stricter regulations can increase variable costs. Second, this argument fails to consider that compliance costs are not the only costs associated with data privacy legislation. These additional, or "hidden" costs, represent the economic impact a new privacy law would have by reducing productivity for both consumers and businesses, and restricting data collection and sharing, which drives innovation. Moreover, they argue that compliance costs will be borne by companies and not consumers, which evidence disproves.

Overly broad privacy legislation would come with both significant compliance costs and enormous hidden costs, whereas a more targeted law that still protects consumer privacy would be far less burdensome on organizations, consumers, and the economy. In order to minimize the economic impact of privacy legislation, Congress should pass a comprehensive law that preempts state and local laws and minimizes the costs of data protection while still addressing actual privacy harms and protecting consumer privacy.

## THE GDPR

The European Parliament passed the GDPR in 2016 and the law went into effect in 2018. It contains several provisions intended to give consumers more control over their personal data, including user rights to data access, portability, deletion, and rectification, as well as a right to

information about how their data is processed, a right to object to data processing, and a right to avoid automated decision-making; obligations on how data controllers and data processors must protect personal data; enforcement by data protection authorities of member states and allowance for a private right of action; and hefty fines up to €20 million or 4 percent of annual global revenue.[5]

Some privacy advocates have called for the U.S. to pass a law similar to the GDPR, arguing that doing so would better protect American consumers' privacy, streamline the current patchwork of federal and state regulations, and harmonize U.S. and EU law.[6] This would follow the trend of states taking inspiration from the GDPR in their privacy laws and bills, as not only does California's law draw on the GDPR, but proposed legislation in Washington and New York have as well.[7]

While streamlining the various privacy regulations in the United States is an important goal that would save billions for businesses that otherwise find themselves subject to multiple, duplicative rules, a GDPR-like law would come with significant costs and may also fail to produce its intended outcomes.[8] After the first year of GDPR enforcement, the Information Technology and Innovation Foundation's (ITIF's) Center for Data Innovation found that the GDPR negatively affects the EU economy and businesses while failing to increase trust among users, negatively impacting users' online access, and straining regulatory resources.[9]

## THE TWIN COSTS OF DATA PROTECTION

Data privacy laws impose costs on organizations that are required to comply with the laws' provisions. The extent of these costs, and the burden they place on organizations, depends on which provisions are included in a given law, as well as the law's enforcement mechanisms.

Estimates of the cost of privacy legislation factor in two types of costs. The first is compliance costs that laws directly impose on organizations by requiring them to comply with certain provisions. These provisions may include requirements to hire and retain data protection officers, conduct privacy audits, build and maintain data infrastructure, and ensure data access, portability, deletion, and rectification for users. Some of these may be fixed costs, such as creating a process and infrastructure for handling data deletion requests, whereas others may be variable costs, such as the cost to respond to each deletion request. Compliance costs may also include costs associated with responding to regulators or civil lawsuits. For example, some privacy laws allow users to sue organizations directly for civil penalties, which is known as a private right of action.

The second set of costs is "hidden costs." These encompass the costs of less productivity and innovation in industries powered by data—which, in today's economy, is virtually every industry. Examples of hidden costs include lower consumer efficiency, less access to data, and lower ad effectiveness. While compliance costs affect every individual organization covered under a law's purview, hidden costs affect the entire economy.

The difference between a broad data privacy law and a more tailored law, in terms of economic impact, is significant. ITIF research conducted in 2019 determined that federal legislation mirroring key provisions of the GDPR or CCPA could cost the U.S. economy approximately $122 billion per year, whereas a more focused, but still effective national data privacy law would cost

about $6 billion per year, around 95 percent less.[10] This includes both direct regulatory compliance costs of up to $17 billion and indirect "hidden" costs of up to $106 billion.[11]

Notably, these hidden costs make up a much larger percentage of the total costs associated with a GDPR-like U.S. privacy law. An effective but streamlined privacy law would minimize not only compliance costs but also the indirect economic costs associated with decreased productivity and innovation, saving the U.S. economy billions of dollars every year.

**Table 1: Annual costs associated with a GDPR-style law versus a targeted law (US $Millions)**

| Description of Cost | GDPR-Style Law ($M) | Targeted Law ($M) |
|---|---|---|
| **Data Protection Officers** | $6,370 | N/A |
| **Privacy Audits** | $440 | $440 |
| **Data Infrastructure** | $5,380 | $5,380 |
| **Data Access** | $340 | $90 |
| **Data Portability** | $510 | $130 |
| **Data Deletion** | $780 | $200 |
| **Data Rectification** | $190 | $50 |
| **Enforcement** | $2,710 | $210 |
| **Lower Consumer Efficiency** | $1,870 | N/A |
| **Less Access to Data** | $71,000 | N/A |
| **Lower Ad Effectiveness** | $32,900 | N/A |
| **TOTAL** | **$122,790** | **$6,500** |

## Compliance Costs

Lawmakers are more likely to consider compliance costs when crafting a new privacy law because those are the costs the law directly imposes on organizations. This category encompasses any costs that arise from organizations changing the way they operate in order to comply with a privacy law's provisions. It also encompasses the cost of duplicative or frivolous enforcement mechanisms in the form of legal fees and potential civil penalties from a private right of action. These compliance costs add up to approximately $16.7 billion per year.[12]

First, privacy laws may require organizations to designate a data protection officer responsible for compliance. This imposes a cost on organizations by requiring them to either hire additional personnel to handle consumer privacy requests, system upkeep, and regulatory compliance or delegate these tasks to existing personnel, thereby diverting their time from other activities. ITIF estimated the annual cost of requiring data protection officers for all U.S. organizations that handle personal data would be $6.4 billion.[13]

Second, privacy laws may require organizations to submit compliance audits, or even direct inspections, conducted either by the organizations themselves or by a third party. ITIF estimated the annual cost of requiring these audits for all U.S. organizations that handle personal data would reach $440 million.[14]

Third, the rights that many privacy laws give users come with costs for organizations that handle those users' personal data. These rights may include the right to access their personal data stored by an organization (data access), port that data to other services (data portability), delete that data (data deletion), or make corrections to that data (data rectification).

In order to fulfill these requirements, organizations need to build and maintain data infrastructure that allows them to store, find, and update users' personal information; create a mechanism to verify and authenticate users to prevent data theft; and process each request they receive to access, port, delete, or correct a user's personal data.

The estimated annual cost of providing a right to data access, portability, deletion, and rectification in the United States would be $7.2 billion, including $5.4 billion for data infrastructure, $340 million for access requirements, $510 million for portability, $780 million for deletion, and $190 million for rectification.[15]

**Federal legislation mirroring key provisions of the GDPR or CCPA could cost the U.S. economy approximately $122 billion per year, whereas a more focused, but still effective national data privacy law would cost about $6 billion per year, around 95 percent less.**

In Europe, companies reported spending an average of $1.3 million on GDPR compliance in 2017 and were expected to spend an additional $1.8 million in 2018.[16] Countries' Data Protection Authorities (DPAs) have further increased compliance costs through decisions that make it more difficult to comply with the GDPR. In February 2022, the Belgian DPA issued a ruling that a widely used technical standard built for publishers, advertisers, and technology vendors to obtain user consent for data processing does not comply with the GDPR.[17] This requires websites and publishers that want to implement GDPR-compliant processes to have to build their own frameworks, creating additional costs that especially burden smaller organizations with fewer resources.

Finally, effective privacy legislation needs some sort of enforcement mechanism. There are multiple avenues for enforcement that are not mutually exclusive, each carrying their own costs and trade-offs.[18] Congress could give the Federal Trade Commission (FTC) the authority to enforce a comprehensive data privacy law, expanding upon the FTC's existing role as the primary federal regulator for consumer privacy.[19] Alternatively, Congress could create a new data protection agency specifically charged with oversight and enforcement of a new privacy law.

Congress could also involve the states by empowering state attorneys general to enforce a new privacy law, in addition to federal enforcement. And finally, Congress could establish a private right of action, enabling users to sue a company directly for violations of the privacy law. This private right of action could be broad or limited in scope, offering only injunctive relief or both injunctive and monetary relief, and applying to all violations or only to specific violations, such as data breaches.

The economic cost of enforcement would be much higher if legislation allowed for duplicative or frivolous enforcement, particularly in the case of a broad private right of action. This would open the floodgates for unnecessary, baseless lawsuits against organizations that handle personal data, which would disincentivize organizations from offering innovative new products or services that may open them up to liability.

Illinois' Biometric Information Privacy Act (BIPA) is a prime example of this. The law regulates the collection of biometric data by companies operating in Illinois or whose products reach consumers in Illinois, and includes a private right of action that allows both consumer class action lawsuits and employer lawsuits. Although BIPA passed into law in 2008, the number of lawsuits exploded after courts ruled in 2019 that plaintiffs are not required to show harm.[20] Between 2008 and 2018, there were 163 BIPA class action lawsuits, while in 2019 alone, there were over 300, and recent BIPA lawsuits have included several high-profile cases with settlements reaching $650 million.[21] This has led some companies to pull out of Illinois or limit the technology available to Illinois consumers.[22]

Privacy activists frame broad private right of action as a gift to consumers, providing them with access to remedies against organizations that have violated their privacy.[23] However, even in the case of legitimate privacy lawsuits, the payouts are often small and attorney fees are often high. Ultimately, privacy lawyers are the only group that would significantly benefit from a broad private right of action.[24]

Meanwhile, the economy would suffer as the high cost of litigation dramatically drives up costs for organizations that handle personal data, diverting funds away from innovating and creating new products and services. Consumers would also suffer as organizations pass these costs along to them by driving up prices, charging for services that were previously free, or offering discounts less frequently. ITIF estimated the annual cost of duplicative enforcement mechanisms would be $2.7 billion if a federal data privacy law included a broad private right of action.[25]

The ADPPA attempts to strike a compromise on a private right of action. It would allow individuals to bring civil actions seeking compensatory or injunctive relief against data holders starting four years after the act goes into effect. To limit duplicative enforcement, individuals must first notify their state attorney general and the FTC of their intent to bring a suit, and if one of those agencies decides to initiate an action, individuals cannot file their own lawsuit. There is also a limited right to cure, whereby if a data holder successfully addresses an alleged problem within 45 days, they can seek dismissal of a demand for injunctive relief.[26] However, this private right of action would still leave the door open for expensive, frivolous lawsuits. The only lawsuits that could proceed under the ADPPA would be those the FTC and state attorneys general opt not to pursue, meaning these suits are likely to be meritless.

Evidence shows that companies pass on compliance costs to consumers in order to reduce the impact they would have on their business. This can come in the form of either raising prices for paid services or charging for services that were previously free. Researchers from the United States and United Kingdom found in 2019 that, across all industries, federal government regulations lead to higher consumer prices, and that this disproportionately impacts low-income households.[27]

One argument for replicating the GDPR's approach to data privacy in the United States is that it would be efficient because organizations that already have to comply with the GDPR's rules would not have to also comply with a competing set of rules. However, this argument not only does not consider hidden costs, which are unrelated to compliance and are instead a result of the economic impact of less productivity and innovation—an inevitable consequence of GDPR-like privacy rules—it also fails to differentiate between multinational and non-multinational organizations, and fixed and variable compliance costs.

The cost savings associated with a GDPR-like law in the United States would only apply to multinational organizations that have users or conduct transactions in the EU. Non-multinational organizations that only operate in the United States or in non-EU foreign markets do not have to comply with the GDPR's rules. An overly broad, GDPR-like U.S. law would pose significant new compliance costs on these organizations.

Additionally, both multinational and nonmultinational organizations still have to pay new variable costs. Many of the compliance costs a GDPR-like law would impose are fixed costs, such as hiring and retaining data protection officers, conducting privacy audits, and some of the costs associated with ensuring data access, portability, deletion, and rectification. But there are also variable costs associated with ensuring data access, portability, deletion, and rectification, and these costs would significantly increase for multinational organizations that already operate in the EU were the United States to pass a GDPR-like data privacy law. The cost of duplicative enforcement—especially a private right of action—would also affect both multinational and non-multinational organizations.

For an example of the costs imposed by GDPR-like legislation, look no further than the CCPA, which mimicked the GDPR in many of its provisions.[28] Despite these similarities, the CCPA still imposed significant compliance costs on California-based firms. A 2019 estimate produced by Berkeley Economic Advising and Research, LLC and prepared for California's attorney general finds that the CCPA would cost the Californian economy upwards of $55 billion in initial compliance costs.[29] As the report notes, many of the firms covered in this estimate already comply with the GDPR.[30] However, the costs of compliance with the CCPA were still significant.

Meanwhile, in Europe, the GPDR has also come with significant costs for businesses. European businesses required to comply with the law saw their profits shrink by an average of 8.1 percent. In the information technology (IT) sector, small firms experienced profit declines of 12.5 percent, while large firms saw a comparatively lesser decline of 4.6 percent, indicating that the costs of the GDPR disproportionately impact smaller organizations.[31]

However, existing compliance costs related to federal privacy laws for sensitive forms of data—such as health or financial data—do create a compelling argument for making a new, comprehensive federal privacy law interoperable with existing laws to simplify compliance for organizations that already handle these forms of data as well as other forms of personal data.

## "Hidden Costs"

The second set of costs associated with new privacy legislation is "hidden costs," or costs that lawmakers are perhaps less likely to consider when crafting a privacy law. These are not costs that a law would directly impose on organizations, but are instead the overall economic costs

associated with less productivity and innovation. These hidden costs add up to approximately $105.8 billion per year.[32]

Though these costs are less obvious than compliance costs, they can be much higher, because they affect the entire economy, not just the organizations that fall within a privacy law's purview. This would especially be the case if new federal privacy legislation were unnecessarily stringent, restricting forms of data usage that benefit the public good and have minimal privacy risks rather than focusing on specific privacy harms and encouraging data innovation where it would benefit consumers and the economy.

The first hidden cost of privacy legislation is lower consumer efficiency. This arises from transparency requirements intended to help users better understand their rights and how their information is collected and used so they can make more informed decisions about how they share their personal data. When these requirements lead to pop-up notices that users must click through in order to access content, they can take time to review and respond to. ITIF estimated the productivity cost of a U.S. pop-up consent notice policy would be $1.9 billion each year.[33]

The second hidden cost of privacy legislation results from lower productivity and opportunity costs associated with rules such as opt-in consent, data minimization, and purpose specification requirements that reduce access to data, limit data sharing, and constrain its use.

Opt-in consent requirements lead fewer users to share their data because most users select the default option of not giving consent, often for irrational reasons. Additionally, obtaining opt-in consent costs significantly more than an opt-out system, wherein users can revoke consent to have their data collected. Given the thin margins involved in data-related transactions such as targeted advertising, companies could end up passing these costs onto consumers.[34]

Data minimization requires organizations to collect no more data than is necessary to meet specific needs, negatively impacting organizations that do not know which data will be most valuable when initially deciding what data to collect, as well as limiting organizations' ability to analyze data in the development of new products and services.

**Hidden costs can be much higher than compliance costs, because they affect the entire economy, not just the organizations that fall within a privacy law's purview.**

Finally, purpose specification requires organizations to disclose to users the purposes for which they are collecting data and not use this collected data for any other reasons. Like data minimization, purpose specification limits innovation, as organizations cannot reuse collected data for new purposes or apply data analytics to collected data.

Opt-in consent, data minimization, and purpose specification requirements are designed to limit. These rules assume more data collection is harmful, ignoring that the positive externalities from data are often public goods. Health researchers use data to track diseases, research cures, and accelerate innovation.[35] Smart city technologies are another example of how data collection can benefit society by reducing traffic, saving energy, and addressing infrastructure needs.[36]

By reducing overall access to data, such requirements not only impede these and other important goals, they also limit how organizations can generate value from data. This would result in an

estimated $71 billion annually in lost value across the U.S. economy, particularly in sectors that rely on data to drive productivity and innovation, including education, transportation, consumer products, electricity, oil and gas, health care, and consumer finance.[37]

The third and final hidden cost of privacy legislation results is lower ad effectiveness. Targeted advertising is one of the key pillars of the Internet economy, and data privacy rules that limit the effectiveness of targeted advertising would hurt businesses that rely on ads to promote their goods and services, apps and services that use the revenue from targeted ads to offer their services at a low or no cost, and consumers that use these free or low-cost online services and do much of their shopping online.[38] ITIF estimated the cost of lower ad effectiveness would be $33 billion in lost value annually.[39]

The GDPR came with significant hidden costs, including fewer mergers and acquisitions due to compliance concerns, data protection requirements acting as a barrier to the development of new technologies, decreased venture funding and fewer venture deals for EU tech firms, and less market reach for advertising vendors.[40]

The existence of hidden costs further undermines the argument that replicating the GDPR's approach in a U.S. federal data privacy law would reduce costs by only subjecting organizations to one cohesive set of rules rather than two conflicting ones. The estimated hidden costs associated with GDPR-style legislation in the United States total $106 million annually, or 86 percent of the total annual cost of GDPR-style privacy legislation.[41] More targeted legislation would significantly reduce the economic cost of privacy legislation, preserving productivity and innovation while reducing actual privacy harms.

## Reducing the Hidden Costs of Privacy

Comprehensive federal data privacy legislation imposes some costs on organizations that handle personal data, and it would be a mistake for Congress to only consider compliance costs when drafting data privacy legislation. Congress should seek to minimize both the compliance costs and the hidden costs by passing a targeted set of rules that still protect consumers. This approach would be significantly less burdensome—on organizations that handle personal data and the overall American economy—than overly broad legislation that mimics the GDPR would be.

ITIF previously estimated the cost of targeted privacy legislation that includes several key components to ensure proper oversight and enforcement and establish a set of user rights. First, to ensure compliance, a targeted federal privacy law could still require privacy audits, which would cost organizations roughly $440 million per year.[42]

Second, to enforce a targeted federal privacy law, Congress could rely on federal and state regulators—specifically the FTC and state attorneys general—instead of allowing a private right of action that would significantly drive up the cost of duplicative enforcement. By allowing both federal and state regulators to take action on violations of federal privacy law, there would be some duplicative enforcement, costing organizations roughly $210 billion per year, a fraction of the projected costs associated with a private right of action.[43]

Third, Congress could still give consumers more control over their data by providing them with the right to access, port, delete, and rectify their data in a targeted privacy law. To drive down

costs, Congress could limit when these requirements apply, such as by only requiring organizations that process sensitive data in certain industries to provide those types of user control, rather than applying it across the board to all organizations processing user data. This would cost organizations roughly $5.9 billion, including $5.4 billion for data infrastructure, $90 million for access requirements, $130 million for portability, $200 million for deletion, and $50 million for rectification.[44]

In total, a broad, GDPR-style U.S. privacy law would cost $122 billion per year, while a more targeted law would cost around 95 percent less, or $6.5 billion.[45]

As a final cost-saving measure, comprehensive, targeted federal data privacy legislation could preempt any existing or future state and local privacy laws. State privacy laws create significant compliance costs not only for in-state organizations but also for out-of-state organizations that find themselves subject to multiple, duplicative rules. ITIF research finds that these out-of-state costs could run from $98 billion to $112 billion annually, exceeding $1 trillion over a 10-year period.[46] By creating a uniform set of rules that applies nationwide and preempting these conflicting state rules, federal legislation would significantly reduce costs and confusion.

## RECOMMENDATIONS

ITIF outlined in a previous report specific recommendations for what Congress should include in a federal privacy law.[47] Several of these recommendations would drive down the costs associated with federal data privacy legislation—including both compliance costs and hidden costs—while still protecting users' privacy and addressing specific privacy-related harms.

- **Federal privacy legislation should set a national standard for consumer data protection and preempt state and local governments from passing their own laws that would add to or subtract from these protections.** This preemption should apply to all state and local data privacy laws. Doing so would create a consistent set of rules for all U.S. organizations to follow, minimizing confusion and costs.
- **Federal privacy legislation should distinguish between sensitive personal data, such as an individual's medical history or financial information, and nonsensitive data.** The goal should be to create different levels of data protection based on the sensitivity and risk of each type of data. Each level would have distinct types of protections. Doing so would reduce costs for organizations that handle nonsensitive personal data and would enable greater innovation using this nonsensitive data.
- **Federal privacy legislation should exempt de-identified data—including anonymized, pseudonymized, and aggregated data—and publicly available data from both of its definitions of nonsensitive and sensitive personal data.** This would likewise enable greater innovation using de-identified or publicly available data in ways that would not infringe on individual users' privacy.
- **Federal privacy legislation should only require organizations to obtain affirmative (opt-in) consent if they are collecting sensitive personal data, such as health or financial data.** Organizations collecting nonsensitive personal data should be required to adhere to an opt-out standard or should only be required to provide notice and choice. Doing so would reduce both the compliance costs and the hidden costs associated with obtaining opt-in

consent in most cases while still increasing transparency around data collection and giving users greater control.

- **When establishing privacy notice requirements, Congress should avoid requiring pop-up notices or interstitials that users must click through to give their consent,** which result in higher costs and lower consumer efficiency with little to no privacy benefit.
- **Federal privacy legislation should provide users with the right to access, port, delete, and rectify their data.** However, Congress should limit when those requirements apply, such as by only requiring organizations that process sensitive data in certain industries to provide those types of user control, rather than applying it across the board to all organizations processing user data.
- **Federal privacy legislation should not include data retention limitations, data minimization requirements, or purpose specification requirements,** which limit innovation and flexibility in ways that may ultimately benefit consumers.
- **Federal privacy legislation should not require a data protection officer.** Instead, it should require organizations to provide a means to contact them for privacy- and security-related concerns, allowing them to be flexible in their staffing and compliance decisions and reducing costs associated with hiring new personnel.
- **Federal privacy legislation should be based on a standard of tangible consumer harm when assessing penalties.** Doing so would help create a system of incentives to promote desirable behavior while discouraging undesirable behavior in a way that limits compliance costs and avoids restricting productivity and innovation.
- **Federal privacy legislation should not create a private right of action.** This would unnecessarily expose companies to substantial legal costs, forcing them to focus more on fighting meritless lawsuits and less on designing safe and innovative products and services for consumers.

One reason some in Congress have pushed for a European-style data protection regime is they believe these regulations come without significant costs—either directly to consumers or to innovation. Indeed, to justify its extensive and burdensome data protection regulations, the EU has crafted a myth that the GDPR actually spurs growth and innovation. As ITIF's and other studies show, this is simply not true.[48] Moreover, stronger data privacy laws do not necessarily increase consumer trust or digital adoption.[49]

An overly stringent federal data privacy law would come with costs not only for businesses that handle consumers' personal data but for the entire American economy. Inaction also comes with costs, as states continue to pass their own laws that each impose overlapping costs on in-state and out-of-state businesses.

A more targeted federal data privacy law would enshrine important consumer privacy rights, prevent real privacy harms, preempt inconsistent state laws, and minimize the impact on productivity and innovation. This approach would strike a balance that benefits consumers and businesses and allows the data-driven Internet economy to continue to thrive.

## About the Authors

Ashley Johnson (@ashleyjnsn) is a senior policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation, and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

Daniel Castro (@CastroTech) is vice president of 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.

## 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 us at www.itif.org.

## ENDNOTES


1. Taylor Kay Lively, "US State Privacy Legislation Tracker," *International Association of Privacy Professionals*, updated March 24, 2022, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
2. Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Costs of a Patchwork of State Privacy Laws" (ITIF, January 2022), https://itif.org/sites/default/files/2022-state-privacy-laws.pdf.
3. Jacob Bogage and Cristiano Lima, "House and Senate members unveil stalled data privacy bill," *The Washington Post*, June 3, 2022, https://www.washingtonpost.com/technology/2022/06/03/internet-privacy-congress-compromise-proposal/; "American Data Privacy and Protection Act [Discussion Draft]," House Committee on Energy and Commerce, accessed June 7, 2022, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Bipartisan_Privacy_Discussion_Draft_Bill_Text.pdf.
4. Daniel Castro and Ashley Johnson, "Why Can't Congress Pass Federal Data Privacy Legislation? Blame California" (ITIF December 13, 2019), https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california.
5. Laura Jehl and Alan Friel, "CCPA and GDPR Comparison Chart" (Thomson Reuters, 2018), https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf.
6. Michele E. Gilman, "Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice," *Arizona State Law Journal* 52 (2020): 368–444, https://scholarworks.law.ubalt.edu/all_fac/1109/; Estelle Masse, "Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers" (Access Now, November 2018), https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf.
7. Bryan Clark, "GDPR in the USA? New State Legislation Is Making This Closer to Reality," *National Law Review*, March 18, 2021, https://www.natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality.
8. Castro, Dascoli, and Diebold, "The Looming Costs."
9. Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (Center for Data Innovation, June 2019), https://www2.datainnovation.org/2019-gdpr-one-year.pdf.
10. Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (ITIF, August 2019), https://itif.org/sites/default/files/2019-cost-data-privacy-law.pdf.
11. Ibid., 2.
12. Ibid., 2.
13. Ibid., 4.
14. McQuinn and Castro, "The Costs," 6.
15. Ibid., 8–14.
16. IAPP and Ernst & Young, "Annual Governance Report 2018" (IAPP and Ernst & Young, 2018), https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.
17. "The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR," Belgian Data Protection Authority, published February 2, 2022, https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr.

18. Jennifer Huddleston, "A Primer on Data Privacy Enforcement Options," *American Action Forum*, May 4, 2020, https://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/.
19. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).
20. Teresa Milano, "The BIPA Litigation Landscape and What Lies Ahead," *Woodruff Sawyer*, April 1, 2021, https://woodruffsawyer.com/cyber-liability/bipa-litigation-landscape/; *Patel v. Facebook, Inc.,* 932 F.3d 1264 (9th Cir. 2019), https://cdn.ca9.uscourts.gov/datastore/opinions/2019/08/08/18-15982.pdf.
21. Joseph Stafford, Michael Duffy, and Ashley Conaghan, "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; Victoria Cavaliere, "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.
22. Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview AH Has Promised To Cancel Relationships With Private Companies," *Buzzfeed News*, May 7, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies; "Familiar face detection," Google Nest Help, accessed May 20, 2022, https://support.google.com/googlenest/answer/9268625?co=GENIE.Platform%3DAndroid&hl=en; Amy Korte, "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/.
23. Becky Chao, Eric Null, and Claire Park, "Enforcing a New Privacy Law" (New America, November 2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/.
24. Daniel Castro, "Who Stands to Benefit the Most From New Data Privacy Laws? Lawyers" (ITIF, August 9, 2019, https://itif.org/publications/2019/08/09/who-stands-benefit-most-new-data-privacy-laws-lawyers.
25. McQuinn and Castro, "The Costs," 15.
26. "American Data Privacy and Protection Act."
27. Dustin Chambers, Courtney A. Collins, and Alan Krause, "How do federal regulations affect consumer prices? An analysis of the regressive effects of regulation," *Public Choice* 180 (2019): 57–90, https://eprints.whiterose.ac.uk/122980/1/Regulation_PC_wp.pdf.
28. Jehl and Friel, "CCPA and GDPR Comparison Chart."
29. David Roland-Holst et al., "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations" (Berkeley Economic Advising and Research, LLC, August 2019), https://iapp.org/media/pdf/resource_center/standardized_regulatory_impact_assessment_CCPA.pdf.
30. Roland-Holst et al., "Standardized Regulatory Impact Assessment," 12.
31. Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally" (Oxford Martin School, January 2022), https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf.
32. McQuinn and Castro, "The Costs," 2.
33. Ibid., 17.
34. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (ITIF, October 6, 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.
35. Ibid.

36. Colin Cunliff, Ashley Johnson, and Hodan Omaar, "How Congress and the Biden Administration Could Jumpstart Smart Cities With AI" (ITIF, March 2021), https://itif.org/sites/default/files/2021-smart-cities-ai.pdf.
37. McQuinn and Castro, "The Costs," 20.
38. Ashley Johnson, "Banning Targeted Ads Would Sink the Internet Economy" (ITIF, January 20, 2022, https://itif.org/publications/2022/01/20/banning-targeted-ads-would-sink-internet-economy.
39. McQuinn and Castro, "The Costs," 21.
40. Chivot and Castro, "What the Evidence Shows," 1–3.
41. McQuinn and Castro, "The Costs," 2.
42. Ibid., 22–23.
43. Ibid., 22–23.
44. Ibid., 22–23.
45. Ibid., 1.
46. Castro et al., "The Looming Costs."
47. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (ITIF, January 2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf.
48. Chivot and Castro, "What the Evidence Shows."
49. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (ITIF, July 2018, https://www2.itif.org/2018-trust-privacy.pdf.